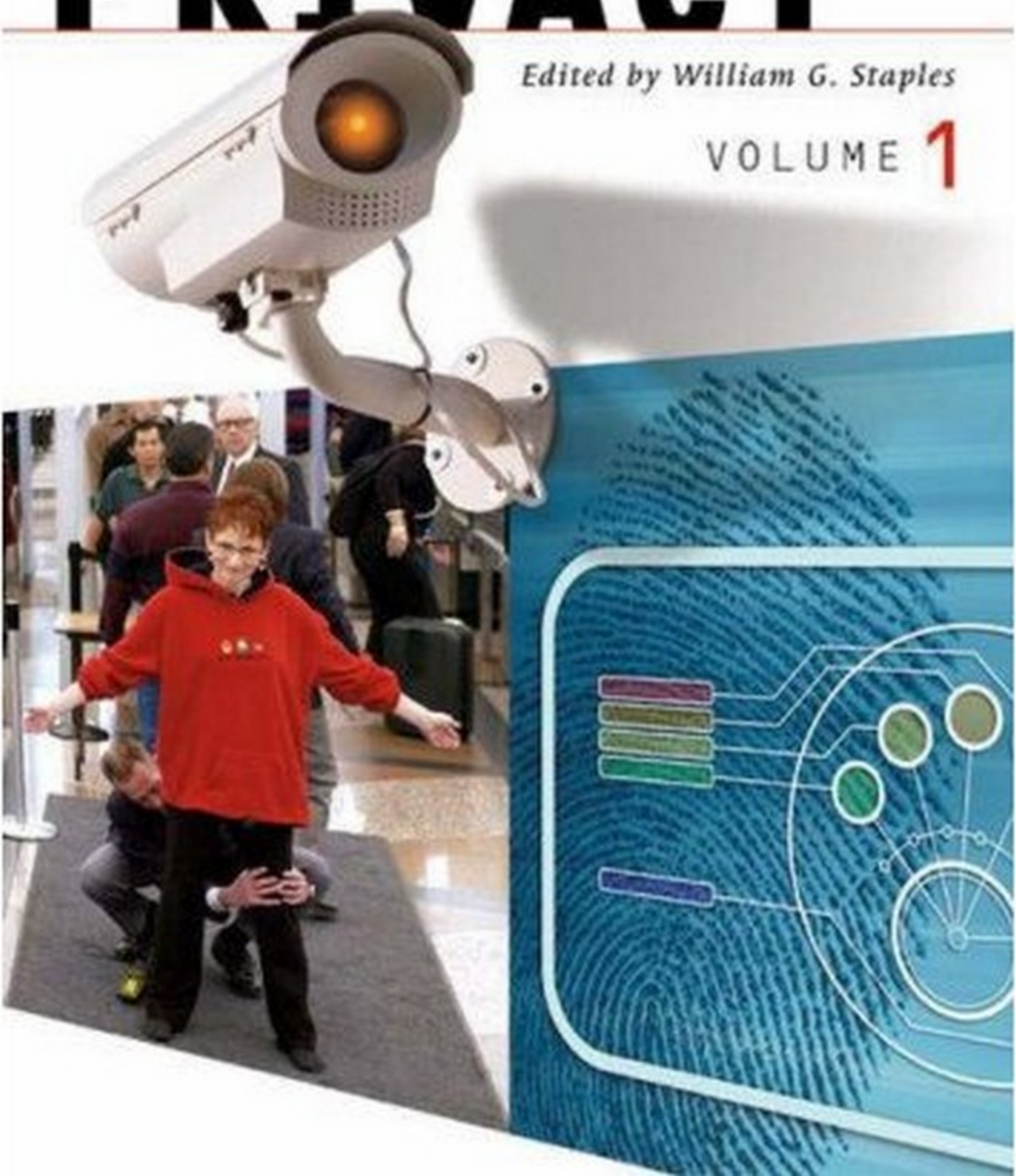


encyclopedia of **PRIVACY**

Edited by William G. Staples

VOLUME **1**



ENCYCLOPEDIA OF PRIVACY

Advisory Board

David J. Brown

The Law Offices of David J. Brown
Lawrence, Kansas

Susan E. Gallagher

Department of Political Science
University of Massachusetts, Lowell

Jill Joline Myers

Law Enforcement and Justice Administration
Western Illinois University

ENCYCLOPEDIA OF PRIVACY



Volume 1: A–M

EDITED BY
WILLIAM G. STAPLES



GREENWOOD PRESS
Westport, Connecticut • London

Library of Congress Cataloging-in-Publication Data

Staples, William G.

Encyclopedia of privacy / edited by William G. Staples.

p. cm.

Includes bibliographical references and index.

ISBN 0-313-33477-3 (set : alk. paper) — ISBN 0-313-33478-1 (vol 1 : alk. paper) —
ISBN 0-313-33479-X (vol 2 : alk. paper) 1. Privacy, Right of—United States—
Encyclopedias. I. Staples, William G.

JC596.2.U5E53 2007

323.44'8097303—dc22 2006031213

British Library Cataloguing in Publication Data is available.

Copyright © 2007 by William G. Staples

All rights reserved. No portion of this book may be
reproduced, by any process or technique, without the
express written consent of the publisher.

Library of Congress Catalog Card Number: 2006031213

ISBN: 0-313-33477-3 (set)

0-313-33478-1 (vol 1)

0-313-33479-X (vol 2)

First published in 2007

Greenwood Press, 88 Post Road West, Westport, CT 06881

An imprint of Greenwood Publishing Group, Inc.

www.greenwood.com

Printed in the United States of America



The paper used in this book complies with the
Permanent Paper Standard issued by the National
Information Standards Organization (Z39.48-1984).

10 9 8 7 6 5 4 3 2 1

Contents

Alphabetical List of Entries	vii
Topical List of Entries	xiii
Preface	xxi
Acknowledgments	xxv
Chronology of Selected Privacy-Related Events	xxvii
The Encyclopedia	1
Resource Guide	625
About the Editors and Contributors	631
Index	641

Alphabetical List of Entries

Abortion
Adoption
Airborne surveillance and intelligence
Air travel
American Civil Liberties Union (ACLU)
Anonymity
Anti-wiretap statutes
Assisted reproductive technologies
Associated Press v. Walker, 388 U.S. 130 (1967)
Authentication
Automatic teller machine
Automobile
Automobile search
Background checks
Banking and financial records
Bank Secrecy Act
Bar code readers and scanners
Bartnicki v. Vopper, 532 U.S. 514 (2001)
Bauer v. Kincaid, 759, F. Supp. 575 (1991)
Big Brother
Biometric identifiers
Birth certificate
Birth control
Blood testing
Bowers v. Hardwick, 478 U.S. 186 (1986)
Boyd v. United States, 116 U.S. 616 (1886)
Brandeis, Louis D. (1856–1941)
Cable Communications Policy Act of 1984
Cady v. Dombrowski, 413 U.S. 433 (1973)
California v. Ciraolo, 476 U.S. 207 (1986)
Camfield v. City of Oklahoma City, 248 F.3d 1214 (2001)
Carnivore

Carroll v. United States, 267 U.S. 132 (1925)
Cellular telephone
Central Intelligence Agency (CIA)
Children's Online Privacy Protection Act of 1998 (COPPA)
Chimel v. California, 395 U.S. 752 (1969)
Civil service laws
Clinton-Lewinsky scandal
Clipper and Capstone chips
Communications Assistance for Law Enforcement Act (CALEA)
Communications Decency Act (CDA)
Computer-Assisted Passenger Prescreening System (CAPPS II) and Secure Flight
Computer Fraud and Abuse Act of 1986
Computer Matching and Privacy Protection Act of 1988
Computers
Confessional culture
Confidentiality
Constitutional protections
Counter Intelligence Program (COINTELPRO)
Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975)
Credit cards
Credit rating
Criminal suspects and arrestees
Cruzan v. Director, Missouri Dep't of Health, 497 U.S. 261 (1990)
Cryptography
Curtilage
Data brokers
Data mining
Davis v. Mississippi, 394 U.S. 721 (1969)
Declaration of Independence
Digital cash
Digital signatures
Dirkes v. Borough of Runnimeade, 936 F. Supp. 235 (1996)
Disclosures
DNA and DNA banking
Do-not-call registry
"Don't ask, don't tell"
Douglas, William O. (1898–1980)
Driver's Privacy Protection Act
Drug testing
Eisenstadt v. Baird, 405 U.S. 438 (1972)
Electronic Communication Privacy Act of 1986
Electronic mail
Electronic surveillance
Electronic toll collection
European Data Protection Directive
Fair Credit Reporting Act
Fair information practices

Family
Family Educational Rights and Privacy Act (FERPA)
Federal Bureau of Investigation (FBI)
Financial Services Modernization Act of 1999
Fingerprints and fingerprinting
Florida v. Bostick, 501 U.S. 429 (1991)
Foreign Intelligence Surveillance Act of 1978 (FISA)
Freedom of association
Freedom of Information Act
Garbage
Gender
Genetic information and testing
Global Positioning System (GPS)
Gossip
Griswold v. Connecticut, 381 U.S. 479 (1965)
Harris v. United States, 331 U.S. 145 (1947)
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Health privacy
Home
Hoover, J. Edgar (1895–1972)
House Un-American Activities Committee (HUAC)
Hudson v. Palmer, 468 U.S. 517 (1984)
Human subjects protections
Identity fraud
Industrial espionage
Inevitable discovery
Internal Revenue Service (IRS)
Internal Security Act of 1950
Internet
Journalism
Katz v. United States, 389 U.S. 347 (1967)
Keystroke loggers
Landlord and tenant
Lawrence v. Texas, 539 U.S. 558 (2003)
Library records
Loving v. Virginia, 388 U.S. 1 (1967)
Manners
McCarthyism
Mere Evidence Rule
Multi-State Anti-Terrorism Information Exchange (MATRIX)
NAACP v. Alabama, 357 U.S. 44 (1958)
National Crime Information Center
National identity cards
National Security Agency
O'Connor v. Ortega, 480 U.S. 509 (1987)
Oliver v. United States, 466 U.S. 170 (1984)
Olmstead v. United States, 277 U.S. 438 (1928)

Open meetings laws
Opt-in vs. opt-out
Osborne v. Ohio, 495 U.S. 103 (1990)
Paparazzi
Paris Adult Theatre I v. Slaton, 413 U.S. 48 (1973)
Partner notification
Password protection
Paternity
Patient rights
Payton v. New York, 445 U.S. 573 (1980)
Peer-to-Peer (P2P) technologies
Pen register
Personally identifiable information
Plain view doctrine
Pretty Good Privacy (PGP)
Prisoners
Privacy, definition of
Privacy, philosophical foundations of
Privacy Act of 1974
Privacy advocacy organizations
Privacy and inequality
Privacy notices
Privacy torts
Private investigators
Private parts
Privilege
Public health and safety
Public/private dichotomy
Public records
Radio Frequency Identification (RFID)
Reasonable expectation of privacy
Red & Black Publishing Co. v. Board of Regents, 262 Ga. 848 (1993)
Red-light and speeding cameras
Reproductive rights
Restrooms and dressing rooms
Right to be let alone
Right to die
Roe v. Wade, 410 U.S. 113 (1973)
Safe harbor principles
Schmerber v. California, 384 U.S. 757 (1966)
Search warrant
Secrecy
Secure Socket Layer (SSL)
Sell v. United States, 539 U.S. 166 (2003)
Senate Select Committee to Study Governmental Operations with Respect to
Intelligence Activities
Sense-enhancing technologies

Sex offender registries
 Sex offenders
 Sexual harassment
 Sexual violence
 Silver platter doctrine
Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 109 S. Ct. 1402 (1989)
 Smart cards
 Sobriety checkpoint
 Social Security number
 Sodomy
South Dakota v. Opperman, 428 U.S. 364 (1976)
 Spam
Stanley v. Georgia, 394 U.S. 557 (1969)
 Stephanie's Law
 Sterilization
 Stop and frisk
 Strip search
 Surveillance
 Surveillance cameras
 Telecommunication Act of 1996
 Telemarketing
Terry v. Ohio, 392 U.S. 1 (1968)
 Thermal sensors
Time, Inc. v. Hill, 385 U.S. 374 (1967)
 Transaction-generated data
 Trespass
 Two-way mirrors
 United States Census
 United States Postal Service (USPS)
United States v. Caldwell, 408 U.S. 665 (1972)
United States v. Dionisio, 410 U.S. 1 (1973)
United States v. Dunn, 480 U.S. 294 (1987)
United States v. Kyllo, 533 U.S. 27 (2001)
United States v. Scheffer, 523 U.S. 303 (1998)
United States v. Steagald, 451 U.S. 204 (1981)
 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)
 Urine analysis
Vernonia School District v. Wayne Acton, 515 U.S. 646 (1995)
 Video Privacy Protection Act of 1988
Village of Bella Terre v. Borass, 416 U.S. 1 (1974)
 Voice identification
 Voyeurism
Warden v. Hayden, 387 U.S. 294 (1967)
Washington et al. v. Glucksberg et al., 521 U.S. 702 (1997)
Watkins v. United States, 354 U.S. 178 (1957)
Webster v. Reproductive Health Services, 492 U.S. 490 (1989)



Weeks v. United States, 232 U.S. 383 (1914)

WHOIS database

Wiretapping

Women and privacy

Workplace privacy

X-ray devices

Zone of privacy

Topical List of Entries

Banking and Financial

- Automatic teller machine
- Banking and financial records
- Bank Secrecy Act
- Credit cards
- Credit rating
- Fair Credit Reporting Act
- Financial Services Modernization Act of 1999
- Privacy notices

Case Law

- Associated Press v. Walker*, 388 U.S. 130 (1967)
- Bartnicki v. Vopper*, 532 U.S. 514 (2001)
- Bauer v. Kincaid*, 759 F. Supp. 575 (1991)
- Bowers v. Hardwick*, 478 U.S.186 (1986)
- Boyd v. United States*, 116 U.S.616 (1886)
- Cady v. Dombrowski*, 413 U.S. 433 (1973)
- California v. Ciraolo*, 476 U.S. 207 (1986)
- Camfield v. City of Oklahoma City*, 248 F.3d 1214 (2001)
- Carroll v. United States*, 267 U.S. 132 (1925)
- Chimel v. California*, 395 U.S. 752 (1969)
- Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975)
- Cruzan v. Director, Missouri Dep't of Health*, 497 U.S. 261 (1990)
- Davis v. Mississippi*, 394 U.S. 721 (1969)
- Dirkes v. Borough of Runnimeade*, 936 F. Supp. 235 (1996)
- Eisenstadt v. Baird*, 405 U.S. 438 (1972)
- Florida v. Bostick*, 501 U.S. 429 (1991)
- Griswold v. Connecticut*, 381 U.S. 479 (1965)
- Harris v. United States*, 331 U.S. 145 (1947)
- Hudson v. Palmer*, 468 U.S. 517 (1984)
- Katz v. United States*, 389 U.S. 347 (1967)
- Lawrence v. Texas*, 539 U.S. 558 (2003)
- Loving v. Virginia*, 388 U.S. 1 (1967)
- NAACP v. Alabama*, 357 U.S. 44 (1958)

O'Connor v. Ortega, 480 U.S. 509 (1987)
Oliver v. United States, 466 U.S. 170 (1984)
Olmstead v. United States, 277 U.S. 438 (1928)
Osborne v. Ohio, 495 U.S. 103 (1990)
Paris Adult Theatre I v. Slaton, 413 U.S. 48 (1973)
Payton v. New York, 445 U.S. 573 (1980)
Red & Black Publishing Co. v. Board of Regents, 262 Ga. 848 (1993)
Roe v. Wade, 410 US 113 (1973)
Schmerber v. California, 384 U.S. 757 (1966)
Sell v. United States, 539 U.S. 166 (2003)
Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 109 S. Ct. 1402 (1989)
South Dakota v. Opperman, 428 U.S. 364 (1976)
Stanley v. Georgia, 394 U.S. 557 (1969)
Terry v. Ohio, 392 U.S. 1 (1968)
Time, Inc. v. Hill, 385 U.S. 374 (1967)
United States v. Caldwell, 408 U.S. 665 (1972)
United States v. Dionisio, 410 U.S. 1 (1973)
United States v. Dunn, 480 U.S. 294 (1987)
United States v. Kyllo, 533 U.S. 27 (2001)
United States v. Scheffer, 523 U.S. 303 (1998)
United States v. Steagald, 451 U.S. 204 (1981)
Vernonia School District v. Wayne Acton, 515 U.S. 646 (1995)
Village of Bella Terre v. Borass, 416 U.S. 1 (1974)
Warden v. Hayden, 387 U.S. 294 (1967)
Washington et al. v. Glucksberg et al., 521 U.S. 702 (1997)
Watkins v. United States, 354 U.S. 178 (1957)
Webster v. Reproductive Health Services, 492 U.S. 490 (1989)
Weeks v. United States, 232 U.S. 383 (1914)

Consumer Privacy

Cable Communications Policy Act of 1984
Credit cards
Data brokers
Data mining
Digital cash
Do-not-call registry
Internet
Opt-in vs. opt-out
Spam
Telemarketing
Transaction-generated data

Ethics and Principles of Privacy

Anonymity
Confidentiality

Constitutional protections
Declaration of Independence
Disclosures
Freedom of association
Human subjects protections
Industrial espionage
Manners
McCarthyism
Privacy, definition of
Privacy, philosophical foundations of
Privacy and inequality
Privilege
Right to be let alone
Secrecy

Gender and Sexuality

Abortion
Assisted reproductive technologies
Birth Control
Bowers v. Hardwick, 478 U.S. 186 (1986)
Clinton-Lewinsky scandal
“Don’t ask, don’t tell”
Eisenstadt v. Baird, 405 U.S. 438 (1972)
Family
Gender
Griswold v. Connecticut, 381 U.S. 479 (1965)
Lawrence v. Texas, 539 U.S. 558 (2003)
Loving v. Virginia, 388 U.S. 1 (1967)
Osborne v. Ohio, 495 U.S. 103 (1990)
Partner notification
Paternity
Paris Adult Theatre I v. Slaton, 413 U.S. 48 (1973)
Private parts
Reproductive rights
Restrooms and dressing rooms
Roe v. Wade, 410 U.S. 113 (1973)
Sex offender registries
Sex offenders
Sexual harassment
Sexual violence
Sodomy
Sterilization
Webster v. Reproductive Health Services, 492 U.S. 490 (1989)
Women and privacy

Law Enforcement

Automobile

Automobile search

Boyd v. United States, 116 U.S. 616 (1886)

Cady v. Dombrowski, 413 U.S. 433 (1973)

California v. Ciraolo, 476 U.S. 207 (1986)

Camfield v. City of Oklahoma City, 248 F.3d 1214 (2001)

Carroll v. United States, 267 U.S. 132 (1925)

Chimel v. California, 395 U.S. 752 (1969)

Communications Assistance for Law Enforcement Act (CALEA)

Criminal suspects and arrestees

Fingerprints and fingerprinting

Florida v. Bostick, 501 U.S. 429 (1991)

Garbage

Hudson v. Palmer, 468 U.S. 517. (1984)

Inevitable discovery

Katz v. United States, 389 U.S. 347 (1967)

Mere Evidence Rule

National Crime Information Center

Oliver v. United States, 466 U.S. 170 (1984)

Olmstead v. United States, 277 U.S. 438 (1928)

Payton v. New York, 445 U.S. 573 (1980)

Plain view doctrine

Private investigators

Prisoners

Search warrant

Silver platter doctrine

Sobriety checkpoint

South Dakota v. Opperman, 428 U.S. 364 (1976)

Stop and frisk

Strip search

Terry v. Ohio, 392 U.S. 1 (1968)

United States v. Caldwell, 408 U.S. 665 (1972)

United States v. Dionisio, 410 U.S. 1 (1973)

United States v. Dunn, 480 U.S. 294 (1987)

United States v. Kyllo, 533 U.S. 27 (2001)

United States v. Steagald, 451 U.S. 204 (1981)

Warden v. Hayden, 387 U.S. 294 (1967)

Weeks v. United States, 232 U.S. 383 (1914)

Legal Statutes and Privacy Laws

Anti-wiretap statutes

Bank secrecy act

Cable Communications Policy Act of 1984

Children's Online Privacy Protection Act of 1998 (COPPA)

Civil service laws

Communications Assistance for Law Enforcement Act (CALEA)

Communications Decency Act (CDA)
Computer Fraud and Abuse Act of 1986
Computer Matching and Privacy Protection Act of 1988
Driver's Privacy Protection Act
Electronic Communication Privacy Act of 1986
Fair Credit Reporting Act
Family Educational Rights and Privacy Act (FERPA)
Financial Services Modernization Act of 1999
Foreign Intelligence Surveillance Act of 1978 (FISA)
Freedom of Information Act
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Internal Security Act of 1950
Open meetings laws
Privacy Act of 1974
Privacy torts
Public records
Stephanie's Law
Telecommunication Act of 1996
Uniting and Strengthening America by Providing Appropriate Tools Required
to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)
Video Privacy Protection Act of 1988

Media

Associated Press v. Walker, 388 U.S. 130 (1967)
Bauer v. Kincaid, 759 F. Supp. 575 (1991)
Confessional culture
Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975)
Gossip
Journalism
Paparazzi
Red & Black Publishing Co. v. Board of Regents, 262 Ga. 848 (1993)
Time, Inc. v. Hill, 385 U.S. 374 (1967)
United States v. Caldwell, 408 U.S. 665 (1972)

Medical and Health Privacy

Blood testing
Cruzan v. Director, Missouri Dep't of Health, 497 U.S. 261 (1990)
DNA and DNA banking
Drug testing
Genetic information and testing
Health privacy
Patient rights
Public health and safety
Right to die
Schmerber v. California, 384 U.S. 757 (1966)
Sell v. United States, 539 U.S. 166 (2003)
Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 S. Ct. 1402 (1989)



Sterilization

Urine analysis

Washington et al. v. Glucksberg et al., 521 U.S. 702 (1997)

Watkins v. United States, 354 U.S. 178 (1957)

National Security

Air travel

Biometric identifiers

Central Intelligence Agency (CIA)

Counter Intelligence Program (COINTELPRO)

Federal Bureau of Investigation (FBI)

Foreign Intelligence Surveillance Act of 1978 (FISA)

Freedom of Information Act

House Un-American Activities Committee (HUAC)

Internal Security Act of 1950

National identity cards

National Security Agency

Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)

Organizations and Committees

American Civil Liberties Union (ACLU)

Central Intelligence Agency (CIA)

Counter Intelligence Program (COINTELPRO)

Federal Bureau of Investigation (FBI)

House Un-American Activities Committee (HUAC)

Internal Revenue Service (IRS)

National Crime Information Center

National Security Agency

Privacy advocacy organizations

Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities

United States Postal Service (USPS)

People

Brandeis, Louis D. (1856–1941)

Douglas, William O. (1898–1980)

Hoover, J. Edgar (1895–1972)

Personal Information

Adoption

Background checks

Bauer v. Kincaid, 759 F. Supp. 575 (1991)

Birth certificate

Computer Matching and Privacy Protection Act of 1988
European data protection directive
Fair information practices
Family Educational Rights and Privacy Act (FERPA)
Identity fraud
Library records
Personally identifiable information
Privacy Act of 1974
Red & Black Publishing Co. v. Board of Regents, 262 Ga. 848 (1993)
Safe harbor principles
United States Census
Social Security number

Private Property

California v. Ciraolo, 476 U.S. 207 (1986)
Curtilage
Home
Oliver v. United States, 466 U.S. 170 (1984)
Landlord and tenant
Stephanie's Law
Trespass
United States v. Dunn, 480 U.S. 294 (1987)
United States v. Kyllo, 533 U.S. 27 (2001)
Warden v. Hayden, 387 U.S. 294 (1967)
Zone of privacy

Surveillance

Airborne surveillance and intelligence
Anti-wiretap statutes
Bartnicki v. Vopper, 532 U.S. 514 (2001)
Big Brother
Electronic Communication Privacy Act of 1986
Electronic surveillance
Katz v. United States, 389 U.S. 347 (1967)
O'Connor v. Ortega, 480 U.S. 509 (1987)
Olmstead v. United States, 277 U.S. 438 (1928)
Private parts
Public/private dichotomy
Reasonable expectation of privacy
Restrooms and dressing rooms
Surveillance
Surveillance cameras
Voyeurism
Wiretapping
Women and privacy
Workplace privacy

**Technology**

- Authentication
- Bar code readers and scanners
- Biometric identifiers
- Carnivore
- Cellular telephone
- Clipper and Capstone chips
- Computer-Assisted Passenger Prescreening System (CAPPS II) and Secure Flight
- Computers
- Cryptography
- Digital signatures
- Electronic mail
- Electronic toll collection
- Global Positioning System (GPS)
- Internet
- Keystroke loggers
- Multi-State Anti-Terrorism Information Exchange (MATRIX)
- Password protection
- Pen register
- Pretty Good Privacy (PGP)
- Radio Frequency Identification (RFID)
- Red-light and speeding cameras
- Secure Socket Layer (SSL)
- Sense-enhancing technologies
- Smart cards
- Thermal sensors
- Two-way mirrors
- Voice identification
- WHOIS database
- X-ray devices

Preface

On any given day, nearly all of us living in the contemporary United States face situations or engage in practices that have implications for personal privacy. We speak on cellular phones in public places, we log on to networked computers that monitor our activities, we purchase goods and services from companies that keep personalized profiles of our buying habits, and we visit medical professionals who retain important personal health information that we assume is kept secure and not shared with others. These and many other everyday events raise intriguing questions and should prompt us to think seriously about the changing nature of privacy in our information-saturated society. The *Encyclopedia of Privacy* is a timely, authoritative reference work designed to offer both basic information and insightful analyses of privacy and privacy-related topics and issues. This book is designed with students and the general reader in mind, although professionals in a variety of fields will also find it to be an invaluable quick-reference guide and source of a number of provocative essays.

By way of introduction to the topic, readers would do well to first consult two “anchor” essays offered here: Professor Judith DeCew’s wide-ranging treatise on the philosophical foundations of privacy and Professor Anita Allen’s insightful entry on the definition of privacy. DeCew traces the deep roots of privacy in the West, from Aristotle through the major political traditions, most of which have assumed and theorized some form of distinction between the public and the private. In the context of modern philosophical debates, DeCew sees several different privacy “camps” that she characterizes as “reductionist,” “coherentist,” and “feminist.” Reductionists deny that there is anything coherent or analytically distinctive or useful about privacy, and generally assert that “privacy rights” are always overlapping with, and may be fully explained by, other property rights or rights to bodily security. Alternatively, coherentists defend the fundamental value of privacy as, as some claim, helping to define our essence as human beings and to protect us against demeaning intrusions and affronts to human dignity. Finally, the feminist critique reminds us that there is a potential “dark side” to an unwavering defense of the special status of privacy rights, since these rights may actually be detrimental to women and others by being used as a shield to mask and maintain power, control, and abuse. What the feminist position illustrates is that the concept



of individualized “privacy rights” is a highly contested view that may in fact run counter to other social and democratic values.

Professor Allen helps us to better understand and define privacy by distinguishing *physical privacy*, *informational privacy*, *decisional privacy*, and *proprietary privacy*. Allen offers a number of examples of each type of privacy, and the reader will note that many of the entries in this volume fit these conceptual categories. But Allen also introduces us to what might be called the “privacy paradox.” As she puts it, “A nation of extensive privacy laws, with a history and culture of privacy protection driven by a concern for civil liberties and human rights, the United States is also a nation in which people can be surprisingly indifferent to privacy and lax about privacy protection.” We see this all around us; for example, citizens voice their outrage when a government surveillance program comes to light but with the same breath advocate the fingerprinting of welfare recipients. While some take a stand against the adoption of a national identification card, others post intimate pictures of themselves on the Internet. Consumers claim that they very much oppose companies tracking their shopping habits, and then they routinely and voluntarily offer personal information in the form of coupons, warranty cards, and contest registration forms. These and other examples suggest that the contemporary privacy landscape is quite complex and defies simplistic and nostalgic interpretations that would have us believe that personal privacy is something that flourished in the past and is now being systematically destroyed.

This two-volume encyclopedia began with a commitment to try to capture some of this complexity. It is the product of more than two years’ work and contains 226 entries ranging from brief technical explanations of various computer technologies to lengthy essays, such as the two outlined above, exploring the philosophical, cultural, and legal bases of our understandings and beliefs about privacy. How did I decide which topics to include and which ones to leave aside? With the help of my Advisory Editors, we began by building a global list of possible topics. We scoured the texts, bibliographies, and indexes of hundreds of scholarly books and articles to help us identify key concepts, events, legal cases and laws, organizations, technological developments, major figures, and ethical debates. After creating this exhaustive list, and keeping in mind the idea that this book would be most useful to the general reader rather than the specialist, I began the process of reducing the number of entries to fit the parameters given to me by the publisher. I eliminated overlap by collapsing topics and focused on, for example, only the court cases that legal scholarship suggested were most vital. I also worked hard to make sure that various “standpoints” were reflected in the final entries, especially with regard to the social dimension of gender.

Once a “working list” of entries was established, I began inviting experts and researchers in a variety of fields—the social sciences, law, technology studies, criminal justice, and others—to contribute entries. More than one hundred of some of the most noted and accomplished scholars, technology experts, policy practitioners, and privacy advocates representing an amazingly diverse group of perspectives ultimately took up the challenge. In many cases, these individuals suggested modifications to topics—for example, narrowing or widening the scope or proposing changes to the length of an entry—while others offered the names of potential contributors. This interactive and cooperative process not only helped me to refine

and improve this book, but it made the final product a truly collaborative effort. The quality of the essays contributed by these individuals reflects not only the breadth of scholarship in the field of privacy studies but also their own deep understanding of and nuanced approach to the issues at hand. In the end, I believe we have “mapped” the privacy terrain with its most fundamental landmarks, which will serve to guide novice researchers in their first excursion into the field.

Locating a topic of interest should be fairly easy. The entries are arranged in a user-friendly, A-to-Z format. The text of each entry is written for the nonspecialist, and jargon has been kept to a minimum. Each article explains the term, describes its importance and relevance to privacy, and often includes concrete examples. Each entry has been cross-referenced with other, related entries denoted by terms that are highlighted in **bold** the first time they appear in a particular entry. Related subjects that do not happen to be cited in the entry appear in a “*See also*” section following many entries. Each entry is also followed by a number of “Suggested Readings” that offer the user more detailed information on the topic. In addition, some popular phrases or terms may be incorporated within larger entries. For example, a reader searching for the computer-related term “cookies” is directed to the more comprehensive entries “Computer” and “Internet.”

The first volume begins with an “Alphabetical Listing of Entries” as well as a “Topical List of Entries.” The latter list should help orient the reader to the major themes and categories that frame the overall project. This is followed by a “Chronology of Selected Privacy-Related Events,” which includes the dates when government acts became law, court decisions were decreed, and various organizations were founded. Such a timeline helps establish a historical context and provides a sense of the trajectory of historical developments.

A detailed subject index for the entire encyclopedia appears in the last pages of Volume 2. A more general “Resource Guide” also appears at the end of Volume 2 that includes a selected bibliography of key books on privacy, as well as a list of relevant websites, organizations, and feature films and documentaries.

Acknowledgments

I have a good number of people to thank for their help on this project. My Advisory Editors, David J. Brown, Susan E. Gallagher, and Jill Joline Myers, devoted long hours to making this book happen, not only by helping me generate the list of entries and finding reviewers, but also writing more than two dozen entries themselves. Brian Zirkle, a doctoral candidate in sociology at the University of Kansas, served as Developmental Assistant and, from the outset, brought his thoughtful, generous, and ultimately indispensable assistance to the project. I thank you all very much for your help, your cooperative spirit, and your good cheer.

One of the benefits of embarking on a venture like this is interacting with and learning from so many different people in a variety of fields. I extend my deep gratitude to the more than one hundred scholars who offered their time, energy, and expertise to this endeavor. Their eager willingness to participate and their dedication to the field of privacy studies and to the public act of scholarship was truly an inspiration to me. Clearly, this work would not exist without their collective help. Special thanks, in this regard, go to Anita Allen, Judi DeCew, Linda Gurak, Doreen Starke-Meyerring, Gary Marx, and Tom Stacey for their major contributions.

In addition, Maya Bernstein, Bob Gellman, and Dan Solove went beyond their role as contributors and reviewed my entry list and/or suggested a number of potential contributors. Matt Dwyer helped organize and edit many of the legal cases included, which was a tremendous help. Shane McCall served as my research assistant during the 2004–2005 academic year and skillfully managed to fill my office with a massive number of books and articles on privacy. The insightful and challenging students in my SOC600 Seminar in Surveillance and Social Control in the spring of 2006 were a constant source of stimulation and amazement. Thanks as well to Steven Ventrano, my former editor at Greenwood Publishing, for inviting me to take on the project and for his sage advice.

I have been fortunate enough to maintain an ongoing conversation about my interest in issues of privacy and surveillance with a number of colleagues, friends, and family members. They include Bob Antonio, Victor Bailey, Nancy Baym, Bill Carswell, Dan Deavours, Ted Frederickson, Marilu Goodyear, Allan



Hanson, Larry Hoyle, Gary Marx, Steven Maynard-Moody, John Monberg, Joane Nagel, Lizette Peter, Wayne Propst, Cliff Staples, and Ian Staples. Finally, thanks to my good friends who constitute the magnanimous and, occasionally, infamous Friday night “Teller’s Group.” You are an endless source of spirited fun, companionship, and community. Cheers to all!

This book is dedicated to Lizette Peter, who teaches me what love is every single day, and to Ian Staples, for becoming the man I am so very proud to call my son.

William G. Staples
Lawrence, Kansas
May 2006

Chronology of Selected Privacy-Related Events

- 1880 A burglary in Tokyo becomes the first recorded case to use fingerprints as evidence.
- 1886 In the case *Boyd v. United States*, the Supreme Court rules that the seizure or compulsory production of one's personal papers to be used as evidence against that person is the same as compelling self-incrimination.
- 1890 Louis Brandeis and Samuel Warren publish the article "The Right to Privacy" in the *Harvard Law Review*.
- 1901 The New York Civil Service Commission begins the first systematic use of fingerprint identifiers in the United States.
- 1914 In the case *Weeks v. United States*, the Supreme Court rules that the warrantless seizure of items from a residence violated constitutional protections.
- 1916 Louis Brandeis is appointed to the Supreme Court.
- 1916 The first birth control center is opened by Margaret Sanger in Brooklyn, New York.
- 1920 The American Civil Liberties Union is founded.
- 1924 J. Edgar Hoover is appointed Director of the Federal Bureau of Investigation.
- 1925 In the case *Carroll v. United States*, the Supreme Court rules that police may make a warrantless search of an automobile if they have probable cause to suspect that it contains contraband.
- 1928 The Supreme Court considers the case *Olmstead v. United States* and finds that wiretapped private telephone conversations recorded by authorities without judicial approval did not violate the Fourth or Fifth Amendment rights of the defendant. This decision was reversed by *Katz v. United States* in 1967.
- 1934 The Federal Communications Act is passed.
- 1938 The House Un-American Activities Committee is commissioned.
- 1939 William O. Douglas is appointed to the Supreme Court.



- 1947 In the case *Harris v. United States*, the Supreme Court affirms the admissibility of evidence of one crime that was found by officers during a proper, but warrantless, search for evidence of another, unrelated crime. The basis for the Court's ruling was subsequently expanded as the test required for the "plain view" doctrine.
- 1949 George Orwell's novel *Nineteen Eighty-Four* is published, introducing the term "Big Brother."
- 1953 Hearings chaired by Senator Joseph McCarthy are held.
- 1956 The first Federal Bureau of Investigation Counter Intelligence (COINTELPRO) program begins.
- 1957 In the case *Watkins v. United States*, the Supreme Court decides that the House Committee on Un-American Activities acted beyond the scope of congressional power.
- 1958 In the case *NAACP v. Alabama*, the Supreme Court first recognizes "freedom of association."
- 1965 The first electronic mail (e-mail) system is created.
- 1965 In the decision regarding the case *Griswold v. Connecticut*, Supreme Court Justice William O. Douglas uses the term "zone of privacy."
- 1965 The first U.S. reports emerge of police using surveillance cameras in public places.
- 1966 The Freedom of Information Act is passed into law.
- 1966 In the case *Schmerber v. California*, the Supreme Court finds that a blood test ordered by police and introduced as evidence in court did not violate the Fifth Amendment guarantee against self-incrimination.
- 1967 In the case *Katz v. United States*, the Supreme Court finds that the Fourth Amendment protection against unreasonable search and seizure requires that the police obtain a search warrant in order to wiretap a public pay phone.
- 1967 In the case *Loving v. Virginia*, the Supreme Court finds that the state of Virginia's anti-miscegenation statute, which banned interracial marriages, violates the Equal Protection Clause of the Fourteenth Amendment.
- 1967 In the case *Warden v. Hayden*, the Supreme Court lets stand a warrantless search by police because there was probable cause and the situation made that course of action imperative.
- 1967 The National Crime Information Center is established.
- 1968 In the case *Terry v. Ohio*, the Supreme Court establishes the "stop and frisk" rule, which permits police to temporarily detain someone for questioning if there are specific facts that would lead a reasonable police officer to believe that criminal activity is occurring.
- 1969 In the case *Davis v. Mississippi*, the Supreme Court holds that an arrest in order to take fingerprint is covered by the Fourth Amendment prohibition against unreasonable searches and seizures.
- 1970 The Fair Credit Reporting Act is passed into law.

- 1970 The Bank Secrecy Act is passed into law.
- 1973 In the case *Roe v. Wade*, the Supreme Court holds that a woman's right to an abortion falls within her right to privacy previously recognized in *Griswold v. Connecticut* and protected by the Fourteenth Amendment.
- 1973 In the case *Paris Adult Theatre I v. Slaton*, the Supreme Court holds that obscene films did not have constitutional protection simply because their display was restricted to consenting adults.
- 1974 The Family Educational Rights and Privacy Act is passed into law.
- 1974 The Privacy Act is passed into law.
- 1975 The first cell phone is patented by Dr. Martin Cooper.
- 1975–1976 The Church Committee reports are published.
- 1976 In the case *South Dakota v. Opperman*, the Supreme Court states that automobiles have less protection under the Fourth Amendment than homes.
- 1978 The Foreign Intelligence Surveillance Act is passed into law.
- 1980 IBM signs a contract with the Microsoft Company to supply an operating system for IBM's new PC model.
- 1984 In the case *Hudson v. Palmer*, the Supreme Court holds that the Fourth Amendment proscription against unreasonable searches does not apply within the confines of the prison cell.
- 1986 In the case *Bowers v. Hardwick*, the Supreme Court finds that there are no constitutional protections for acts of sodomy and that states can outlaw such practices.
- 1986 The Electronic Communications Privacy Act becomes law.
- 1986 In the case *California v. Ciraolo*, the Supreme Court decides that a warrantless, aerial observation of a home and yard did not constitute an illegal search or violate the Fourth Amendment.
- 1986 The Computer Fraud and Abuse Act is passed into law.
- 1986 So-called smart cards begin to be distributed in the United States.
- 1987 In the case *O'Connor v. Ortega*, the Supreme Court finds that a supervisor's search of a public employee's office did not violate the employee's "reasonable expectation of privacy."
- 1988 The Video Privacy Protection Act is passed into law.
- 1988 The Computer Matching and Privacy Protection Act is passed into law.
- 1989 In the case *Webster v. Reproductive Health Services*, the Supreme Court finds that none of the provisions of Missouri legislation restricting abortions infringe upon the right to privacy or the Equal Protection Clause of the Fourteenth Amendment.
- 1990 The Supreme Court hears its first "right to die" case in *Cruzan v. Director, Missouri Dep't of Health*, and finds that while individuals enjoy the right to refuse medical treatment, incompetent persons are not able to exercise such rights.



- 1990 The Human Genome Project formally begins.
- 1992 The World Wide Web is invented by Tim Berners-Lee at the European Particle Physics Laboratory in Switzerland.
- 1992 The first CCTV video surveillance system is installed in Newcastle, England.
- 1993 President Bill Clinton institutes the “Don’t ask, don’t tell” policy in the military.
- 1994 The Communications Assistance for Law Enforcement Act becomes law.
- 1994 The Electronic Privacy Information Center is established.
- 1994 The first use of the Sexually Violent Predator Law (Stephanie’s Law) is made in Kansas.
- 1994 The Driver’s Privacy Protection Act is passed into law.
- 1995 In the case *Vernonia School District v. Acton*, the Supreme Court finds that the school’s student athlete drug policy does not violate the prohibition against unreasonable search and seizure of the Fourth Amendment.
- 1995 The Communications Decency Act is passed into law.
- 1996 The Health Insurance Portability Act becomes law.
- 1996 The Telecommunication Act is passed into law.
- 1997 Carnivore is invented.
- 1997 Princess Diana dies in a car crash, sparking debate about a celebrity’s right to privacy versus the freedom of the press.
- 1998 The European Data Protection Directive goes into effect.
- 1998 The Children’s Online Privacy Protection Act is passed into law.
- 1999 The Financial Services Modernization Act is passed into law.
- 2000 In the case *Lawrence v. Texas*, the Supreme Court holds that the Texas statute making it a crime for two persons of the same sex to engage in certain sexual conduct violates the Due Process Clause of the Fourteenth Amendment.
- 2001 In the case *Bartnicki v. Vopper*, the Supreme Court holds that the First Amendment protects the public disclosure of an illegally intercepted cellular telephone call.
- 2001 The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) is signed into law by President George W. Bush on October 26, just 45 days after the attacks of September 11.
- 2001 In the case *Camfield v. City of Oklahoma City*, the Supreme Court finds that the city violated a citizen’s rights under the Video Privacy Protection Act by obtaining his video rental records without a warrant.
- 2001 In the case *United States v. Kyllo*, the Supreme Court finds that the use of a thermal-imaging device to detect heat emanating from a private home violates Fourth Amendment protections.

- 2003 In the case *Sell v. United States*, the Supreme Court finds that the federal government may compel a mentally ill criminal defendant to take antipsychotic drugs in order to render him competent to stand trial.
- 2003 The National Do-Not-Call Registry goes into effect.
- 2006 Congress reauthorizes the USA Patriot Act as permanent legislation.



Abortion

By the time American women reach the age of 45, about one in three will have had an abortion. Despite its prevalence, the abortion experience is still relegated to the private realm, while the abortion issue continues to generate a storm of protest in the public sphere. To understand this paradox, one must consider the history of abortion, as well as the ideology and tactics of the pro-choice and pro-life movements. The fiercely polarized debate over abortion raises many difficult questions about privacy: Should abortion have been constitutionally and rhetorically grounded in the right to privacy? Can a minor have an abortion without parental consent? If a married woman seeks to terminate a pregnancy, must she notify her husband? Is the right to privacy meaningless if abortion services are inaccessible? How do abortion clinics protect patient **confidentiality**, and can these medical records be subpoenaed? Should anti-abortion activists be able to broadcast the identities of abortion providers and patients, and what impact does this have? How do women manage the stigma of abortion? Will the abortion pill someday enable women to end unwanted pregnancies in the privacy of their own **homes**, and could this depoliticize the issue? Finally, how will the recent changes to the Supreme Court shape abortion policies and practices in the twenty-first century?

During the first half of the twentieth century, abortions were illegal, secretive, and heavily stigmatized, but American women still found ways to get them. Working behind closed doors, some doctors sympathetically aided female patients who were desperate to terminate unwanted pregnancies. In the 1950s and 1960s, women of privilege were sometimes able to get approval from hospital committees for “therapeutic” abortions, while poor women and women of color were more likely to have to rely on self-induced or back-alley abortions, which were painful, life-threatening, and even more covert. In public discourse, this subject was taboo. The Sheri Finkbine case was the first to shine the national spotlight on abortion. During her pregnancy in 1962, Finkbine had been given thalidomide, a tranquilizer that was later discovered to produce severe birth defects. When she went public with her story in order to warn others about the dangers of this drug, the hospital where she was planning to go canceled her scheduled abortion, and she was forced to travel to Sweden for the procedure. Two years later, a German measles outbreak in

the United States resulted in the births of over 20,000 congenitally abnormal babies. Awareness of this situation drove thousands of women to terminate their pregnancies, and it also prompted scrutiny of the restrictive abortion laws by both the medical community and the public.

The 1960s brought technological advances in **birth control**, a sexual revolution, and a climate that was ripe for social protest. During this decade, the second wave of the feminist movement was instrumental in mobilizing support for abortion rights since the abortion issue fit well with the feminist battle cry at the time: “The Personal Is Political.” In the late 1960s, the National Abortion Rights Action League (NARAL) appeared on the political scene, and in Chicago activists created the legendary underground abortion network known as “Jane.”

The *Roe v. Wade*, 410 U.S. 113 (1973) decision, which legalized abortion in 1973, was in many ways a response to this changing social climate and to state-level efforts to reform abortion laws. Some states, like New York, had already lifted their bans on abortion. The case of *Roe v. Wade* involved a challenge to a Texas law, which made abortion a criminal act unless a woman’s life was in danger. The Supreme Court determined that the *inferred* right to privacy in the Constitution was “broad enough to encompass a woman’s decision whether or not to terminate her pregnancy.” Previously, the Court had used a similar rationale to strike down statutes prohibiting married couples’ use of birth control (*Griswold v. Connecticut*, 381 U.S. 479, 1965) and criminalizing the distribution of contraceptives to unmarried people (*Eisenstadt v. Baird*, 405 U.S. 438, 1972). In *Roe*, the Court used a “strict scrutiny” standard, which provides the highest level of **constitutional protection** for Americans’ most fundamental rights. However, the right to privacy for women’s decisions about pregnancy was not absolute: the *Roe* decision stipulated that a state could claim a “compelling” interest in preserving life once the fetus is capable of surviving outside the womb.

Framing abortion as a personal privacy issue for women has been advantageous for the pro-choice movement. Signs at pro-choice rallies boldly proclaim these messages: “Keep Your Laws Off My Body” and “U.S. Out of My Uterus.” Perhaps even more resonant are the slogans that underscore the individual’s right to freedom, like “My Body, My Choice.” The notion of self-determination is fundamental to the American value system. In contrast, radical feminist claims for “abortion on demand” have never been palatable for mainstream audiences. Feminist scholars and legal analysts have debated the efficacy of grounding reproductive rights in privacy as opposed to other possibilities such as the right to health care, the right to equal protection, or the right to consent to bodily intrusion by a fetus. For example, philosophy professor and founder of the National Network of Abortion Funds, Marlene Gerber Fried, sees the rhetoric about abortion as a “private choice” as limited, isolating, and ironically counter to the feminist claim that the personal is political.

The pro-life movement comes at this issue from an entirely different perspective. In this view, the right to privacy pales in comparison with the right to life. Scholars like Kristin Luker, author of *Abortion and the Politics of Motherhood*, explain that competing world-views are at the heart of the conflict over abortion. For pro-life activists, abortion not only represents the destruction of human life, but it also symbolizes a decline in traditional **family** values. The legalization of abortion galvanized the pro-life opposition, as movement successes often do, and it fueled a new era of clashes in judicial, political, and social arenas. Organizations

like the National Right to Life Committee and Operation Rescue (now called Operation Save America) emerged as fierce challengers. According to the National Abortion Federation, which tracks legislative initiatives, 500 bills that would further restrict abortion services were introduced in Congress in 2005, and 26 were signed into law. The pro-life movement's tenacity in pursuing restrictive legislation and its tactical ingenuity have often forced the pro-choice movement into a defensive posture.

The legal precedent that was set in *Roe* has endured for over three decades, but in *Planned Parenthood of Southeastern Pennsylvania v. Casey* (1992), the Court introduced a new standard that allows states to place restrictions on abortion prior to fetal viability, provided that these do not constitute an "undue burden" to the woman. As part of this decision, parental consent laws and waiting periods were allowed, but requiring a woman to inform her husband was considered a substantial obstacle and was therefore deemed unconstitutional.

According to a 2005 Gallup Poll, 64 percent of Americans said they would be in favor of a law requiring that the husband of a married woman be notified if the woman decided to have an abortion. An even higher percentage favored parental consent laws for minors. Opponents stress that most teens do involve a parent or other trusted adult in the decision to terminate an unwanted pregnancy, and that minors are allowed to make other confidential decisions about medical care. For example, all 50 states grant minors the authority to approve the diagnosis and treatment of sexually transmitted diseases. Currently, 34 states have some type of parental involvement stipulation regarding the decision to terminate a pregnancy. In Arkansas, for example, the minor must bring her parent or guardian, or provide that person's notarized signature as an indication of consent, to the clinic. Some states allow minors to obtain a judicial bypass in recognition of the fact that some teens may be victims of incest or subject to abuse if parents were to find out about the pregnancy. There is evidence that parental consent laws increase the likelihood of second-trimester procedures, but these laws may also lower rates of sexual activity, pregnancy, and abortion for young women.

Poor and rural women's access to abortion has also been curtailed. With the cost of a first-trimester surgical abortion averaging around \$400, the cost of this procedure is prohibitive for many women. In addition, 87 percent of U.S. counties lack even a single abortion provider. In states like Wyoming, women must drive hundreds of miles or travel to neighboring states for abortion services. Waiting periods can be particularly taxing for women who have to travel out of state. Although there has been a drop in the number of abortions in recent years, there is an insufficient geographic distribution of abortion providers. In large cities, the situation may be different. In Detroit, for example, abortion clinic owners compete for patients. Some try to gain a competitive edge by offering a more private, spa-like atmosphere, complete with amenities like aromatherapy candles and relaxing music.

This example contrasts dramatically with the emotionally charged battleground outside many abortion clinics. The front lines of the abortion wars have been chronicled extensively. In some places, pro-life activists assemble in peaceable prayer vigils or offer sidewalk counseling and resources to women who are conflicted about their decision. In other places, women must run what they describe as

an intimidating gauntlet of protestors, where they are subjected to gruesome photographs of bloodied fetal parts, pleas of “Don’t kill your baby!” and even threats like “God will punish you!” Members of Operation Save America, who participate in blockades do so in an impassioned effort to compel women to turn away from what the protestors see as the horrors of abortion. Although some women are able to deflect anti-abortion accusations with hostility, others feel shaken, invaded, or tearful. To offset this emotionally taxing journey, clinic workers may try to create a safe space inside the clinic. This can be done with sympathetic reassurances or with security measures like bulletproof glass. While some women feel more at ease with these safeguards to protect their privacy, others perceive the lock-down system as prisonlike and frightening.

Security systems are used to protect clinic workers and patients from sieges, bombings, arson, anthrax, stalking, and violence. Many equate these acts perpetrated by the radical fringe of the anti-abortion movement with terrorism, although those who have murdered abortion doctors see themselves as protecting the lives of unborn babies. Two important victories for the pro-choice movement in this regard came in 1994. The first was the Freedom of Access to Clinic Entrances Act, which makes it a federal offense for any person to threaten, attempt to sabotage, or engage in destructive acts against clinics, or to use violent behavior directed at clinic personnel with the purpose of blocking reproductive health services. The second was *Madsen v. Women’s Health Center*, in which the Supreme Court ruled that a 36-foot buffer zone protecting clinic entrances and a ban on disruptive noise do not curtail the protestors’ rights to free speech: “The First Amendment does not demand that patients at a medical facility undertake Herculean efforts to escape the cacophony of political protests.”

In addition to protesting against those seeking abortions, anti-abortion activists have tried to increase the emotional costs for abortion providers. Protestors have picketed outside providers’ homes, tracked them with binoculars and cameras, and posted identifying information about them and their families. In 1995 the American Coalition of Life Activists (ACLA) distributed wanted posters for a dozen abortion providers who they charged were “Guilty of Crimes Against Humanity.” In 1997 Neal Horsley’s compendium Nuremberg Files website made headlines because the names of abortion providers who had been murdered were struck out, making it look very much like a hit list. Unlike handing out leaflets, posting information on the **Internet** can reach millions of people in a matter of seconds. Such activities affect the privacy rights that help protect abortion providers from harassment and danger. At the state and local levels, laws, ordinances, and injunctions have been sought to restrict these kinds of activities. The **Driver’s Privacy Protection Act of 1994** made it more difficult to obtain personal information based on names and license plates. The Ninth U.S. Circuit Court of Appeals in San Francisco ruled in *Planned Parenthood v. ACLA* that the wanted posters were disseminated to intimidate doctors and constituted a “true threat” of violence. The plaintiffs were awarded \$109 million in damages.

Anti-abortion activists also have made attempts to uncloak patient privacy. Although it is difficult to estimate the extent to which these strategies are used, there have been reports of women who have received abortions being tracked down by phone calls, finding anti-abortion literature on their doorsteps, and having their

family members or acquaintances informed of their abortion decision. In 2001 a woman in Illinois was taken from an abortion clinic to a hospital for the repair of a cervical tear. As she was wheeled out to the ambulance, a protestor took her picture and uploaded it to the Missionaries to the Unborn website, along with information that had been obtained about her hospitalization, age, medical history, family, and hometown. The patient sued the hospital for failing to protect her medical records, as well as the anti-abortion activists for “publicly humiliating her.” In 2002 a website called abortioncams.com was launched, with the explicit goal of shaming “homicidal mothers” and deterring them from entering abortion clinics. Anti-abortion activists have claimed that women going to clinics are using public streets, and that the activists’ “journalistic” right to take pictures is protected by the First Amendment. Opponents counter that women going to a clinic to obtain abortions is not a newsworthy event, and that having their pictures taken is emotionally distressing to the women.

To help protect patient privacy, some clinics enlist volunteers to escort patients. Women’s faces can also be shielded from protestors with umbrellas, or clients can be encouraged to use private entrances. Yellow-page advertisements for abortion providers almost always mention confidentiality. Although the procedures for protecting privacy vary, options of one-on-one counseling, official notices of privacy practices relating to medical records, and forms to indicate preferences regarding follow-up contact may be available. Particularly in smaller communities, a woman might worry about her car being seen in the clinic parking lot or her name being called out in the waiting room. In larger clinics, women may feel they are “herded like cattle” into an open recovery area, or there may be only a thin curtain preventing a woman from being exposed as she undergoes a pelvic exam or reacts with an emotional display. Like providers, patients need privacy to protect them from possible retaliation. Privacy may also enable them to make decisions free from the influence of others and to avoid being judged for their choices.

The question of whether abortion is morally right or wrong continues to be debated, and the public is sharply divided. According to a 2006 Gallup Poll, 53 percent of Americans consider themselves to be pro-choice, while 42 percent consider themselves to be pro-life. A strong, consistent, majority have supported a woman’s right to an abortion under dire circumstances—in cases where the mother’s life is in danger, when conception occurred during rape, or if genetic tests confirm fetal abnormality—but fewer are supportive of abortion under any conditions.

Consequently, women confide with great trepidation, often testing the waters before revealing information. Abortion is usually a closely guarded secret because it is still stigmatized and associated with sexual irresponsibility, although certainly some women do not adopt that point of view. In *Stigma: Notes on the Management of Spoiled Identity*, sociologist Erving Goffman explains that individuals can manage stigma by dividing up their social world, which entails sharing the discrediting information with a relatively small group while concealing it from everyone else. A woman who has an abortion may also try to pretend that everything is okay because she does not want to burden others with the knowledge. Ultimately, this code of silence isolates women from their support networks and renders women who have had abortions invisible in our society. In 2002 approximately

1.29 million abortions were performed in the United States, but personal stories were available infrequently because the abortion experience is so very private.

The abortion pill has the potential to make the abortion experience even more private. Emergency contraception, also referred to as Plan B or the morning-after pill, prevents implantation. It is effective for 72 hours after contraceptive failure or unprotected sex. RU-486, which can be used within 49 days of conception, was approved by the FDA in 2000. At the present time, this “medical abortion” typically involves multiple trips to a clinic. In the first visit, a woman takes mifepristone to block progesterone, without which the lining of the uterus breaks down, ending the pregnancy. This is followed by misoprostol, which causes the uterus to contract and empty. In the final visit, the clinician uses a blood test or an ultrasound to ensure that the abortion is complete. The reviews of this procedure are mixed. Some women feel that it is less invasive, more natural, more like a miscarriage, more humane, relatively easy, not terribly painful, and more private. Others report considerable bleeding, cramping, nausea, and pain from passing the embryo. They also express worries about expelling the material outside of a controlled clinical setting. The drugs may also suppress the immune system and make women more vulnerable to infections. Clinic workers have speculated about the potential of medical abortion to diffuse anti-abortion demonstrations.

Before he took office, President George W. Bush boldly stated, “I do not like abortions. I will do everything in my power to restrict abortions.” Bush’s former attorney general, John Ashcroft, in an effort to defend the federal “partial-birth” abortion ban, sought sensitive medical records of more than a thousand women who had received abortion care. His attorneys argued that “individuals no longer possess a reasonable expectation their histories will remain completely confidential.” Bush’s long-awaited opportunity to nominate justices to the Supreme Court finally came in 2005. The appointments of Chief Justice John Roberts and Judge Samuel Alito have been accompanied by a surge in anti-abortion initiatives. In March 2006 Republican Governor Mike Rounds of South Dakota signed a restrictive abortion ban, which is intended to be a direct challenge to *Roe v. Wade*. As pro-choice organizations mobilize supporters to prevent this law from taking effect, similar abortion bans are pending in at least 10 other states. According to a poll taken by the Pew Research Center in 2005, only 32 percent of Americans would like to see *Roe v. Wade* overturned. But in an ABC News–*Washington Post* poll that same year, 42 percent said they want to make abortion harder to get. At this historic moment, Justice Harry A. Blackmun’s words in the dissenting opinion in *Webster v. Reproductive Health Services* (1989) appear even more prophetic: “Women of this Nation still retain the liberty to control their destinies. But the signs are evident and very ominous, and a chill wind blows.”

See also: **Constitutional protections; Women and privacy**

Suggested Reading: Allen Guttmacher Institute. www.guttmacher.org. Online, March 2006; Blanchard, Dallas A. *The Antiabortion Movement and the Rise of the Religious Right: From Polite to Fiery Protest*. New York: Twayne Publishers, 1994; Fried, Marlene Gerber. *From Abortion to Reproductive Freedom: Transforming a Movement*. Boston: South End Press, 1990; Goffman, Erving. *Stigma: Notes on the Management of Spoiled Identity*. New York: Simon & Schuster, 1986 (1963); Hull, N. E. H., and Peter Charles Hoffer. *Roe v. Wade: The Abortion Rights Controversy*

in *American History*. Lawrence: University Press of Kansas, 2001; Luker, Kristin. *Abortion and the Politics of Motherhood*. Berkeley: University of California Press, 1984; Mohr, James C. *Abortion in America: The Origins and Evolution of National Policy, 1800–1900*. New York: Oxford University Press, 1978; NARAL Pro-choice America. www.prochoiceamerica.org. Online, March 2006; National Right to Life. www.nrlc.org. Online, March 2006; Petchesky, Rosalind Pollak. *Abortion and Woman's Choice: The State, Sexuality, and Reproductive Freedom*. New York: Longman, 198; Reagan, Leslie J. *When Abortion Was a Crime: Women, Medicine, and Law in the United States, 1867–1973*. Berkeley: University of California Press, 1998; Solinger, Rickie (ed.). *Abortion Wars: A Half-Century of Struggle, 1950–2000*. Berkeley: University of California Press, 1998; Staggenborg, Suzanne. *The Pro-Choice Movement: Organization and Activism in the Abortion Conflict*. New York: Oxford University Press, 1991.

Jennifer Keys

Adoption

In historical terms, the legal institution of adoption in the United States is relatively new. It was between the mid-1800s and the 1920s that the states began to pass laws providing for the adoption of children. Before then children had been adopted informally and in some instances by individual legislative acts, or they had come to live with other families under indenture contracts or as a result of legislation authorizing charitable organizations to place children. Under these new adoption statutes, initially the court records of adoptions were not subject to **confidentiality**, and adopted children were not issued new **birth certificates**. Over time, states began to issue new birth certificates and, gradually, to close adoption records—to the public, to all parties to the adoption except for the adult adoptee, and ultimately (in almost all the states by 1990) to the adult adopted individuals themselves.

The notion of privacy is a complex one in relation to adult adoptees' access to their own original birth certificates. Denying adult adoptees access preserves the **secrecy** of the birth parent's identity, but it also keeps information about the adoptee's own birth and identity secret. Beginning in the late 1960s and the 1970s, a movement to restore adult adoptees' access to their records has been led by a coalition of adoptees, birth parents, and adoptive parents. In response to this movement, a number of states have opened to adult adoptees birth records that were not closed at the time of their births, and have prospectively provided for such access in future adoptions. A number of other states also have opened original birth records that were closed at the time they were prepared. Mechanisms established in most of these states to protect birth parents' privacy consist of either "contact vetoes," which permit birth parents to choose whether they wish to be contacted by adoptees, or "**disclosure** vetoes," which permit birth parents to prohibit the release of identifying information. Many other states have considered but not enacted similar "open records" legislation. Opponents of the legislation argue that it violates promises of confidentiality and denies the privacy of birth parents. In legal challenges to the laws that have opened records, the courts have held that neither state law nor the U.S. Constitution guarantees lifelong **anonymity** for birth parents.

The 1930s were a key period in the history of adoption records. States then began providing for the issuance of new birth certificates in which the adoptive parents' names were substituted for the birth parents' names. Also during the 1930s and early 1940s, many states enacted laws to make adoption records confidential. Most of these laws restricted access to the parties to the proceedings. By the mid-1940s more than half the states reportedly protected adoption court records from public inspection. By 1955, according to legal commentators of the time, it had become commonplace and noncontroversial to make the records available only by court order, and to keep the original birth certificates available to adult adoptees but make them accessible to others only by court order.

Rapid changes in state laws continued, however, and by 1960 twenty-eight states reported to the federal government that they made original birth certificates available only by court order, although in a number of those states access to court records remained available to the parties of the proceedings. Twenty states reported making original birth certificates available on demand to adult adoptees. Of those states, four closed the birth records to adult adoptees as well as to the public in the 1960s, seven more did so in the 1970s, and another seven did so after 1979. Two states, Alaska and Kansas, never closed the original birth records to adult adoptees.

In the period from the 1930s through the 1960s, the reasons proffered for closing adoption records were, first, to protect adoptees and their families from public disclosure of the circumstances of the adoptee's birth and, second, in adoptions in which the adoptive parents and birth parents did not know one another, to protect adoptees and their adoptive families from interference or harassment by birth parents. Many commentators and courts later assumed that one important reason for closing the records was to permanently conceal the identities of birth parents; however, in the legal, social service, and other social science literature of the time there is virtually no discussion of the need to protect birth parents from adult adoptees who might seek information about their original families. On the contrary, leading legal and social service authorities in the 1940s and 1950s recommended that original birth certificates remain available to adult adoptees. This was the recommendation, for example, of the United States Children's Bureau, one of the most influential national voices in adoption law and practice; it was echoed by the American Association of Registration Executives and in the first Uniform Adoption Act, which was promoted in 1953 by the National Conference of Commissioners on Uniform State Laws. The surrender documents that many birth mothers signed required them to promise not to search out their children or their children's adoptive families, and in many cases the adoptive parents retained documents that contained the birth mother's name. With respect to counseling birth mothers, the most influential private child welfare organization, the Child Welfare League of America, advised adoption services providers to make it clear to birth mothers that they have no right to any information about the children they placed for adoption.

It is only possible to speculate as to why many states were closing birth records to adult adoptees when the stated reasons for doing so related only to protection of the adoptee and adoptive **family**, and when adoption services and adoption law experts were recommending keeping original birth certificates available to adult adoptees. The policy of closing records to adult adoptees appears to have been associated with changing ideas about adoption rather than with remedying any

problems that had arisen as a result of adult adoptee access. As records were closed generally to the public and then to the parties, and as adoption increasingly came to be seen as a perfect substitute for family formation via childbirth, it appears that lifelong secrecy came to be regarded as an essential feature of adoptions in which birth and adoptive parents are unknown to one another.

After World War II adoption became increasingly popular in an atmosphere that strongly encouraged the establishment of traditional families and in which nature—that is, genetic inheritance—was no longer viewed as more important than nurture—or environment—in the development of children. Psychological literature began to portray unmarried, expecting white women, at least, as having become pregnant because of emotional problems. If these women placed their children for adoption, they could avoid the powerful stigma attached to unwed motherhood, and could be helped to become stable wives and mothers later on. In the process, infertile couples would have an opportunity to form families. Adoption agencies increasingly engaged in “matching” practices, attempting to carefully match infants and adoptive parents on the basis of socioeconomic status and expected intellectual capacity, as well as physical characteristics. If adoptive families were truly to be no different from biological ones, then the sealing of records would make their legal documentary existence identical. Closed records, of course, would also shield adoption arrangements from later scrutiny, to the advantage of less-than-scrupulous adoption providers.

As lifelong secrecy became viewed as a desirable if not essential feature of adoption, adult adoptees who sought information about their birth families increasingly were seen as emotionally disturbed and ungrateful, and even as posing a threat to their birth parents. In opposition to such attitudes, and inspired in part by several books by adoptees—including social worker Jean Paton, adoptees’ rights advocate Florence Fisher, and psychologist Betty Jean Lifton—a nationwide advocacy movement developed in the 1960s and early 1970s seeking greater openness in adoption, including adult adoptee access to original birth certificates. In the following years, adoptees individually sought access to records, arguing in court, usually without success, that there was good cause for opening their records. Collectively, adoptees argued in court, again usually unsuccessfully, that they had a constitutional right to the information in their records. At the same time, studies were showing that most birth parents either were willing or wished to be contacted by the child or children they had relinquished. Other studies, professionals involved in adoption, and national professional organizations began characterizing adoptees’ interest in their birth families as a normal and natural part of adoption. By the end of the century, the movement for greater openness had led to the creation of hundreds of mutual support organizations and search services for adoptees and birth parents seeking information about or contact with one another.

In 1980 an advisory panel of the U.S. Children’s Bureau drafted a model state adoption act under which adult adoptees would have access to both original birth certificates and court records. After receiving negative comments on the draft, however, the Department of Health, Education, and Welfare ultimately promulgated a model law dealing only with the adoption of children with special needs. Instead of opening adoption records, many states began establishing passive or active mutual consent registries, or both, through which adoptees and birth relatives could

exchange information or make contact. In passive registries both parties must register and provide sufficiently detailed and accurate information to establish a match; success rates for those using these registries are very low. In active registry systems one party, most often the adult adoptee, can register and have an intermediary conduct a search for the birth parents.

Whether today's adult adoptees are successful in their search for information about birth relatives depends on factors such as the information the adoptive families already have in their possession; the luck, experience, and resources adoptees have in their search for birth relatives, often including the funds they have available for hiring private assistance; and the states in which they were born and adopted. In recent years, four states have opened to adult adoptees records that had been sealed when they were adopted, one state has agreed to open records to adult adoptees unless a birth parent has filed a disclosure veto, an additional number of states have opened records prospectively and have opened records that were not closed at the time the adoptions were made, and both Alaska and Kansas have continued to provide unrestricted access to original birth certificates by adult adoptees.

Tennessee was the first of the four states that in recent years have provided unrestricted access to adult adoptees. In 1995 Tennessee enacted legislation allowing adoptees who are at least 21 years old to access their original birth certificates as well as the court and agency records of their adoptions. Protection of the privacy of birth parents whose children were born after the date records were closed is provided by a contact veto system (and a disclosure veto option for living birth parents in cases of rape or incest). Birth parents and other specified birth relatives may register their willingness or unwillingness to have contact, and contact initiated in violation of a contact veto is both a misdemeanor and grounds for a civil suit. In 1998 Oregon citizens voted in a ballot initiative for a state constitutional amendment allowing adoptees 21 years of age and older to receive copies of their original birth certificates upon request. Birth parents may file contact preference forms on which they indicate whether they would like to be contacted and, if so, whether they would prefer to be contacted through an intermediary. Alabama, in 2000, and most recently New Hampshire, in 2004, also passed laws under which adult adoptees may receive copies of their original birth certificates upon request. In both of those states, birth parents may file contact preference forms to indicate whether they wish to be contacted directly, whether they wish to be contacted through an intermediary, or whether they would prefer not to be contacted but have an updated medical form available to the adoptee.

In Delaware, under a law that took effect in 1999, birth parents may file a disclosure veto blocking the release of identifying information. The veto must be periodically renewed. When an adult who was adopted before the law was enacted requests a copy of an original birth certificate, and there is no veto on file, the state attempts to notify the birth parents. Sixty-five days after the request, if no veto has been filed as a result of the state's efforts, a copy is provided to the adoptee. Similar options to the disclosure veto are available in the states that have opened records prospectively. These states include Colorado, Hawaii, Maryland, Montana, Nevada, Oklahoma, Washington, and Vermont. States that have re-opened some records that were not sealed when the adoptions took place include Ohio, Michigan, and Montana.

Both Tennessee's and Oregon's laws providing adult adoptees with access to records were challenged unsuccessfully in court. The parties challenging the Tennessee law—two unnamed birth mothers, an adoptive couple, and a child-placing agency—argued in federal court that the law violates the constitutional rights of birth mothers to familial privacy, to reproductive privacy, and to the nondisclosure of private information. The United States Court of Appeals for the Sixth Circuit in 1997 held, first, that the law does not interfere with any constitutional right to marry and bring up children or with any right individuals may have to either adopt or give up children for adoption. Second, the court held that the right to give up a child for adoption is not part of a constitutional right to reproductive privacy, and that even if it were, such a right would not be unduly burdened by the law. Finally, the court held that the Constitution does not include a general right to nondisclosure of private information.

The challengers then filed suit in state court, claiming that the law impairs the vested rights of birth parents who surrendered children under prior law, and also that it violates the right to privacy guaranteed by the Tennessee Constitution. In its 1999 decision, the Supreme Court of Tennessee noted that early adoption statutes had not sealed records, and that later amendments permitted disclosure to an adoptee if a court found that disclosure was in the adoptee's and the public's best interest. The court concluded, therefore, that there had never been "an absolute guarantee or even a reasonable expectation" that records were permanently sealed (*Doe v. Sundquist* 1999, 925). The court explained that when courts made determinations that records should be disclosed, there was no requirement that birth parents be notified. In addition, the court held that under the Tennessee Constitution, the law does not infringe on familial privacy rights related to marrying and having children, does not interfere with the right to procreational privacy, and does not implicate any right to nondisclosure of personal information.

Similarly, the Oregon law was challenged in the state courts. In a 1999 decision of the Oregon Court of Appeals, to which the Oregon Supreme Court denied review, the court's reasoning was similar to that of the Tennessee Supreme Court. According to the court, Oregon adoption laws had never "prevented all dissemination of information concerning the identities of birth mothers. At no time in Oregon's history have the adoption laws required the consent of, or even notice to, a birth mother on the opening of adoption records or sealed birth certificates" (*Does v. State* 1999, 832). The court further noted that under Oregon law, the decision to seal the original certificate was within the discretion not of birth parents but of the adoptive parents, the adoptee, or the court granting the adoption. The court concluded that earlier state law had not indicated any intent to enter into a statutory contract with birth mothers to prevent disclosure of their identities and, therefore, the new law does not impair obligations of contract in violation of the Oregon Constitution. If employees of private entities or even state agents misrepresent state law, the court said, they cannot bind the state to arrangements in contravention of state law.

Rejecting the challengers' additional claims that the law violates state and federal constitutional rights to privacy, the Oregon court noted that adoption had been unknown at common law, that early adoption statutes had no provisions for protecting the identity of birth mothers, and that there is neither a fundamental right to

place a child for adoption nor a correlative right to place a child for adoption under circumstances that guarantee her anonymity. Unlike a unilateral decision to prevent pregnancy or not to carry a pregnancy to term, placing a child for adoption “requires, at a minimum, a willing birth mother, a willing adoptive parent, and the active oversight and approval of the state” (see *Does v. State* 1999, 836).

See also: **Health privacy; Reproductive rights**

Suggested Reading: Cahn, Naomi R., and Joan Heifetz Hollinger. *Families by Law: An Adoption Reader*. New York: New York University Press, 2004; Cahn, Naomi R., and Jana Singer. “Adoption, Identity, and the Constitution: The Case for Opening Closed Records,” *University of Pennsylvania Journal of Constitutional Law* 2 (1999): 150–194; Carp, Wayne C. *Adoption Politics: Bastard Nation and Ballot Initiative* 58. Lawrence: University Press of Kansas, 2004; Carp, Wayne C. *Family Matters: Secrecy and Disclosure in the History of Adoption*. Cambridge, MA: Harvard University Press, 1998; Samuels, Elizabeth J. “The Idea of Adoption: An Inquiry into the History of Adult Adoptee Access to Birth Records,” *Rutgers Law Review* 53 (2001): 367–437; Wegar, Katarina. *Adoption, Identity, and Kinship: The Debate over Sealed Birth Records*. New Haven, CT: Yale University Press, 1997.

Elizabeth J. Samuels

Airborne surveillance and intelligence

A technique employed principally by large state or corporate actors, the collection by airborne devices of electromagnetic (EM) signals and emissions from the earth’s surface or atmosphere has existed for over 140 years. Insofar as privacy can be equated with the ability to conceal or control one’s communications and information about oneself, the relevance of airborne surveillance and intelligence to issues of privacy is twofold. First, in many ways, EM emissions are regarded as passing through public space, and so the information they contain is generally considered outside the realm of privacy. Technological innovation and industry commercialization, however, have complicated this situation through their expansion of the detail, scope, and applications of airborne **surveillance**. Second, *privacy* and *security* are typically regarded as being in opposition, such that trade-offs are depicted as necessary to achieve a balance between the conflicting interests of state security and individual privacy. Telephones may be **wiretapped**, for example, if law enforcement officers suspect they might be used in planning terrorist activities. In contrast, airborne surveillance marks a circumstance wherein security is made *analogous* to privacy: the ability of states and organizations to conceal and control their communications or information about themselves can be significantly eroded through airborne surveillance.

Airborne platforms offer a number of surveillance advantages, including an unobstructed, panoramic view of the earth’s surface (even of hostile or difficult-to-reach regions), better atmospheric clarity, reduced EM noise, and the relative safety and inconspicuousness afforded by high altitude. Most recently, unmanned aerial vehicles (UAVs) have offered the possibility of robotic or remote control, thereby placing no humans at risk. As early as the end of the eighteenth century, the French employed observers in balloons to help direct artillery fire against distant enemies. Beginning hardly more than a decade after the development of the daguerreotype in

1839, and continuing through the present, groups have collected photographs (both secretly and overtly) from balloons, dirigibles, kites, aircraft, rockets, and most recently, orbital satellites. This activity—usually referred to as remote sensing—has been highly refined since first proposed for survey applications in the 1850s; today it is a highly specialized technical discipline and a growing commercial enterprise.

The advent of radio communication in the early 1900s opened up the possibility of broadcast signal interception, and today informative electromagnetic signals of many types are readily intercepted by airborne platforms, a technical practice referred to as signals intelligence, or SIGINT. Not only communications signals, but emissions associated with aircraft and ship operations, weapons control radars, and nuclear detonations are routinely monitored. Principally a tool of government intelligence organizations, SIGINT powerfully shaped international relations in the twentieth century (as did remote sensing), and its use marks a regime in which issues of “privacy” arise primarily in the guise of “state security.”

Airborne surveillance systems are divided into two broad categories, *active* and *passive*. Active systems rely on the “illumination” of a subject or “target” by a transmitting source—a laser or radar beam, for example—and the reception of the reflected portion of that source’s transmissions. Examples of this type include the U.S. military’s AWACS aircraft and the Canadian RadarSAT satellite. Passive systems (which include the majority of airborne surveillance systems) depend either on emissions from the subject itself—the infrared emissions from human bodies, for example, or signals from a radio device such as a **cellular telephone**—or on “natural” illumination (i.e., the sun, moon, or EM radiation from the target’s surroundings). In some instances, particularly in the realm of international policy, airborne surveillance may be restricted on the basis of whether it is done actively or passively, since active transmissions are effectively treated as an intrusion, while passive emissions are considered in the public domain. This understanding is not unequivocal, however. U.S. courts have typically held that emissions that escape from within private buildings and residences—excessive thermal emissions associated with the cultivation of illegal crops, for example—are private property, and their interception without a warrant (even from outside the building) can constitute illegal search and seizure.

A number of developments in airborne remote sensing have brought its privacy implications to the fore in recent years. First, innovations in electronics and electro-optics have improved system resolution (the ability to resolve detail and distinguish fine differences in color or brightness), shortened processing time, and extended system coverage around the clock and around the globe. These improvements have enabled a broad variety of previously infeasible applications, both military and civil. Aside from surveilling or planning the movements of troops and equipment, remote sensing has been successfully employed in the monitoring of refugee flows, weapons proliferation, famine, genocide, and other humanitarian disasters, as well as in the support of law enforcement, mapping and surveying, **journalism**, environmental health assessment, verification of environmental treaty compliance, forest fire control, detection of toxic releases, inventory of natural resources, natural disaster mitigation, urban planning and development, resource prospecting, and scientific research. This proliferation of civil applications has increased pressure on

state governments to privatize the industry and has fostered a growing commerce in airborne and satellite imagery.

In another parallel with information technologies (IT) generally, the exchange of aerial image data has intensified, thanks largely to the growth of digital technologies and the Internet. While a far sight from the Orwellian scenario in which anyone who can afford it can continuously monitor the daily movement and activities of specific individuals, the online stores of several commercial imagery providers have hawked aerial images “of one’s own house” since the beginning of the twenty-first century. As outlined in President Truman’s 1955 “Open Skies” doctrine (intended to promote “mutual transparency” between the United States and the Soviet Union), legal distinctions between the “airspace” over a nation as sovereign territory and “low earth orbit” as an international commons not unlike the open ocean has placed satellite-borne surveillance systems on a unique regulatory landscape. It is by virtue of international policies built on that doctrine that the TIROS weather satellites, the Landsat system for earth observation, and today’s commercial high-resolution satellites (IKONOS and Quickbird, for example) have been able to provide increasingly detailed imagery irrespective of which nation controls the imaged terrain. The shifts fostered by airborne surveillance—the shift toward transparency and disclosure as political objectives, the shift toward an open market for aerial images and other data—are noteworthy less because of the challenges they imply for *individual* privacy than because of the analogous challenges they raise for *state and corporate* privacy.

See also: **Electronic surveillance; Thermal sensors; *United States v. Kyllo*, 533 U.S. 27 (2001)**

Suggested Reading: Baker, John C., Keven M. O’Connell, and, Ray A. Williamson. *Commercial Observation Satellites: At the Leading Edge of Global Transparency*. Santa Monica, CA: RAND, 2001; Federation of American Scientists. *Intelligence Resource Program*. <http://www.fas.org/irp>. Online, March 2006; Lindgren, David T. *Trust but Verify: Imagery Analysis in the Cold War*. Annapolis, MD: Naval Institute Press, 2000; Monmonier, Mark. *Spying with Maps: Surveillance Technology and the Future of Privacy*. Chicago: University of Chicago Press, 2002; Pike, John. *Global Security*, <http://www.globalsecurity.org>. Online, March 2006; Streetly, Martin. *Jane’s Electronic Mission Aircraft Systems*. Surrey, UK: Jane’s Information Group, 1997.

Lane Denicola

Air travel

Air travel privacy has underpinnings in several constitutional protections and various court decisions, including those related to freedom of association, interstate travel, and the right to be secure from unreasonable search and seizure. In the heavily regulated air transportation industry, however, increased security measures have limited passengers’ expectations of privacy in airports and on airplanes. Furthermore, while aviation security has traditionally focused on the physical screening of people and baggage, passengers’ personal information is increasingly a focal point for security measures.

Before the 1960s, security measures for domestic air travel were relatively cursory. After several hijackings around the world in the late 1960s and early 1970s, however, the Federal Aviation Administration required that all passengers and

luggage must be searched prior to flight. Airports began using magnetometers, or metal detectors, to physically screen passengers for concealed metal weapons. When the constitutionality of magnetometer searches was challenged, numerous courts determined that the government's interest in requiring such searches justified the invasion of passengers' privacy.

The United States government began using "watch lists" to prescreen passengers in the early 1990s. These lists contain information about people known or thought to pose a risk to aviation security. An individual whose name appears on the "no fly" list is not permitted to board an airplane. People on the "selectee" list must undergo additional screening before they are permitted to fly. Some people with names similar to those on watch lists have experienced delays and extensive screening during air travel.

Since the terrorist attacks of September 11, 2001, the United States and other countries have worked to establish new and effective forms of aviation security. The Transportation Security Administration (TSA), an agency within the Department of Homeland Security, is specifically tasked with assessing threats to domestic air transportation. Since 9/11, the agency has instituted numerous aviation security measures, such as requiring passengers to show photo identification to board an airplane. The United States has also begun developing methods of advanced passenger prescreening. Shortly after the terrorist attacks, the TSA proposed the creation of a comprehensive prescreening system that would use passengers' personal information to verify their identities and to make threat assessments. The proposal was abandoned in 2004 because of privacy and other concerns, and the agency began developing a second prescreening system that would rely heavily on government watch lists.

The government and private sector are also exploring the utility of a "trusted traveler" system, in which travelers would volunteer personal information and **biometric identifiers** such as **fingerprints** and iris scans. The government would compare these data to information maintained in public and private databases to assess each passenger's risk level. If cleared, the passenger would be permitted to go through shorter lines at airport security checkpoints and possibly be subject to less intense physical screening.

See also: **Computer-Assisted Passenger Prescreening System (CAPPS II) and Secure Flight; Constitutional protections**

Suggested Reading: Etzioni, Amitai. *How Patriotic Is the Patriot Act? Freedom versus Security in the Age of Terrorism*. New York: Routledge, 2004; Flaherty, David H. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill: University of North Carolina Press, 1992; Goldberg, Carole. *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security*. New York: W. W. Norton, 2002; Regan, Priscilla. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press, 1995; Transportation Security Administration. <http://www.tsa.gov>. Online, March 2006.

Marcia Hofmann

American Civil Liberties Union (ACLU)

The American Civil Liberties Union (ACLU) is a nonprofit, nonpartisan organization that works to protect and uphold the United States' Bill of Rights. Traditionally,

the organization has focused primarily on guaranteeing individuals' rights to free expression, equal protection under the law, due process, and privacy.

The ACLU was officially formed in 1920 by a group of social activists that included Roger Baldwin, Crystal Eastman, and Albert DeSilver. The organization grew out of the movement to protect conscientious objection and free speech during World War I. Since then, the ACLU has held a consistent, prominent position in the discussion of constitutional rights and their relation to contemporary issues. Throughout its history, the organization has taken strong public stances on a variety of civil liberty issues, including those related to school prayer, obscene materials, abortion, drug decriminalization, public demonstration, and privacy invasion.

After extensive growth during the opening years of this century, the ACLU now claims more than 400,000 members in state and local chapters nationwide. It is headquartered in New York City, with a sizable national legislative office in Washington, D.C. However, most of the organization's work is conducted by its state and local affiliates, of which there are over 50. Annual dues and contributions from members provide the ACLU's primary financial support, although it also receives some grants from private foundations and individuals. The ACLU does not receive government funding. Additionally, the organization is politically unaligned; it does not officially support or oppose political candidates or ideologies. It operates under the belief that everyone's rights are threatened if one person's rights are not protected. As a result of maintaining this absolutist approach to civil liberties, the organization has drawn criticism for defending such controversial groups as Nazis, Communists, and the Ku Klux Klan.

In its work to protect civil liberties, the ACLU pursues a variety of initiatives, including community-based activism and legislative lobbying. Still, its most prominent and effective efforts have been in the nation's courts, as the organization regularly takes on cases in which civil liberties are possibly threatened. The organization handles close to 6000 such court cases each year, and it appears before the United States Supreme Court more than any other group outside of the federal government. In those civil liberty cases where it is not directly involved, the ACLU also frequently submits amicus curiae briefs in support of its position. The ACLU has at times referred to itself as "the nation's largest law firm," a claim that is supported by the organization's national network of local offices and its corps of nearly 5000 affiliated attorneys.

These extensive legal resources have been key to the organization's development and to its success in the courtroom. With them, the ACLU has influenced a variety of notable court decisions. For instance, the organization provided defense counsel in such landmark cases as *Stromberg v. California* (symbolic speech), *Engel v. Vitale* (school prayer), *Brandenburg v. Ohio* (inflammatory speech), *Tinker v. Des Moines Independent Community School District* (student rights), *Edwards v. Aguillard* (science education), and *Cruzan v. Director of the Missouri Department of Health* (right to die). The ACLU also provided amicus curiae briefs in key decisions including *Hirabayashi v. United States* (wartime internment), *Brown v. Board of Education* (school segregation), *Gideon v. Wainwright* (right to counsel), and *Miranda v. Arizona* (police interrogation).

The ACLU has also been active in the movement to preserve and protect individual privacy. As might be expected, their most notable effects in this area have

been recorded in a number of Supreme Court decisions. Perhaps most notably, the ACLU represented the defendant the 1965 *Griswold v. Connecticut* decision that struck down a state ban on contraceptive use. In the decision, the Court cited “marital privacy” and acknowledged that although not clearly stated in the Constitution, privacy was protected by “several fundamental constitutional guarantees.” Additional cases related to reproductive rights, including *United States vs. Vuitch* (1971), *Eisenstadt v. Baird* (1971), *Planned Parenthood v. Casey* (1992), and *Stenberg v. Carhart* (2000), further defined this position. The ACLU has successfully protected privacy rights in other contexts as well. For instance, *Chandler v. Miller* (1997) cited the Fourth Amendment in invalidating a Georgia state statute that required political candidates to submit to **urine** tests.

Taken together, these decisions have helped further define and clarify privacy rights under the law. However, privacy remains a primary focus of the ACLU. In the early years of this century, the ACLU has become increasingly concerned with the growth of a “**surveillance** society” in which corporate and governmental organizations pose new threats to personal information and privacy. The organization’s “Technology and Liberty Project,” for instance, currently focuses on a myriad of privacy issues. As part of this project, the ACLU has challenged the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)**, **Internet** censorship, and breaches of online **anonymity**.

See also: **Constitutional protections; Privacy advocacy organizations**

Suggested Reading: Walker, Samuel. *In Defense of American Liberties: A History of the ACLU*. Carbondale: Southern Illinois University Press, 1990.

Steve Munch

Anonymity

Historically, the concept of anonymity was associated with a state of namelessness. Being an *anonym* afforded certain advantages. It enabled the nameless to speak without fear of reprisal, or to engage in acts of charity or other forms of benevolence. At the same time, it made possible wrongdoing without accountability.

With the advent of **computer**-based communications networks, there has been a resurgence of interest in the nature and value of certain types of anonymity. The range of techniques by which individuals are able to operate incognito creates a virtual laboratory for experimenting with the social construction of identity. However, as the Internet’s surveillance potential becomes better understood and exploited, the measure of anonymity shifts from its historical focus on names to a broader investigation of a range of personal identifiers that can be linked to an individual. These include date of birth, marital status, **Social Security number**, passport information, property ownership, vehicle registration, driver’s license number, facial characteristics, height, **e-mail** address, place of business, phone number, **credit card** history, iris shape, **fingerprints**, retinal image, employment record, blood chemistry, roadway usage, gait pattern, consumer purchases, Internet search history, Internet protocol address, and other identifiers. Unbeknownst to many, the increasing ability to link these identifiers to an individual has resulted in a diminished ability to maintain anonymity, resulting in applications for subpoenas and court orders requiring third parties to disclose identifying information for the

purposes of private lawsuits or police investigation. In light of the numerous possible identifiers in an information age, anonymity is perhaps best understood as a state of disconnection between one's self and one's identifiers; a state in which data cannot be associated with a particular individual, either from the data itself, or by combining it with other data. The value of anonymity, as philosopher Helen Nissenbaum observes, lies not in the capacity to be unnamed, but in the possibility of acting or participating while remaining unreachable.

Anonymity's characteristic of "unreachability" provides one means of achieving what legal scholar Alan Westin has defined as self-directed informational privacy: people who are able to disconnect their identities from their actions are better able to determine for themselves when, how, and to what extent information about them is communicated to others. Although it does not offer seclusion in the usual spatial sense, being anonymous affords a kind of isolation. Whereas credit card payments create traceable transactions, allowing a consumer's activities to be tracked and a data profile to be created, anonymous payments preserve privacy.

Historically, the value of anonymity has had less to do with its privacy-enhancing potential than its political purpose. Anonymity has always been a crucial thread in the fabric of democracy. Anonymous voting ensured that citizens were free actors, that their political participation would remain uninfluenced by the tyranny of the majority or by undue pressure from other powerful groups. The *Federalist Papers*, a series of newspaper articles that became a bedrock of U.S. constitutional thought, although not truly anonymous, were written pseudonymously, using a fabricated name to cloak the identities of their authors while still allowing a mediated form of attribution. The same strategy was later employed by nineteenth-century female novelists to prevent **gender** discrimination from influencing how their work was received.

Now, as then, anonymity enables people to discuss taboo subjects with others. Whether face-to-face in a self-help group, or peer-to-peer in an online chat, sexual abuse, addiction, and disease are regularly confronted and sometimes overcome anonymously. For many persons, the mere assurance of anonymity is what emboldens them to participate in the first place. Alternatively, anonymity also enables unlawful associations and antisocial behavior, causing one U.S. Supreme Court justice to refer to anonymity as the "refuge of scoundrels."

Because anonymity can yield good or bad outcomes, some perceive a conflict regarding its value and role in democratic societies. In the United States, political anonymity is a constitutional entitlement flowing from the right to freedom of expression and **freedom of association**. But the right to anonymous communication is not immutable; it must be balanced against state interests in protecting people's reputations, in fighting fraud and crime, and in safeguarding national security. Whereas few would disagree that anonymous voting is desirable and anonymous criminal activity is undesirable, between these extremes lies a sea of uncertainty.

As the Internet continues to evolve, anonymity's future abounds with question marks. The information trade has turned "dataveillance" into big business. Cyber-crime legislation and the expanding ability of law enforcement agencies to collect personal information and intercept electronic communications has been proposed or enacted in many jurisdictions, and the demands for identification for everything from **air travel** to building entry are on the rise. At the same time, blogs, chat

rooms, instant messaging and a number of other online environments provide exciting new venues for social and political participation that permit and even encourage individuals to conceal their actual identities. Millions of people using them have made clear their desire to withhold disclosure of their identities for a variety of legitimate social purposes, inspiring a number of **cryptographers** to develop systems of provable anonymity. The extent to which such applications will be permitted or adopted by governments or markets in the twenty-first century remains uncertain. Their potential uses and broader questions concerning the importance and impact of anonymity in a networked society are under investigation by a growing number of academics and privacy advocates.

See also: **Authentication; Confidentiality; Personally identifiable information**

Suggested Reading: Clarke, Roger. *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>. Online, December 2005; Marx, Gary T. "What's in a Name? Some Reflections on the Sociology of Anonymity," *Information Society* 15 (1999): 99–112; Nissenbaum, Helen. "The Meaning of Anonymity in an Information Age." *Information Society* 15 (1999): 141–144; *On the Identity Trail*. www.anonequity.org. Online, December 2005.

Ian R. Kerr

Anti-wiretap statutes

In its narrowest sense, **wiretapping** refers to interception of telephonic voice communications. This method of eavesdropping has been around for as long as the telephone itself and has always been strictly regulated. As communications methods became more sophisticated, wiretapping methods followed suit, and laws regulating wiretapping had to be updated to cover **cellular phones** and electronic communications such as e-mail, fax transmissions, and digital-display pagers. Anti-wiretapping laws can be split into two categories: first, laws that prevent private citizens from intercepting another's telecommunications; and second, laws that restrict law enforcement officials from doing the same.

The first category of laws is relatively straightforward: under federal law, it is illegal for any third party to intercept any telephonic or electronic communication between other individuals. However, if one of the parties to the conversation records or consents to the recording of the conversation, the interception of the communication is generally not barred under federal law, as long as the communication is not being intercepted for the purpose of committing a criminal or tortious act. This practice is also permissible under many state laws, but at least 11 states prohibit recording a conversation even if one of the parties consents to the recording.

Laws regulating law enforcement wiretaps are a bit more complicated and more controversial. By far the most important federal statute is Title III of the Omnibus Crime and Control Act of 1968. This law states that an order authorizing law enforcement wiretaps (known as a "Title III order") will be issued only if the government can demonstrate (1) probable cause to believe that the interception will reveal evidence of one of a limited list of predicate crimes, with the suspected crime named in the application; (2) probable cause that the communication facility is being used in committing the crime; (3) normal investigative procedures have been tried and failed, are unlikely to succeed, or are dangerous; and (4) the surveillance will be

conducted in a way that minimizes the interception of irrelevant communications. Every Title III request must be authorized by a United States Attorney. This is a relatively high burden on law enforcement: in order to obtain a standard **search warrant**, the government need only show probable cause that a crime has occurred. Law enforcement officials are routinely able to meet this burden, however; in 2004, for example, no state or federal judge denied a law enforcement request for wiretap authorization (Administrative Office of the United States Courts, 2004).

Title III has undergone two significant amendments since its passage. In 1986, Title III was amended by the **Electronic Communication Privacy Act (ECPA)**, which extended the Title III restrictions to digital and electronic telecommunication. The **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)** eased some restrictions on wiretapping. For example, the PATRIOT Act allows law enforcement agents to apply for “roving wiretaps,” which permit agents to trace calls not just in the jurisdiction in which the authorization was ordered but anywhere in the United States. It also extended the “pen/trap” rule from telephonic to electronic communications. During 2004, there were 1710 intercepts conducted in the United States, an increase of 19 percent over the previous year. The vast majority of these intercepts (76 percent) were pursuant to drug investigations.

Other forms of wiretapping are less invasive because they do not involve intercepting the substance of the communication; thus, they are not as strictly regulated by law. For example, Title III restrictions apply only to intercepting the *content* of the message, and do not apply to intercepting the incoming or outgoing *address* of the communication. In the context of telephonic communications, this is commonly known as “tracing” the origin or destination of a call; law enforcement agents use a pen/trap device to determine the number a call is going to or the number that a call came from. In the context of electronic communications, such as e-mail, this might involve intercepting the “To” and “From” line of the message, rather than the entire message. In other words, for telephonic intercepts, a different device is used to trace a call, whereas for electronic communications, the same method is used to intercept the addresses and to intercept the communication, but the law enforcement agent only looks at the address lines.

Despite this difference, the legal standard for intercepting “addressing” information is the same irrespective of the type of communication that is intercepted. In order to receive authorization to intercept this information, the government must show that “the information likely to be obtained is relevant to an ongoing investigation.” This is a far lower standard than is required under Title III, and even lower than is required for a traditional search under the Fourth Amendment. (The Supreme Court has held that the Fourth Amendment does not apply to a wiretap that only intercepts addressing information.) Furthermore, if law enforcement officers fail to follow these requirements, the evidence can still be used against the suspect at trial, although the officers could be subject to criminal and civil liability if a court determines that the law enforcement officials did not act in good faith.

There are also separate rules for so-called stored communications: e-mails or voice mails that are stored on a remote server. As with using phone traces and intercepting e-mail addresses, recovering stored communications from third parties is not considered a “search” under the Fourth Amendment, so there are no

constitutional restrictions on such surveillance. However, federal law creates different legal standards based on the type of communication being sought; for example, a warrant is generally required to recover unopened e-mail, while a subpoena with notice to the party is sufficient to recover opened e-mail or subscriber information.

Finally, there is the question of audio and video surveillance—the practice of installing a hidden microphone or camera in a home or office and recording suspects’ words and/or actions. Technically, these forms of surveillance are not wiretapping, because they do not involve intercepting electronic signals sent over the telecommunications network. They are, however, strictly regulated by the federal government; in fact, they are governed by the same strict standards as wiretapping. Audio surveillance (commonly known as “bugging”) is expressly covered by Title III, and although video surveillance is not, courts have held that the Fourth Amendment places the same high restrictions on video surveillance as Title III places on wiretapping.

See also: Electronic surveillance; Federal Bureau of Investigation; Katz v. United States, 389 US 347 (1967)

Suggested Reading: Administrative Office of the United States Courts. 2004 *Wiretap Report*. U.S. Courts, <http://www.uscourts.gov/wiretap04/contents.html>. Online, March 2006; Alberti, Anthony. *Wiretaps*. Bethesda, MD: Austin & Winfield, 2002; Diffie, Whitfield, and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press, 1999; Regan, Priscilla M. *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill: University of North Carolina Press, 1995; Reporters Committee for Freedom of the Press. *A Practical Guide to Taping Phone Calls and In-Person Conversations in the 50 States and D.C.* <http://www.rcfp.org/taping>. Online, March 2006; Wingfield, John. *Bugging: A Complete Survey of Electronic Surveillance Today*. London: R. Hale, 1984.

Ric Simmons

Assisted reproductive technologies

Assisted reproductive technologies (ART) are medical interventions that help single people and infertile couples have children by increasing the likelihood of conceiving naturally or by creating embryos *ex utero* (outside the womb) for implantation into the mother or surrogate. Examples of ART include fertility drug treatment, artificial insemination, in vitro fertilization (IVF), and intracytoplasmic sperm injections (ICSI). ART may also involve prenatal testing and preimplantation genetic diagnosis (PIG) to help parents select embryos that are free of inherited diseases. Gametes (sperm or eggs) or embryos may be frozen and stored for later use in ART; therefore, the disposition of excess gametes or embryos may also impact privacy considerations.

In 1890 Justice **Louis D. Brandeis** described privacy as “the right to be let alone.” This definition is pertinent to ART since parents often want to be left alone by sperm and egg donors, separated couples might want surplus embryos to be left alone rather than implanted, and sperm and egg donors want to protect their **anonymity**. The First, Fourth, and Fifth Amendments to the Constitution as well as case law have established that issues related to reproduction, sexuality, and **family** are private, and that government should limit its intrusions in these areas. However,

the New York State Task Force on Life and the Law noted that, while ART as employed by married couples with their own gametes will likely be protected under the federal Constitution, noncoital reproduction including surrogacy and reproductive cloning may not be. Nonetheless, the **Privacy Act of 1974** and the **Health Information Portability and Accountability Act (HIPAA)** of 1996 mandate the **confidentiality** of private, **personally identifiable information**.

Various parties may be involved in ART, each with privacy rights and each with expectations that information about identity and health will remain confidential. First, there are the individuals and couples who wish to become parents. Through ART, they may become biological parents or they may parent children who are not genetically related. Second, there are sperm and egg donors, some of whom are known to prospective parents and some of whom are anonymous. Third, there are surrogate mothers. Fourth, there are the children born using ART.

Gamete donation is either directed, in which case the donor knows the recipient, or anonymous, in which case the donor does not. In both cases, the parents seeking donor assistance with ART may stipulate that they or their children be left alone. For example, a co-worker or friend might volunteer to donate sperm with the understanding that his identity should remain private unless the parents later want to reveal it. Similarly, parents may not want the circumstances of conception revealed to other family members or to the child for fear the child will reject the nongenetic parent(s).

Many egg and sperm donors prefer to remain anonymous. They want to help infertile couples but do not yet want to become parents; therefore, their identities are withheld from prospective parents as well as from any biological offspring. When sperm and egg donors choose to remain anonymous, certain private information, such as health status and some **genetic information**, is disclosed so that prospective parents can make an informed choice about conception, but the donor's identity is not disclosed. Still, some children want to learn the identity of their biological parent(s). In addition to personal reasons, there may be compelling medical reasons to seek out a donor, such as the need for a biological relative's bone marrow. Several countries have laws or policies that support a child's access to donor information or identity, including Switzerland, Austria, the Netherlands, Sweden, and the United Kingdom (Ethics Committee 2004, 528). A bill in Canada's parliament would allow 18-year-old children to access nonidentifiable health information, and a donor may authorize release of his or her identity to children. In order to protect the privacy of anonymous donors, sperm banks and fertility clinics should discuss these policies with donors prior to donation because identifying an anonymous donor for any reason jeopardizes the donor's privacy.

Children born using ART also have the right to be left alone by sperm or egg donors. Normally it is up to the parents to decide whether or not to disclose the circumstances of their conception, including the identity of known donors. Also, as preconception and preimplantation genetic testing become available, parents who select for certain genetic characteristics or select against for nonlethal diseases may face later objections from their children, either that the testing itself revealed information that the adult child would reasonably want to remain private (such as carrier status for cystic fibrosis) or that the testing itself is a violation of "fetal privacy."

When, if ever, can the anonymous donor's right to privacy be overridden? When the donor, parents, and child all consent, then disclosure by sperm bank or fertility clinic is permitted. Many sperm banks test donors for HIV infection, which means that some sensitive health information that might have been unknown to the donor is revealed in the process of sperm donation and shared with prospective parents. It is ethically justified to test all gamete donors for HIV and other sexually transmitted diseases to protect the offspring and the women who will become pregnant using donated gametes. The identity of an HIV-infected potential donor normally remains confidential, but the safety and health of women and newborns may legitimately override some privacy concerns. Discrimination and stigmatization are likely to ensue if the patient's identity is revealed, however, so the patient's name should only be revealed to a limited number of authorized individuals and only for compelling patient safety and public health reasons. HIV testing is recommended, not mandated, for all couples who wish to have biological children. It is not mandated in part because such a mandate could not be enforced except in the context of ART, which could be seen as discrimination against infertile people.

Issues of privacy are compounded when HIV-positive individuals want to become biological parents. Ethically, the risk of transmission must be balanced against the desire to be biological parents. ART may be employed to decrease the risk of transmission. Following education and counseling, HIV-discordant couples may be able to use intracytoplasmic sperm injections, where one sperm without the virus is injected into a harvested egg and IVF is employed. HIV-positive pregnant women and their newborns can also be treated with antiretroviral drugs to decrease transmission.

There are special privacy issues that arise with deceased sperm donors. The main question is who may use extracted and frozen sperm for the purpose of reproduction. Some argue that without the deceased man's prior consent, postmortem "reproduction" should be prohibited. Others believe that surviving family members, particularly spouses, have proprietary right to use sperm for procreation without previous consent from the deceased donor.

ART raises the question of who is the legally and ethically responsible parent in disputes concerning frozen embryos and donated gametes. One legal scholar writes that "if courts resolve frozen preembryo disputes that involve non-gamete providers based on the constitutional right to privacy, then they should find that the constitutional right to privacy encompasses the interests of both gamete and non-gamete providers. Individuals who create preembryos with the intent to become a parent have made an intimate decision involving procreation, marriage, and family life that falls squarely within the right to privacy" (Dillon 2003, 625). Normally, privacy rights protect citizens from intrusion into family affairs, but intrafamilial disputes may raise questions about custody. In the case of *In re Buzzanca*, a California appeals court determined that a divorced couple whose child was conceived using anonymous sperm and egg donation and a surrogate mother were the legal parents, reasoning that it was their intention to become parents—not their biological relationship to the child—that was legally important. *Kass v. Kass* involved a woman who, in the course of divorce proceedings, sought sole custody of five frozen preembryos created through the couple's IVF treatment. The New York Court of Appeals ruled that the preembryos did not implicate "a woman's right to privacy

or bodily integrity before implantation”; therefore, the contract signed by Mr. and Mrs. Kass prior to cryopreservation was binding. It stipulated that unused preembryos should be donated for research. These disputes raise complicated issues about who constitutes family: biological or “intentional” parents or both?

Protecting the privacy of those involved in ART helps to prevent discrimination and stigmatization and upholds constitutional privacy protections; however, an individual’s right to privacy may be overridden, especially in cases where divorced or separated families must discern who has custody when biological and nonbiological parents are involved.

See also: **Abortion; Adoption; Birth certificate; Health privacy; Patient’s rights; Reproductive rights**

Suggested Reading: Botkin, J. R. “Fetal Privacy and Confidentiality,” *Hastings Center Report* 25 (1995): 32–39; Coleman, Carl H. “Assisted Reproductive Technologies and the Constitution,” *Fordham Urban Law Journal* 30 (2002): 57–70; Davis, David S. “Discovery of Children’s Carrier Status for Recessive Genetic Diseases: Some Ethical Issues,” *Genetic Testing* 2 (1998): 323–327; Dillon, L. M. “Conundrums with Penumbra: The Right to Privacy Encompasses Non-Gamete Providers Who Create Preembryos with the Intent to Become Parents,” *Washington Law Review* 78 (2003): 625–651; Ethics Committee of the American Society for Reproductive Medicine. “Human Immunodeficiency Virus and Infertility Treatment,” *Fertility and Sterility* 77 (2002): 218–222; Ethics Committee of the American Society for Reproductive Medicine. “Informing Offspring of Their Conception by Gamete Donation,” *Fertility and Sterility* 81 (2004): 527–531; Foster, Jennifer, and Barbara Slater. “Privacy and Assisted Human Reproduction: A Discussion Paper,” *Health Law Review* 11 (2002): 56–61.

Denise M. Dudzinski

***Associated Press v. Walker*, 388 U.S. 130 (1967)**

Associated Press v. Walker, 389 U.S. 28 (1967) and *Curtis Publishing Company v. Butts*, 388 U.S. 130 (1967) were consolidated and decided in one opinion issued by the United States Supreme Court in 1967. Although the language of the majority opinion suggests otherwise, the Court later confirmed that this decision made public figures essentially the same as public officials within the meaning of the First Amendment in relation to an action against libel. In other words, the First Amendment (and the Fourteenth Amendment as applied to the states) prohibits either public officials or public figures from recovering damages for libel unless they prove actual malice or reckless disregard for the truth. In *Walker/Butts*, the Supreme Court established a guideline to determine the presence of actual malice or reckless disregard for the truth.

Libel law had earlier substantially changed paths when the Supreme Court issued its decision in *New York Times v. Sullivan* (1964). That landmark decision established that the First Amendment (and the Fourteenth Amendment as applied to the states) prohibited a public official from recovering damages for a defamatory falsehood relating to the official’s conduct in his or her official capacity. The Court carved out one qualification by which a defamatory falsehood could lead to damages: actual malice, or reckless disregard for the truth. The definition given for actual malice was with knowledge that the statement was false or with reckless disregard of whether it was false.

With this decision as a base, the Court issued its opinion in *Walker/Butts*. The Court first addressed the factual background of *Butts*. In that case, the *Saturday Evening Post* published an article about Wallace Butts, who at the time of publication was the athletic director at the University of Georgia. The article alleged that Butts aided in a conspiracy to “fix” a college football game between the University of Georgia and the University of Alabama that had been played in 1962. Before serving as athletic director, Butts had served as a football coach; at the time of publication of the article, he was negotiating a contract with a professional football team. In short, he was a well-known public figure. The article was undeniably aimed at harming Butts, and he sued for an enormous sum in compensatory and punitive damages.

In *Walker*, the facts were different. That suit arose out of the circulation of a news report giving an eyewitness account of a riot on the campus of the University of Mississippi in 1962. The report declared that Walker, a retired military leader, incited and led the violent crowd against federal marshals sent there to contain the riot. It also suggested that Walker encouraged the use of violence and informed the protesters how to buffer the effects of tear gas. Like Butts, Walker sued for an enormous sum in compensatory and punitive damages.

Beginning its analysis of the constitutional arguments before it, the Court initially noted that the media is comprised of businesses that seek to turn a profit: “Like other enterprises that inflict damage in the course of performing a service highly useful to the public . . . they must pay the freight; and injured persons should not be relegated [to remedies that] make collection of their claims difficult or impossible unless strong policy considerations demand.” Thus, the Court had to strike a balance between preserving a strong and open media, and protecting the sanctity of individuals’ reputations and integrity in the face of untruthful and defamatory statements. The Court pointed out that the First Amendment protections are not without limit; this is confirmed by the validity of statutes on federal securities regulation, mail fraud, and common law actions against deceit and misrepresentation.

The Court was reluctant to simply draw the line at falsity. As it did in prior cases, it suggested that “falsity alone should not strip protections from the publisher.” The Court reiterated that some error in the public debate is inevitable, and that asking a jury to decide what is the meaning of “true” might “effectively institute a system of censorship.” Instead, the Court focused on the element of conduct “to resolve the antithesis between civil libel actions and the freedom of speech and press.”

The Court then proceeded to define its constitutional standard for assessing liability for defamation against public figures such as Butts and Walker. Ultimately, it concluded that “a ‘public figure’ who is not a public official may also recover damages for a defamatory falsehood whose substance makes substantial danger to reputation apparent, on a showing of highly unreasonable conduct constituting an extreme departure from the standards of investigation and reporting ordinarily adhered to by responsible publishers.” The Court emphasized that this standard only applies to actions involving public figures or matters of public interest.

Having set the standard, the Court then applied it to the facts of the cases of both Butts and Walker. As to Butts, the Court emphasized that the article about him was not “hot news” that urgently needed to be published. The article’s editors had



ample time to investigate the facts and confirm their validity. The evidence revealed that there was an obvious lack of foundation for the story, and that the publisher had failed to meet even the most elementary standards of professional **journalism**, as the court had defined the standard. Butts was accordingly entitled to collect money damages for the publisher's defamatory statements.

Despite this finding, the Court reached an opposite result when assessing the factual background of Walker's case. Far from finding "actual malice," the trial court in that case had found that the evidence did not support anything beyond ordinary negligence. Also, the article in this case required immediate publication, in contrast to the relaxed time frame in the case of Butts. The factual background in this case was also "internally consistent" and overall reasonable. Therefore, the Court refused to find any actionable defamation. Walker was accordingly not entitled to recover damages from the Associated Press.

See also: Bauer v. Kincaid, 759 F. Supp. 575 (1991); *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975); *Red & Black Publishing Co. v. Board of Regents*, 262 Ga. 848 (1993); *Time, Inc. v. Hill*, 385 U.S. 374; *United States v. Caldwell*, 408 U.S. 665 (1972)

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Dobbs, Dan B., and Paul T. Hayden. *Torts and Compensation: Personal Accountability and Social Responsibility for Injury*, 4th ed. St. Paul, MN: West Group Publishing, 2001; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Goodale, James C. *Communications Law*. New York: Practicing Law Institute, 1999.

Ryan C. Hudson

Authentication

Authentication, in its most general form, is a process for gaining confidence that something is, in fact, what it appears to be. In everyday life, people continually authenticate people, objects, and other entities around them by consciously or subconsciously assessing clues that provide evidence of authenticity.

In communication and transaction settings, authentication is typically understood as the process of confirming a claimed identity. This involves two steps: first a user must present a user identifier (such as "John Doe" or "Employee 13579") that uniquely represents the user in the verifier's context. The second step, identity authentication, involves verifying that the presenter of the user identifier is authorized to do so—that the presenter is the user to whom the user identifier has been assigned.

Single-factor identity authentication ascertains that the presenter possesses something associated with the presented user identifier that is not generally accessible. This can be something the user knows (such as a **password** or a **cryptographic** key), something the user has (such as a smart card), or something the user is (i.e., a user **biometric identifier**). Each of these three single-factor authentication methods has limitations: what the user knows may be guessed, forgotten, or shared with others; what the user has may be costly, faulty, lost, stolen, or replicated; and what the user is cannot be revoked, does not permit privacy, and requires

human involvement. To strengthen the process of identity authentication, several single-factor methods may be combined, resulting in multi-factor authentication.

When authenticating claimed identities, verifiers implicitly place trust in the authenticity of the clues themselves. In cases where verifiers are effectively agents or proxies of the user, users can be trusted with creating their own identifiers and using their own authentication method. For example, a self-generated username and password suffice to protect access to one's own **computer**. In many communication and transaction systems, however, the security interests of verifiers and users are not aligned. In these cases, verifiers require clues that originate from trusted parties, also referred to as issuers, in order to gain confidence in the authenticity of presented user identifiers. Kerberos tickets and X.509 identity certificates are well-known examples of certified user identifiers that are issued by trusted parties; these certified identifiers contain cryptographic authenticity marks that are hard to forge.

When the same certified user identifiers are relied on by multiple verifiers, both users and verifiers must place tremendous trust in the issuer, which houses the power to trace, profile, and impersonate any user. For example, all user interactions with verifiers can be inescapably traced and linked on the basis of the X.509 identity certificates that they use. Identity authentication and privacy are not competing interests that need to be balanced, however. Advances in modern cryptography allow for the creation of certified user identifiers that provide users and verifiers with all the privacy and security benefits of noncertified, self-generated identifiers.

More generally, modern authentication techniques such as digital credentials enable issuers to certify user identifiers (and, more generally, identity assertions) in such a manner that no tracing, linking, and impersonation powers arise in them.

See also: **Anonymity**

Suggested Reading: Brands, Stefan. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. Cambridge, MA: MIT Press, 2000. <http://www.credentica.com/technology/book.html>. Online, March 2006; Clarke, Roger. "Anonymous, Pseudonymous and Identified Transactions: The Spectrum of Choice." Proc. IFIP User Identification & Privacy Protection Conference, Stockholm, June 1999. <http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html>. Online, March 2006; London School of Economics and Political Science. *The Identity Project: An Assessment of the UK Identity Cards Bill and Its Implications*. Version 1.09, June 27, 2005. <http://is.lse.ac.uk/idcard/identityreport.pdf>. Online, March 2006.

Stefan Brands

Automatic teller machine

The automatic or automated teller machine (ATM) enables bank customers to perform banking services without the assistance of a bank employee. The most basic task an ATM performs is enabling a customer to withdraw cash from the customer's bank account. Other banking services that may be added to the ATM's primary function include account balance updates and money transfers. Recently, ATMs have been configured to vend postage stamps and prepaid mobile phone minutes. The evolution of the ATM from cash dispenser to multi-purpose necessity of modern life was facilitated greatly by a fully integrated multibank network.



Barclays Bank in Enfield Town in north London set up the world's inaugural ATM on June 27, 1965. Although John Shepherd-Barron receives consideration as the inventor of this particular installation, the ATM's evolution into a modern cash dispenser was assisted by many inventors. In 1939 Luther George Simjian registered patents for an early incarnation of an ATM. While they are not the original inventors of the device, Don Wetzel and two fellow engineers registered a patent on June 4, 1973, for the first machine that is considered to be a modern and successful cash machine. In 1969 the Rockville Centre branch of Chemical Bank installed the first ATM in the United States.

The first generation of the cash machine was off-line and dispensed prepackaged bundles of cash in a fixed denomination. At first, banks did not employ a computer network to stay in contact with ATMs. Since funds were not withdrawn automatically from a customer's account, ATM rights were not issued to all bank customers. Rather, banks were very selective about those to whom ATM cards were distributed (e.g., **credit card** holders with good banking history). To ensure that the bank customer withdrawing money from the machine was the authorized user, ATM cards had to be different from credit cards so account information could be included. (At this time, credit cards were void of information-laden magnetic strips.) The personal identification number (PIN) the user enters was compared to the PIN stored on the ATM card's magnetic strip.

While the PIN concept is still relatively unchanged with regard to ATM usage, technology has served as a catalyst for increased security safeguards. Customers continue to insert a plastic card with a magnetic stripe into the ATM and confirm they are the authorized user by entering a numeric **password** or code (PIN) that is at least four digits in length. Typically, if a user enters the incorrect PIN three times consecutively, the machine does not return the card to the individual as an effort to thwart unauthorized persons from deducing the proper passcode by conjecture. In addition to the standard magnetic striped plastic card, some ATMs use **smart cards** to store customer data, and a new generation of machines may include **biometric identifiers** such as iris of the human eye or **fingerprint** scanning. This means that the biometric information would have to be stored in databases by the bank or another organization, thereby raising concerns about privacy and security.

The ability to connect a bank's network to an ATM is a modern-day convenience. This communications network provides the foundation for the entire ATM system: the approval of a transaction by the authorizing (or card issuing) institution. This advancement allows travelers to withdraw money from ATMs outside their hometowns and even home countries.

ATMs contain secure cryptoprocessors, on which the integrity of the machine relies. ATMs are able to connect directly via a dial-up modem using a telephone line. Currently, more and more ATMs take advantage of high-speed **Internet** connections, thus decreasing the amount of time devoted to a transaction.

For security purposes, the United States requires encryption by law. Prior to 2005, ATM dealings were typically encrypted with Data Encryption Standard (DES). Starting in 2005, most transactions require using Triple DES (TDES) as the encryption method. While the algorithm is thought to be secure, the risk of attack is always present. There is some speculation that TDES is archaic and needs to be replaced by the Advanced Encryption Standard (AES), the encryption standard of the United States government.

Regarding ATMs and theft, banks are held responsible when a customer's money is stolen. However, there have been many difficult-to-verify accounts of banks making it exceedingly challenging to recoup even a portion of the lost funds. There are situations of fraud where a bank unwittingly has committed the fraud. Bank fraud occurs at ATMs if the bank accidentally supplies the machine with the incorrect bills. Consequently, the ATM would dispense far more cash to each authorized user than had been requested. First-time users of incorrectly stocked machines are rarely prosecuted. A user who repeatedly frequents the overgenerous ATM, however, is usually tried. Banks accuse their customers of fraud because of the presence of "phantom withdrawals" from ATMs. In this situation, the customer states that the withdrawal of funds never occurred, but the bank's records indicate that such a transaction took place. A renowned **cryptography** researcher, Ross Anderson, has uncovered errors in banking security by investigating numerous instances of this phenomenon.

Initial safeguarding of ATMs against theft concentrated on creating a cash dispenser that was impervious to attempted hackings: a safe that also functioned as a cash dispenser. ATMs were commonly located in the sides of buildings for walk-up service as well as for drive-through convenience. This type of protection strategy led to numerous ram-raiding attempts by thieves. The nomenclature of this style of assault refers to the tactics used by thieves to crack open the safe by literally ramming into it.

As time went on, the typical location and installation of ATMs changed, largely as a result of the institution of dye marking packets and the use of smoke bombs attached to money bundles housed inside the ATM. It is far more common to find a free-standing ATM in a retail store as opposed its wall-mounted predecessor. Technological advances also paved the way for the use of numerous security cameras, so that the ATM as well as the area around the ATM can be monitored. As an additional security measure, some free-standing ATMs located inside retail establishments only dispense written tickets, and users must then redeem the tickets for cash from a store employee.

By the early years of the twenty-first century, criminal activity involving ATMs was commonly classified into two categories based on the amount of technological prowess displayed by the perpetrator. In the decidedly low-tech method, a lookout observes the victim entering his or her PIN into the nearby ATM. As the victim moves away from the **surveillance cameras**, the lookout's accomplice then steals the victim's ATM card. Short of the convenience in locating potential victims, this method offers virtually no other benefits to the criminals. In addition, this criminal activity is equivalent in risk and penalty to other violent crimes. Aided by the low cost and high availability of wireless cameras and magnetic card readers, the high-tech mode of criminal operation is growing in popularity. The criminal installs a card reader on top of the ATM's existing real card reader. The wireless camera allows the perpetrator surreptitiously to gain the user's PIN. This type of high-tech criminal activity poses a comparatively smaller risk to the thieves. Banks are striving to create effective stops for the latter fraud category by working to make the external features of ATMs tamper evident in order to prevent the use of piggy-backed card readers and wireless camera surveillance. In addition, many banks are now using smart cards that cannot be read by nonauthenticated devices. Although



the ATM has been hailed as one of the top 100 ideas of the twentieth century, security and privacy aspects of the ATM continue to be an issue.

See also: **Authentication; Banking and financial records**

Suggested Reading: Anderson, Ross. *Perspectives: Automatic Teller Machines*. <http://axion.physics.ubc.ca/atm.html>. Online, December 2005; Broome, Lissa, and Jerry W. Markham. "Banking and Insurance: Before and After the Gramm-Leach-Bliley Act," *Journal of Corporation Law* 25 (2000). www.uiowa.edu/~lawjcl. Online, December, 2005; Inventors. *Automatic Teller Machines (ATM)*. <http://inventors.about.com/library/inventors/blatm.htm>. Online, December 2005.

Christine Berry Lloyd

Automobile

The automobile poses a unique challenge for both police and the driving public within the framework of **constitutional protections**, especially Fourth Amendment rights. Unlike a fixed dwelling or **home**, a car can be moved at will. This mobility increases the possibility of criminals evading police and destroying incriminating evidence. Issues involved in an **automobile search** also pose important questions about whether some restrictions of privacy rights are necessary in order to promote greater security against foreign and domestic dangers. The automobile and other moving vehicles, such as the truck used by Timothy McVeigh to blow up the Alfred P. Murrah Federal Building in Oklahoma City in 1995, can be real threats. The car search issue is significant for the driving public because of the increasing powers of intrusion by the police and the reduced expectations of privacy exemplified by police checkpoints on roads.

In *Carroll v. United States*, 267 U.S. 132 (1925), the Supreme Court provided the first definitive rationale for warrantless searches and seizures of automobiles, focusing on the differences between a fixed dwelling and a movable vehicle. However, the leeway allowed in *Carroll* did not exempt the police from respecting Fourth Amendment rights. The court was clear in its intentions that police must have probable cause for believing a vehicle was carrying contraband goods; otherwise, persons lawfully using the highways would be subject to inconvenience and the indignity of such a search. By emphasizing probable cause, the court provided a constitutional rationale for police and law enforcement officials to stop the vehicle and conduct a search.

Historically, the Court has expanded the powers of the police to conduct warrantless car searches. *Chambers v. Maroney*, 399 U.S. 42 (1970) reaffirmed the Court's position that warrantless searches of cars and their contents are permissible. The Court also expanded car searches by allowing the police to stop and question persons traveling in their automobiles based on anonymous tips. If police find evidence that establishes suspicion of criminal activity, such evidence can be used against the driver and other persons in the automobile (*Alabama v. White*, 496 U.S. 325, 1990). The expansion of warrantless car searches impacts all drivers on American highways, especially drivers entering the United States from Canada or Mexico. Police and law enforcement officials have more intrusive powers at the border, and may conduct more intrusive car searches in order to prevent contraband from entering the United States (see, for example, *United States v. Flores-Montano*, 541 U.S. 149, 2004).

More intrusive car searches would appear to represent a further erosion of Fourth Amendment protections provided in *Mapp v. Ohio*, 367 US 643 (1961),

which established the exclusionary rule that allows illegally seized evidence to be excluded in criminal court proceedings. Critics of *Mapp* believe the exclusionary rule went too far by blocking police arrests that should have been made. By 1984, the Supreme Court did allow evidence to be used in criminal cases that did not conform to the requirements of the exclusionary rule (*United States v. Leon*, 468 U.S. 897). The Court established the good faith exception to the exclusionary rule, whereby the police may gain evidence by reliance on a warrant that police believe to be valid, even if it is subsequently found to be invalid.

A rollback of car searches is unlikely. Domestic and international concerns appear to make the American public more willing to give the police more leeway, which serves to limit Fourth Amendment protections against searches and seizures and rights to privacy. The initial passage and renewal of the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)** by the United States Congress illustrates that national policymakers are willing to legislate further restrictions on these civil liberties. The September 11, 2001, attack and destruction of the twin towers of the World Trade Center heightened fears of terrorist attacks and added to the urgency of demands for remedies. Increased concerns about terrorism and the public focus on crime-control efforts have combined to enlarge the scope of permissible police behavior in searching vehicles.

Police checkpoints illustrate this increasing toleration of intrusive police activity. The checkpoint is significant in car searches because the individual can arrive at the checkpoint with no prior suspicion of wrongdoing by police, and yet be subjected to a car search, as illustrated in *New York v. Class*, 475 U.S. 106 (1986) and *United States v. Flores-Montano*, 541 U.S. 149 (2004), both of which affirmed that police may search one's car without prior suspicion. At checkpoints, police often discover alcohol intoxication or find contraband in vehicles that can be used as evidence in court proceedings against the driver. The automobile, because it is not a fixed building, will continue to test how far the police can intrude on Fourth Amendment protections and the right to privacy, as well as what limitations people are willing to accept in order to live in a more secure society.

See also: Cady v. Dombrowski, 413 U.S. 433 (1973); *Schmerber v. California*, 384 U.S. 757 (1966); *Sobriety Checkpoint*; *South Dakota v. Opperman*, 428 U.S. 364 (1976)

Suggested Reading: Devetski, Timothy J. "Fourth Amendment Protection against Unreasonable Seizure of the Persons: The New Common Law Arrest Test for Seizure," *Journal of Criminal Law Criminology* 82, no. 4 (Winter 1992): 747–772; Flaherty, David H. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill: University of North Carolina Press, 1992; Hall, Kermit L. *Conscience, Expression and Privacy: The Supreme Court in American Society*. New York: Garland, 2000; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LeFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed. St. Paul, MN: West Publishing Company, 1996.

D'Linell Finley



Automobile search

A car search, simply put, is the intrusion into the interior of an **automobile** by an agent of the government. From a privacy standpoint, the question is whether owners and occupants of automobiles have a **reasonable expectation of privacy** in automobiles under the Constitution. While it is easy to state what a car search is, it is significantly more difficult to delineate the issues related to privacy and car ownership or occupancy. Briefly, the concerns relate to the following: searches with warrants and searches in the absence of a warrant; searches when the car is occupied and when it is not; searches of open areas in the car and searches of closed or locked areas of the car; searches of containers found in the car; and searches of the driver of the car and of passengers in the car. The situation is further complicated when the question of the government's right to stop a car is raised.

The courts have long recognized that citizens do not surrender all the protections of the Fourth Amendment by entering an automobile. The Supreme Court first required that persons in a car must have a "constitutionally protected reasonable expectation of privacy" before there could be any constitutional violation in *Katz v. United States*, 389 U.S. 347 (1967). By its very physical characteristics, a car offers less privacy than does a **home**. The Supreme Court noted in *Cardwell v. Lewis*, 417 U.S. 583 (1974) that "a car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view." Further, the courts have noted that since a multitude of state laws and regulations govern the ownership, maintenance, and operation of automobiles, drivers should expect that the state, in enforcing those laws and regulations, will intrude to some extent upon a driver's privacy.

While it is not possible to delineate the entire history of privacy in an automobile, or other vehicle, here, there are some basic principles that must be addressed. When discussing the basis for any right or expectation of privacy in an automobile, the foundation is found in the Fourth Amendment to the Constitution, which states, in part, "The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated, and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

It is also important to understand that generally, a **search warrant** is an order obtained by the government from an independent judge upon showing there is probable cause to invade someone's privacy. Ordinarily, the probable cause will be the belief that evidence of a crime, or a person to be arrested, will be found in the area to be searched. A warrant must list with specificity the area to be searched, the items to be seized, or the person to be arrested. While the person whose privacy is invaded usually has no prior opportunity to challenge a search warrant, before evidence seized as a result of issuance of the warrant can be used in court, the person can challenge the warrant's validity. All of the requirements for a search warrant to be issued for a home must also be met for a search warrant to be issued for a car.

Despite the language of the Fourth Amendment, the Supreme Court has created a number of exceptions when searches and seizures of evidence or persons are permitted without a warrant. For example, in exigent circumstances when police officers have a good faith belief that evidence will be destroyed, criminals will escape, or the safety of the officers require it, warrantless searches will be allowed. The moveable

nature of cars and trucks creates the kind of exigent circumstances the courts have historically relied upon to authorize government's warrantless actions.

The history of cases dealing with privacy in automobiles has not been even. The Supreme Court has taken various twists and turns in its efforts to balance the needs of law enforcement and the privacy concerns of citizens. Logically, one of the first questions to be asked about searching cars is whether police can stop the vehicles.

Before 1976, the courts in this country were divided on whether officers could randomly stop cars without having a reasonable suspicion that a violation of the law was occurring. The Supreme Court considered *Delaware v. Prouse*, 440 U.S. 648 (1976) in order to resolve the conflict. In that case, an officer testified that he had nothing else to do, so he randomly stopped the defendant's car to check the driver's license and registration. Upon approaching the car, he smelled marijuana, and when he reached the car, he could see a bag of marijuana on the floor. The driver was subsequently arrested. In affirming the Delaware courts' suppression of the evidence seized during the random stop, the Supreme Court held that "the marginal contribution to roadway safety possibly resulting from a system of spot checks cannot justify subjecting every occupant of every vehicle on the roads to a seizure—limited in magnitude compared to other intrusions but nonetheless constitutionally cognizable—at the unbridled discretion of law enforcement officials."

Stopping multiple cars at road blocks, however, is a different question. In *United States v. Ortiz*, 422 U.S. 891 (1975), the Supreme Court first ruled that searching cars during routine traffic checkpoint stops was a violation of Fourth Amendment rights. A year later, the Court ruled that checkpoint stops were acceptable. In *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976), the Court approved use of Border Patrol checkpoint operations to inquire about occupants' citizenship status. The practice required slowing all oncoming traffic "to a virtual, if not a complete, halt" at a highway roadblock, and sending vehicles selected by Border Patrol agents to another area for a more thorough inspection. Recognizing that the governmental interest involved was the same as that furthered by roving-patrol stops, the Court nonetheless sustained the constitutionality of the Border Patrol's checkpoint operations.

The Court reaffirmed **sobriety checkpoint** stops in *Michigan Dept. of State Police v. Sitz*, 496 U.S. 444 (1990) when the need to protect lives and property trumped the need to protect drivers' Fourth Amendment rights. The courts have also upheld pretextual stops in cases where officers find some alternative reason to stop a car when they really want to search it. For example, in *Whren v. United States*, 517 U.S. 806 (1996), undercover officers wanted to stop a car with young occupants on the belief they were involved in drug activities. They followed the car, driven by a youthful driver, and after the driver turned without signaling, the officers approached the car when it was stopped at a traffic light and instructed the driver to put the car in park. At the same time, one officer saw two bags of marijuana in the driver's hands. The trial court refused to suppress the drugs seized. In affirming that ruling, the Supreme Court noted, "Not only have we never held, outside the context of inventory search or administrative inspection . . . that an officer's motive invalidates objectively justifiable behavior under the Fourth Amendment; but we have repeatedly held and asserted the contrary."

When talking about a car search pursuant to a warrant, all the general rules governing search warrants apply. In the case of warrantless searches, once a car is



stopped, however, the road is much less defined. The seminal Supreme Court case authorizing a warrantless search of a car was *Carroll v. United States*, 267 U.S. 132 (1925). The case resulted from the stop and search of a notorious bootlegger's car between Detroit and Grand Rapids, Michigan, during prohibition. The Court relied on an officer's probable cause to believe there was contraband in the suspect automobile in order to justify the stop and subsequent seizure of both the car and the liquor found in the car.

One of the more logical circumstances under which a warrantless search of a car is acceptable is the "**plain view**" exception. Simply, if contraband is plainly visible to an officer once the car is stopped, the officer has the right to seize it, and it will be admitted into evidence at trial. For example, in *Colorado v. Bannister*, 449 U.S. 1 (1980), the court refused to block the admission of wrenches and stolen items that were discovered by an officer looking into a car window after he had stopped the driver for speeding. The court held simply that there was probable cause to seize the items without a warrant.

Similarly, items found in a car during a *Terry* search are also admissible although *Terry* searches are conducted without a warrant. In *Terry v. Ohio*, 392 U.S. 1 (1968), the Court upheld an officer's right to search pedestrians for weapons if there was an articulable suspicion of criminal activity justifying a stop of the pedestrian. The *Terry* rationale, the need to protect the officer's safety, has been applied to car searches as well.

The Court was quick to apply *Terry* to specific automobile situations. For example in *Adams v. Williams*, 407 U.S. 143 (1972), it held that police, acting on an informant's tip, could reach into the passenger compartment of an automobile to remove a gun from a driver's waistband even where the gun was not apparent to police from outside the car, and the police knew of its existence only because of the tip. That decision rested, in part, on the Court's concern about the danger for police officers in traffic stop and automobile situations.

The Court again recognized that investigative detentions involving suspects in vehicles were especially fraught with danger to police officers in *Pennsylvania v. Mimms*, 434 U.S. 106 (1977). There, the Court held that police may order persons out of a car during a stop for a traffic violation and may frisk those persons for weapons if there is a reasonable belief that those persons are armed and dangerous. Consider *Michigan v. Long*, 463 U.S. 1032 (1983). In that case, although the driver was outside the car, an officer had searched the interior of the car after seeing a hunting knife on the floor. During the search, marijuana was found, and the driver was charged with possession. In the *Michigan* ruling, the Court looked to *New York v. Belton*, 453 U.S. 454 (1981) to expand the *Terry* search concept. In discussing searches incident to arrest, the *Belton* decision explained that the concept of "within a person's immediate control" had not been successfully defined. Thus, to provide a "workable rule," the Court held that "articles inside the relatively narrow compass of the passenger compartment of an automobile are in fact generally, even if not inevitably, within 'the area into which an arrestee might reach in order to grab a weapon'" Applying the rules governing search incident to arrest, the *Belton* decision also ruled police could examine the contents of any open or closed container found within the passenger compartment, "for if the passenger compartment is within the reach of the arrestee, so will containers in it be within his reach."

As noted, search incident to arrest is another of the justifications approved by the Supreme Court for searching a car without a warrant. The search incident to arrest doctrine was clarified in *United States v. Robinson*, 414 U.S. 218 (1973). There, the Court directed that “in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a ‘reasonable’ search under that Amendment.” While a search incident to arrest was initially limited by the courts, as seen in *Belton*, it is a doctrine that has expanded over time. Indeed, in *Thornton v. United States*, 541 U.S. 615 (2004), the court allowed a search of the interior of a car even though the driver had stepped out of the car before he was arrested. Police may also search a vehicle and its contents without a warrant in the course of conducting an “inventory search” following a lawful arrest or vehicle seizure.

It had been a long-standing rule that in carrying out a warrantless search of a car, police are generally prohibited from searching the passengers in the car. This, too, is a barrier that has fallen over time. If officers have a reasonable suspicion that passengers may be armed, passengers may be subjected to a *Terry*-style search. Further, if while searching the car, officers find sufficient evidence to provide probable cause to arrest passengers, they may conduct a search incident to arrest.

There have been cases in which a car search led to the arrest of the car’s occupants, rather than the arrest of the passengers justifying a search. In *Maryland v. Pringle*, 540 U.S. 366 (2003), the Supreme Court approved the arrest of three automobile passengers after investigating officers found \$763 and five baggies of cocaine in the car, and all three occupants denied any knowledge of the drugs or cash. The car had been stopped for speeding. After giving the driver a verbal warning, the officer asked for and received permission to search the car. The Court held that “an entirely reasonable inference from these facts [is] that any or all three of the occupants had knowledge of, and exercised dominion and control over, the cocaine. Thus a reasonable officer could conclude that there was probable cause [to arrest all three].”

The powers of police to conduct searches of containers in cars have expanded over time, along with the other powers discussed here. In 1977, the Supreme Court decided *United States v. Chadwick*, 433 U.S. 1, and held that a warrantless search of a footlocker stored in the open trunk of a defendant’s car was a violation of the defendant’s Fourth Amendment rights. The evidence, a large quantity of marijuana, was not admissible.

Three years later, the Supreme Court did a complete turnaround and allowed a thorough search of a car and sealed containers within the car when there was probable cause to believe the car, or the containers, contained drugs or other contraband. In *United States v. Ross*, 456 U.S. 798 (1982), the Court reviewed the *Carroll* decision to find that, historically, warrantless searches of cars were appropriate to seize contraband in transit. It was a small step for the Court to find that containers within the car should be subject to the same search to achieve the same goal. It ruled that “the rationale justifying a warrantless search of an automobile that is believed to be transporting contraband arguably applies with equal force to any movable container that is believed to be carrying an illicit substance.”

The Court then noted that its decision was a direct contradiction of the holding in *Chadwick*, but then relied on *Carroll* to rule that “when a legitimate search is



under way, and when its purpose and its limits have been precisely defined, nice distinctions between closets, drawers, and containers, in the case of a home, or between glove compartments, upholstered seats, trunks, and wrapped packages, in the case of a vehicle, must give way to the interest in the prompt and efficient completion of the task at hand This rule applies equally to all containers, as indeed we believe it must.”

Suggested Reading: Black, Henry C. *Black’s Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Bellamy, Kristi Michelle. “The ‘Automatic Companion’ Rule and Its Constitutional Application to the Frisk of Car Passengers,” *American Journal of Criminal Law*. 27 (2000): 217–232; Bergman, Paul, and Sara J. Berman-Barrett. *The Criminal Law Handbook: Know Your Rights, Survive the System*. Berkeley, CA: Nolo Press, 2005; Bodemheimer, Davis J., and James W. Ely, Jr., eds. *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Dix, George E. *Gilbert Law Summaries: Criminal Law*. Orlando, FL: Harcourt Legal & Professional Publishers, 2001; Levin, Michael. *The Complete Idiot’s Guide to Your Civil Liberties*. New York: Penguin Putnam Inc., 2003; Skelton, David. *Contemporary Criminal Law*. Burlington, MA: Butterworth-Heinemann, 1997.

David J. Brown

B



Background checks

Background checks are investigations into the character or history of an individual. They are performed by government and private-sector employers, by purchasers of corporations who are performing due diligence checks on the acquired corporation's leaders, by insurance companies and other litigants who wish to investigate individuals making claims, by charitable organizations who are seeking volunteers, and sometimes by family members or friends who are suspicious of the individual's love interest. A number of factors have contributed to a dramatic increase in background checks, including fears of terrorism and workplace violence, liability for employee negligence, risks associated with hiring litigious employees, employee fraud and embezzlement, the possibility of volunteers abusing the elderly or children, and the low cost and high speed with which electronic public records databases can be searched.

Background checks vary greatly in procedure and scope, depending on the purpose for which the check is performed. A background check for a national security position can cost \$10,000, involve polygraph testing and an in-depth exploration of the applicant's associations, and focus on past or current behavior that could subject the applicant to extortion.

Regular employment background checks are much less expensive, ranging from a simple electronic records search that can cost less than \$50 to in-depth vetting for corporate executives, which can run into thousands of dollars. Regular employment background checks focus on criminal convictions and arrests, past litigations, a history of insurance or worker's compensation claims, driving record, **credit card** and other debt, drug and alcohol use (which may be explored using **urine analysis** or hair or **blood testing**), medical problems, and military history. They can involve interviews with neighbors and other associates, and verification of educational status and of prior employment. Because of concerns about employee theft, major employers have created cooperative anti-shoplifting databases that may be queried to see whether an applicant has ever been accused of dishonesty without actually being charged with a crime. In the retail and service sector, background checks often are combined with "personality tests" designed to gauge an individual's attitudes toward workplace organization, work ethic, and honesty.



In the employment context, background checks are governed by the federal **Fair Credit Reporting Act** (FCRA) and by state regulations. The FCRA requires employers to obtain consent from the employee before engaging in a background check, specifies procedures to prevent stale and inaccurate information from being provided to the employer, and gives the employee the right to an “adverse action” notice if the check is used to deny employment. The Federal Equal Employment Opportunity Commission bars employers from relying solely on criminal conviction information; the nature of the conviction must be relevant to the job, or there must be some independent, sound business reason for taking action against the individual. State laws impose further restrictions, in some cases including prohibitions on the use of derogatory information more than seven years old or arrest data that did not result in a conviction.

Outside the employment context, investigating the background of another may not be subject to any kind of regulation. For instance, charitable organizations may investigate prospective volunteers to avoid risks of elder or child abuse. Sometimes individuals suspicious of a friend’s or family member’s personal activities will initiate a background check. These unregulated checks can amount to cursory scans of public records databases or more involved inquiries, including illegal “asset searches” performed by investigators who trick banks and other organizations into revealing the subject’s financial status.

See also: **Workplace privacy**

Suggested Reading: Etzioni, Amitai. *The Limits of Privacy*. New York: Basic Books, 1999; Flaherty, David H. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill: University of North Carolina Press, 1992; Givens, Beth. *Employment Background Checks: A Job-Seeker’s Guide*. Privacy Rights Clearinghouse, <http://www.privacyrights.org/fs/fs16-bck.htm>. Online, March 2006; Rosen, Les. *Criminal Records and Getting Back into the Workforce: Six Critical Steps for Ex-Offenders Trying to Get Back into the Workforce*. Privacy Rights Clearinghouse, <http://www.privacyrights.org/ar/rosencrim.htm>. Online, March 2006; Smith, Robert Ellis. *Workrights*. New York: E.P. Dutton, 1983; Solove, Daniel J. “Digital Dossiers and the Dissipation of the Fourth Amendment Privacy,” *Southern California Law Review* 75 (2002): 1083–1167.

Chris Jay Hoofnagle

Banking and financial records

Most individuals have high expectations of privacy with regard to their banking records and other financial information. People generally do not expect information about their bank accounts, **credit card** transactions, and other financial matters to be shared with outside parties without their permission. The shift from cash to checks and to debit and credit cards has made paying for goods and services more convenient, but it has resulted in vast amounts of data stored automatically in **computers** and databases, and it raises the potential for databases to be linked in order to share and combine information obtained from different sources. The result can be a detailed compilation of information about an individual’s saving, spending, and even travel habits.

One of the problems created by the presence of financial information in databases is the increased risk of **identity fraud** or theft (assuming another person's identity for financial gain). As more **personally identifiable information** becomes available, it becomes easier for criminals to access details that were previously considered private. A second problem is government access to bank and financial records that individuals would prefer to keep secret. The possibility of government **surveillance** of financial activities threatens some of our fundamental freedoms.

Several federal laws have been enacted to protect banking and financial privacy in the United States, although they all have important exceptions that allow information to be shared with government authorities and private-sector entities for various purposes.

The Right to Financial Privacy Act (RFPA) creates a right of privacy with respect to an individual's bank records. It was enacted in response to the Supreme Court's decision in *United States v. Miller* (1976), where the Court found that bank customers had no legal right to privacy in their banking transactions. The Court concluded that when individuals voluntarily share or develop records in the ordinary course of a business relationship with another entity (as in a bank-customer relationship), they have relinquished their expectation of privacy and therefore have no constitutional protection against government access to such records.

Congress enacted the RFPA in response to the *Miller* decision. The RFPA bars federal government agencies from obtaining records from a financial institution unless the customer authorizes access; a valid summons, subpoena, or **search warrant** has been prepared; or there is an appropriate written request from a government official who is authorized to obtain the records. Moreover, the government agency must give individuals notice and an opportunity to object before any **disclosures** can be made. The RFPA governs only disclosures to the federal government and its officers, agents, and departments; it does not govern the sharing of information with private businesses or with state governments. As for the sharing of financial information in the private sector, the **Fair Credit Reporting Act** and the **Financial Services Modernization Act of 1999**, also known as the Gramm-Leach-Bliley Act (GLBA) and discussed later, provide some protection for individuals. State laws may provide similar protection against access by state government officials and agencies.

The RFPA has many exceptions. The most noteworthy is the **Bank Secrecy Act** (BSA), which requires federally insured banks to retain records and create reports that could be useful in tax, criminal, or regulatory investigations. The law was passed to address concerns that the shift from paper to computerized records would make law enforcement in relation to white-collar crime more complicated. The BSA not only allows banks and other financial institutions (including gambling casinos and dealers in precious metals) to disclose financial records to the federal government in certain circumstances; it actually *requires* them to report the transactions. Moreover, when banks report information to the federal government pursuant to the BSA, they are required *not* to disclose to their customers that reports have been filed about them.

Among other transactions, the law requires the reporting of deposits or withdrawals of more than \$10,000 in cash in one day, or the purchase of money orders, cashier's checks, traveler's checks and similar instruments involving more than



\$3000 of cash. The bank must report the individual's name, address, and occupation, as well as other information about the transaction in a "currency transaction report" to the **Internal Revenue Service**. For transactions exceeding \$5,000 into or out of the United States, the amount, date, and identity of the recipient must be reported. Moreover, if it appears that the customer is taking action to evade the reporting requirement, the bank must file a "suspicious activity report" explaining the activity. All of these reports are electronically filed and are immediately available to United States Attorneys and law enforcement agencies throughout the country. Financial institutions face heavy penalties if they do not comply. The BSA was strengthened in 2001 by the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)**, which gave government authorities increased access to bank records in an effort to track financial transactions that could identify terrorists.

The purpose of the BSA is to aid law enforcement in policing money laundering, tax evasion, embezzlement, drug dealing, and other criminal behavior. A single report about a customer is usually of no concern to authorities, but multiple reports may signal a need for further investigation. Businesses that routinely deal in large amounts of cash, such as bars and restaurants, can be exempted from having their deposits and withdrawals monitored, although such an exemption is not routinely granted.

The BSA covers banks, retailers, gasoline companies, and other issuers of credit cards; traveler's check issuers; the U.S. Postal Service; securities dealers; and casinos. In addition to the mandatory disclosure of the transactions discussed previously, certain financial information is not protected by the RFPA and therefore can be disclosed to government officials without customer consent; these include disclosures that do not identify a customer personally, disclosures in connection with the financial institution's own interests (such as the perfection of security interests and information relating to federal government loans), disclosures relating to bank regulatory supervision, disclosures authorized under other federal laws, and emergency disclosures to federal agencies with foreign intelligence or other national security functions.

With respect to the private sector, the GLBA imposes limits on the collection and sharing of information in the financial services industry. The GLBA grew out of a movement to reform the financial services industry and eliminate the historical separation of banks, brokerage companies, and insurers. After the collapse of the banking industry in the Great Depression, Congress passed the Glass-Steagall Act, which prohibited national and state banks from affiliating with securities investment companies. In 1956 Congress passed the Bank Holding Company Act, which prohibited banks from owning non-bank companies in general. The Bank Holding Company Act was amended in 1982 to prohibit banks from engaging in insurance underwriting activities. As the financial services industry evolved in the 1980s and 1990s, however, Congress repealed these prohibitions in the GLBA, and banks were once again allowed to engage in a wide range of financial services activities, including insurance and securities investments.

Congress perceived significant privacy risks in allowing banks, brokerage firms, and insurers to merge or affiliate, so it included in the GLBA a series of provisions designed to limit the sharing of customer information. Another motivating force

was the adoption of the **European Data Protection Directive** in 1995. The directive applies to any entity that maintains personal information on EU citizens. This means that U.S. companies must ensure that information on EU citizens is treated in accordance with the privacy standards in effect in Europe. Congress fashioned the privacy protections of the GLBA with the intention that compliance with the GLBA would also mean compliance with the EU rules.

The privacy protections in the GLBA are far from absolute, however. The GLBA sets no limits on the type of information that financial services companies can collect and retain on individuals. Individuals who interact with a financial services company must understand that virtually all information that the business can uncover about them can be stored in a database. Moreover, the GLBA expressly authorizes banks, insurers, investment companies, and other financial services organizations that are affiliated with each other, through common ownership or otherwise, to share personal financial information without the customer's permission. An affiliate is a company that controls, is controlled by, or is under common control with another company. Although affiliates must tell customers that they are sharing this information, individuals cannot block the sharing of information among affiliated institutions. Because large conglomerates of affiliated entities dominate the financial services industry, sharing of personal information without customer consent is routine.

Customers can choose to opt out of any disclosure arrangement involving the sharing of their personal data between a conglomerate and a non-affiliated third party. A non-affiliated company is one that is unrelated to the financial services company possessing personal information about the customer. Non-affiliates may include companies that want the information in order to compile mailing lists for their own marketing purposes.

Individuals must read the privacy policy of the financial institution to learn how to exercise their **opt-in and opt-out** rights. The GLBA does not require consent from the customer before any data can be distributed to others. To opt out, the customer usually has to call a toll-free number or mail in a response card indicating the consumer's opt-out choice. Even if customers take the initiative and exercise their limited opt-out rights, they must trust the financial services company to honor the request and maintain adequate security procedures to prevent unauthorized sharing and access.

Financial institutions cannot disclose customer account numbers or access codes to a non-affiliated third party for use in marketing activities. Thus, even if customers do not opt out of an information sharing arrangement with non-affiliates, credit card and debit card numbers, PINs, and account passwords cannot be sold.

The GLBA also requires financial services companies to develop systems to ensure that customer information is secure against "hacking" and other unauthorized access. The law also prohibits certain kinds of "pretexting," the practice of collecting personal information under false pretenses. Pretexters pose as law enforcement officials, social workers, potential employers, bank personnel, or other parties and create convincing stories in order to elicit information from unsuspecting businesses and consumers. The GLBA criminalizes the use of fraudulent statements to solicit financial information.

To apprise customers of the privacy practices of a business, the GLBA requires financial institutions to provide customers with notices that explain how



the company handles personal information and shares it with others. The notice must be clear and conspicuous and must accurately describe the firm's privacy practices. It must explain, in general terms, what information the company collects, with what other companies it shares the information, and how it safeguards its databases. The notice must be given to customers by mail or through another in-person method of communication. Acceptable ways of communicating this information depend on the type of business. For example, an online lender may post its privacy policy on its website and require that the customer acknowledge its receipt before applying for a loan. The dissemination of privacy notices or privacy policies in the financial services industry is now commonplace.

The GLBA exempts several categories of transactions from its privacy protections. Financial institutions can disclose customer information with credit reporting agencies, government regulatory agencies, and a company that is purchasing the business. They can also share information with outside firms that provide essential services, such as data processing, check printing, or mortgage servicing, and with firms that agree to jointly market the company's products and services. These exceptions allow much information to be shared without consumer knowledge or consent.

The GLBA applies only to "nonpublic" personal information—data that cannot be obtained from sources in the public domain. Most of the information about customers in a financial institution's database is nonpublic, but information that is publicly available, such as a mortgage loan recorded in the public records, is not covered by the GLBA.

The Fair Credit Reporting Act (FCRA), which protects the privacy of consumer information held by credit bureaus, also governs certain transactions involving banks and other financial institutions. Under the FCRA, credit reporting agencies (credit bureaus) can release the credit reports of consumers to financial institutions when individuals apply for credit, open bank accounts, or initiate other financial transactions. When a financial company obtains a credit report, it may want to share the report with an affiliated business. Under the FCRA, the credit report cannot be shared with affiliates unless the consumer has first been notified and given the opportunity to opt out. This is similar to the opt-out right under the GLBA, and the opt-out notice is likely to be included in the privacy policy delivered to the customer under the GLBA. However, unlike the case with the GLBA, consumers who exercise their opt-out rights under the FCRA can prevent the sharing of information among affiliates, but only information obtained from a credit report that has been issued by a credit reporting agency.

See also: **Digital cash**

Suggested Reading: Cate, Fred H., Robert E. Litan, Michael Staten, and Peter J. Wallison. *Financial Privacy, Consumer Prosperity and the Public Good*. Washington, DC: Brookings Institute, 2003; Electronic Privacy Information Center. *Right to Financial Privacy Act*. www.epic.org/privacy/rfpal/. Online, March 2006; Fischer, Richard L. *The Law of Financial Privacy*. Washington, DC: A.S. Pratt & Sons, 2002; Gandy, Oscar. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press, 1993; Garfinkle, Simson. *Database Nation*. New York: O'Reilly, 2000; Regan, Priscilla. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina

Press, 1995; Rubin, Paul H., and Thomas M. Lenard. *Privacy and the Commercial Use of Information*. Amsterdam: Kluwer Academic Publishers, 2002; Scousen, Mark. *The Complete Guide to Financial Privacy*, 4th ed.. New York: Simon & Schuster, 1983; Smith, Jeff H. *Managing Privacy: Information Technology and Corporate America*. Chapel Hill: University of North Carolina Press, 1994.

James P. Nehf

Bank Secrecy Act

The United States Congress enacted the Currency and Foreign Transactions Reporting Act, more commonly known as the Bank Secrecy Act, in 1970. This legislation requires banks and other financial institutions to report information on their customers to the federal government. This information is to be collected and transmitted, without the knowledge or consent of customers, whenever the financial institution detected “suspicious activity.” Financial institutions are required to report transactions over \$10,000 in cash to the Treasury Department by means of the Currency Transaction Report. Once this information is filed, it becomes available to most law enforcement agencies through the Financial Crimes Enforcement Network (FinCEN) of the Treasury Department. Information posted on FinCEN can be accessed by law enforcement agencies without a requirement of probable cause. This means that there is no need for a judge to issue a **search warrant**, court order, or subpoena for this information.

The original intent of the Bank Secrecy Act was to identify the source and dollar amount of any transaction consisting of currency or other monetary instruments coming into or leaving the United States. The purpose of having financial institutions track these transactions was to create an audit trail with the Treasury Department to allow the apprehension and prosecution of individuals involved in the act of money laundering or tax evasion. Although the act left the responsibility of reporting these types of suspicious activities with the individual financial institutions, subsequent legislation created additional regulation with regard to these activities.

The Money Laundering Control Act was passed in 1986 to provide for criminal prosecution of those employees of financial institutions who aid in the laundering of money. Penalties can be imposed on employees who either assist in the act of laundering money or circumvent the reporting procedures by creating several smaller transactions that avoid the reporting requirements set by the Bank Secrecy Act. These penalties were strengthened by additional legislation in 1992 and 1994 requiring all financial institutions to institute policies designed to educate their employees with the goal of achieving full compliance with the legislation. Due to different interpretations by different financial institutions, it was recognized in 1996 that there was a need to standardize the information collected. This resulted in the creation of the Suspicious Activity Report, to be used by all U.S. financial institutions. This report is filed any time a financial institution believes that a transaction has been made that violates U.S. law or is just suspicious in nature.

In reaction to the events of September 11, 2001, Congress passed the **Uniting and Strengthening America by Providing Appropriate Tools Required to**



Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act). Title III of the act, called the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, added the most power to the Bank Secrecy Act since its inception in 1970. Financing of terrorist activities could be fought by such measures as prohibiting financial institutions in the United States from doing business with foreign shell banks, improving cooperation and information sharing among institutions, and creating more rigorous customer identification procedures.

With the modifications made to the original Bank Secrecy Act, the number of federal and state law enforcement agencies utilizing the reports generated about suspicious activity has increased tremendously. These agencies include the U.S. Treasury, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, and several international organizations, to name just a few. However, the role of gatekeeper of this information remains with FinCEN. FinCEN has been given the authority to post regulations and interpretive guidance and to pursue civil cases against violators as necessary. FinCEN relies on the federal banking agencies to examine banks within their areas of responsibility for compliance with the policies and procedures set up under the Bank Secrecy Act and subsequent legislation.

Since the inception of the Bank Secrecy Act the reasons for gathering information on financial transactions have changed, although the overall process has remained constant. In the War on Drugs, information gathered through this act has assisted in identifying, detaining, and prosecuting individuals involved in money laundering. In conjunction with the Drug Enforcement Agency, and with the cooperation of foreign governments, many individuals involved in narcotics trafficking have been identified and their networks destabilized. Now, amidst the “War on Terror,” the focus remains on the flow of money to groups who wish to harm others, albeit in a different way.

However, drug dealers and terrorists are not the only focus of law enforcement efforts utilizing this information sharing capacity. Corrupt businesses, politicians, and others seeking to benefit from fraudulently exploiting others also use money laundering. Such entities and individuals can adversely affect the securities markets, as shareholders are essentially being robbed of their assets without their knowledge. This can make their stock worthless and cause the markets to tumble.

Whether by preventing criminals from funneling funds to terrorists and drug dealers or preventing corrupt business people and politicians or other individuals from defrauding citizens and shareholders, the goal of this legislation is to help maintain trust in the financial markets of the United States. By monitoring information on who is making large monetary transactions and combining that information with other sources, the Department of the Treasury can track criminal activity and protect the general population.

See also: **Banking and financial records; Financial Services Modernization Act of 1999**

Suggested Reading: Etzioni, Amitai. *How Patriotic Is the Patriot Act? Freedom versus Security in the Age of Terrorism*. New York: Routledge, 2004; Federal Deposit Insurance Corporation. *Bank Secrecy Act and Anti-Money Laundering*. www.fdic.gov. Online, December 2005; Hyde, Lorraine. *Bank Secrecy Act and*

Anti-Money Laundering Service. Austin, TX: Sheshunoff & Co., 1996; Powis, Robert E. *Bank Secrecy Act Compliance*, 5th ed. New York: McGraw-Hill, 1996.

Christine Berry Lloyd

Bar code readers and scanners

A bar code scanner was first used in 1974, when a pack of Wrigley's chewing gum was scanned in an Ohio supermarket. Since then this technology has proliferated to include over 300 different bar codes now used for inventory control, tracking of hospital patients, prescription drug labels, library checkout, and even **DNA** coding. The privacy issues relating to bar codes pertain to what information is collected and to what uses this information is put.

The basic technology in bar code scanning involves an electromagnetic laser scanner that produces a beam of light. The light is shone on a bar code tag that consists of lines and spaces of varying thickness and printed in different combinations. The bar code is a linear binary code of 1s and 0s. The light hits the bar code and is reflected by the white portions of the code while being absorbed by the black lines. The reflected portion is sensed by a detector in the scanner, which converts it to an electrical signal. This signal is then translated into the binary language of the computer, a string of 0s and 1s. A computer, either on-site or central, matches the code to the item name. The main benefits of bar codes are speed and efficiency. For instance, entering 12 characters of data on a keyboard takes 6 seconds whereas scanning a 12-character bar code takes 0.3 second.

The first bar coding system was the Universal Product Code (UPC). This coding is now ubiquitous in retail markets. The information from bar codes is used by retail managers to monitor customer purchases and respond instantly to changes in demand. In some cases information on purchases is electronically transmitted to the distributor, who uses it to instantly restock products. The bar code also allows stores to track customer buying patterns when it is coupled with the demographic information associated with supermarket loyalty cards.

The basic bar code, like the Universal Product Code, is vertically redundant, meaning that information is repeated vertically. Newer bar code technologies include two-dimensional codes that store information along the height as well as the length of the symbol. The 2-D symbol can be read with a handheld moving-beam scanner by sweeping the horizontal beam down the symbol and can include an expanded amount of information. This technology was originally designed for items with space limitations but has expanded to include applications where the ability to encode a portable database makes it attractive to businesses. For example, storing name, address, and demographic information on direct mail business reply cards allows businesses to immediately access demographic information rather than check it against a larger database.

Two-dimensional bar codes are now used on driver's licenses in about 30 states. Included in the information on these codes is not only what is listed on the front of the driver's license, but also **biometric identifiers**. For example, a Georgia license stores two digital **fingerprints** as well as the person's signature. A Tennessee driver's license stores a facial recognition template. Kentucky recently has embedded a black-and-white electronic version of the driver's photograph in the bar code.

This information can be accessed by private individuals who purchase the appropriate bar code scanner. For example, bars and convenience stores use this technology to monitor age for alcohol sales and also to capture customer information not only for marketing purposes but also for denying sales to disagreeable patrons. Privacy rights activists charge that the information encoded on the driver's license creates a de facto **national identity card** that can be registered in many databases.

There are instances where the information from bar codes has had significant consequences. The government of the German Federal Republic in the 1970s used bar code technology to check civil servants' political leanings by tracking their borrowing of politically questionable books from the public library. This simple cataloging technique thus has become an instrument of governmental control, a development that has contemporary relevance in the United States in conjunction with the provisions of the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)**. Bar codes in this context have the potential to undermine civil liberties and the right to privacy.

The newest generation of bar code is the **radio frequency identification tag** (RFID). This tag contains tiny computer chips linked to a small antenna. Devices called readers detect information from these tags using radio wave transmitters when the tag moves into the range of the reader. This technology is being developed for retail use as well as for government documents such as passports and elementary school ID cards. Privacy activists worry that because this type of technology allows signals to be read from hundreds of feet rather than being scanned at the point of the card, personal information is much more vulnerable and the **surveillance** capacity of computer chips is broadened as they are brought into individual residences. The amount of information that can be stored on these chips is much greater compared with conventional bar codes.

Suggested Reading: Altheide, David L. "An Ecology of Communication: Toward a Mapping of the Effective Environment." *Sociological Quarterly* 35 (1994): 665–683; The Barcode Source. www.barcoderesource.com. Online, March 2006; Garfinkle, Simson. *Database Nation*. New York: O'Reilly, 2000; Moore, Adam D. *Information Ethics*. Seattle: University of Washington Press, 2005; Rubin, Paul H., and Thomas M. Lenard. *Privacy and the Commercial Use of Information*. Amsterdam: Kluwer Academic Publishers, 2002.

Shelley L. Koch

***Bartnicki v. Vopper*, 532 U.S. 514 (2001)**

During contentious collective-bargaining negotiations between a Pennsylvania high school teachers' union and the local school board, Bartnicki, the chief union negotiator, and Kane, the union president, had a conversation on a **cellular telephone** that was intercepted and recorded by an unidentified person. A nonbinding arbitration proposal, generally favorable to the teachers, had all but settled the dispute, when Vopper, a radio commentator critical of the unions, played the tape of the intercepted conversation on a segment of his public affairs talk show dedicated to covering the settlement. The tape was subsequently aired on another station and its content was published in the local newspapers. In the recorded conversation, Bartnicki and Kane discussed the timing of a proposed strike, the difficulties created by

public comment on the negotiations, and the need for a dramatic response to the school board's intransigence.

Bartnicki and Kane filed suit against Vopper and other members of the media. It was discovered that Vopper obtained the tape from Jack Yocum, the head of a local taxpayers' association opposed to the union's demands. Yocum testified that he discovered the tape in his mailbox. When he played it, he recognized the voices of Bartnicki and Kane. He played it for the school board and then delivered it to Vopper, as well as to other individuals and media representatives. Both parties sought summary judgment. Bartnicki alleged that each of the defendants who aired or published the contents of the tape "knew or had reason to know" that the recording of the private phone conversation had been obtained in violation of both federal and state **anti-wiretap statutes**. Bartnicki sought actual damages, statutory damages, punitive damages, and attorney's fees. The defendants argued that there was no violation because (1) if the interception was illegal, the defendants had nothing to do with the it; (2) the conversation might have been intercepted inadvertently, not illegally, and therefore the defendant's actions were not unlawful; and (3) if the defendants had violated the statute by disclosing the conversations, the **disclosures** were protected under the First Amendment and the defendants were not liable for damages. The district court found that the defendants had clearly violated the statute; they "knew or had reason to know" that the information was obtained through an illegal interception. Actual involvement in the illegal interception was not required. However, whether the interception was inadvertent was a disputed fact, so summary judgment was denied. The court did, however, grant a motion for an interlocutory appeal, which sought an answer to the following questions of law: "(1) whether the imposition of liability on the media defendants under the [wiretapping] statutes solely for broadcasting the newsworthy tape on [Vopper's] radio news/public affairs program, when the tape was illegally intercepted and recorded by unknown persons who were not agents of [the] defendants, violates the First amendment; and (2) whether imposition of liability under the [anti-wiretapping] statutes on Defendant Yocum solely for providing the anonymously intercepted and recorded tape to the media violates the First Amendment."

All parties agree that the wiretapping statutes are content-neutral laws of general applicability. They do not seek to discriminate against any particular speech content or single out a particular viewpoint; they seek to protect privacy. A content-neutral regulation is subject to the "intermediate scrutiny standard"; that is, it will be sustained under a First Amendment challenge if it advances important governmental interests unrelated to the suppression of free speech and does not burden substantially more speech than necessary to further those interests. The Court of Appeals for the Third Circuit determined that under this standard, the wiretapping statutes were invalid because they deterred significantly more speech than necessary to protect the privacy interests at stake. Bartnicki appealed.

The United States Supreme Court granted certiorari. It accepted the following findings of facts: (1) The conversation was intercepted illegally (i.e., in violation of the wiretapping statutes). (2) The defendants violated the wiretapping statutes because they knew or should have known that the conversation was intercepted illegally. (3) The defendants played no part in the interception itself; they obtained the information from the tapes lawfully, even though someone else unlawfully intercepted the

information. (4) The subject matter of the conversation was a matter of public concern. The Court also accepted that (5) the wiretapping statutes were content-neutral laws of general applicability and that intermediate scrutiny was the appropriate standard to apply. The Court was required to determine only whether the application of these statutes, under these particular facts, violated the First Amendment.

The Court began its analysis of this question by setting out general principles of law from previous cases. *Smith v. Daily Mail* held that “state action to punish the publication of truthful information seldom can satisfy constitutional standards.” *Florida Star v. B.J.F.* held that “if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information absent a need . . . of the highest order.” *New York Times v. United States* upheld the publication of documents of great public importance stolen by a third party, focusing primarily on the character of documents’ contents and the consequences of the disclosure. That case, however, did not resolve the issue here: whether the government may punish not only unlawful acquisition of information, but the ensuing publication as well. The Court noted that it had carefully tried to avoid categorical holding of whether publication of truthful information may ever be punished under the First Amendment.

The government argued that two important interests are served by the statute: preventing disclosure deters parties from intercepting private communications, and it minimizes the harm to persons whose private communications have been illegally intercepted. The Court took these up in turn. It opined that the interest of deterrence is insufficient to justify punishing disclosures in this case. The defendants published lawfully obtained information of public interest by someone who was not involved in the initial illegality. While illegal interceptors are usually known, and usually disclose intercepted communications for public praise or financial reward, imposing sanctions on the media in this case will not deter unidentified scanners from such antisocial conduct. The Court found, however, that the government’s interest in minimizing harm to the invasion of privacy was a considerably stronger argument. The wiretapping statutes encourage uninhibited exchange of ideas and information among private parties, and fear of public disclosure might have a chilling effect on speech. Therefore, the statutes may be applied in most cases without violating the First Amendment, in order to prevent disclosures of trade secrets or domestic **gossip**. However, in this case, enforcement of the statute imposes sanctions on the publication of truthful information of public concern, implicating the core purposes of the First Amendment. The Supreme Court held, relying on the general proposition that freedom of expression upon public questions is secured by the First Amendment, that privacy concerns must give way in publishing matters of public importance.

Justice Breyer, joined by Justice O’Connor, concurred in the opinion and agreed with the narrow holding limited to these special circumstances: radio broadcasters engaged in no unlawful act aside from the broadcasting itself, and the information involved a matter of unusual public concern, namely, a threat of harm to others. The concurrence went on to explain why the majority’s opinion should not be read as signifying a broad constitutional immunity to the media.

Justices Scalia and Thomas joined Chief Justice Rehnquist in his dissent. The dissent expressed concern over the loss of privacy signified by the majority’s opinion. It

faulted the majority for limiting the holding to “matters of public concern” without defining that amorphous term. It argued that the majority opinion diminishes the First Amendment rather than enhances it because the opinion will have the effect of chilling the speech of citizens who increasingly rely on electronic technology—cellular telephones and **electronic mail**—to communicate. The dissent found fault with the majority’s reliance on the line of cases it referred to. Further, it disagreed with the majority view that Bartnicki and Kane, by discussing a matter of public importance, somehow were contributing to a public debate and that their privacy interests were subordinate to the disclosure of these statements. The dissent argued that the right to privacy, at its narrowest, must include the right to be free from surreptitious eavesdropping and the involuntary broadcast of cellular telephone conversations.

See also: Katz v. United States, 389 U.S. 347 (1967); *Olmstead v. United States*, 277 U.S. 438 (1928)

Suggested Reading: Alberti, Anthony. *Wiretaps*. Bethesda, MD: Austin & Winfield, 2002; Barte, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black’s Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Diffie, Whitfield, and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press, 1999; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Goodale, James C. *Communications Law*. New York: Practising Law Institute, 1999; Hall, Kermit L. *Conscience, Expression and Privacy: The Supreme Court in American Society*. New York: Garland, 2000; Smith, Robert Ellis. *Compilation of State and Federal Privacy Laws*. Providence, RI: Privacy Journal, 1992.

Larkin R. Evans

***Bauer v. Kincaid*, 759 F. Supp. 575 (1991)**

Traci Bauer was the editor-in-chief of the *Southwest Standard*, a newspaper for Southwest Missouri State University students. She brought an action against Southwest Missouri State University when it refused to release information about criminal occurrences that were committed on the SMSU campus. She claimed that under the Missouri Open Records Act (MORA), the university was obligated to provide all of the information that it collected and maintained regarding criminal activity. The act requires that all public governmental bodies provide all **public records** upon request for the purpose of ensuring that all public meetings would be conducted openly and subject to public examination. It also was intended to provide a record of the decisions that each public official made and to make it available to the public for examination. The act was to be interpreted literally and, unless otherwise protected by law, there could be no exception as to what records were available for general viewing and copying.

The defendants, the Southwest Missouri State University Board of Regents, among others, claimed that under the **Family Educational Rights and Privacy Act (FERPA)**, the school was prohibited from providing the requested documents. FERPA requires that federal funds be withheld from any educational agency that releases records regarding any student without the student’s consent. They also



claimed that SMSU's Safety and Security Department, which maintained the requested files, was not a public governmental body and therefore was not subject to the regulations under MORA.

Using MORA's definition of "governmental body," the district court deemed that the Board of Regents was obligated to surrender the records to the *Southwest Standard*. The university's claim that the records were maintained by the Safety and Security Department was simply an attempt to shield the university from the requirements under MORA. Even if SMSU's Safety and Security Department was not considered a public governmental body, it was under the command of the university's Board of Regents; therefore, the records were subject to MORA. The court ruled that it was unreasonable to believe that the university's Board of Regents did not have any authority or legal control over the Safety and Security Department.

The court specifically responded to the assertion that the university was not required to provide the requested records because it was protected under FERPA. The defendants claimed that "directory information" was the only information that FERPA allowed to be released to the public. The court ruled that FERPA did not provide exemption to the university from the Open Records Act because the information requested was not information that FERPA intended to protect. The protection provided under FERPA covered information that students were required to divulge on applications for admission as well as information on a student's academic progress at the university. There is no mention in the act of the protection of criminal investigation or incident reports conducted under the jurisdiction of the university.

Even if the reports were covered by the act, this would not prohibit the university from releasing them. The act's purpose is to impose penalties on educational entities that release information described in the act. The act does not impose a law that bars schools from releasing information; instead, it allows federal funds to be withheld from schools whose policies permit the release of information. The court ruled that because the information was not directly protected under FERPA, and because the act itself is not binding law, the university was not exempt from the Open Records Act.

The District Court of Missouri ordered the release of all records held by Southwest Missouri State University regarding criminal occurrences on the campus on the grounds that the Board of Regents was a governmental body and therefore was in violation of MORA. Furthermore, the court dismissed the university's argument that FERPA exempted it from producing the requested information because the act was not intended to protect the kind of information being sought by the newspaper.

See also: Associated Press v. Walker, 388 U.S. 130 (1967); *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975); *Journalism; Open Meetings Laws; Red & Black Publishing Co. v. Board of Regents*, 262 Ga. 848 (1993); *Time, Inc. v. Hill*, 385 U.S. 374; *United States v. Caldwell*, 408 U.S. 665 (1972)

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*. 7th ed., St. Paul, MN: West, 1999; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Goodale, James C.

Communications Law. New York: Practicing Law Institute, 1999; Hall, Kermit L. *Conscience, Expression and Privacy: The Supreme Court in American Society*. New York: Garland, 2000; Smith, Robert Ellis. *Compilation of State and Federal Privacy Laws*. Providence, RI: Privacy Journal, 1992.

Sean M. Peek

Big Brother

“Big Brother” is a fictional character in George Orwell’s novel *Nineteen Eighty-Four*. In the book Orwell, the pen name of the English writer Eric Blair (1903–1950), depicts a dystopian futuristic society deprived of privacy, freedom, and history and controlled with the use of totalitarianism, terror, and dehumanizing practices. These practices include a variety of ubiquitous physical and mental surveillance techniques that penetrate every aspect of the society. It is through **surveillance** that privacy is obliterated and people are reduced to numbers. A phrase that appears throughout the text, “Big Brother Is Watching You,” symbolizes the apocalyptic relationship between a dehumanizing system of surveillance serving the needs of the oligarchic political regime, and the destruction of personal privacy.

The main protagonist, Winston Smith, introduces us to the society, where private and public locales are continuously monitored by devices referred to as “telescreens.” Whether positioned in an apartment, a house, an office, or an open public space, the telescreens can always watch you. What’s more, the telescreens are not merely recording cameras, but they are also the medium for instructing individuals on what they must do on a daily basis: wake up at a certain time, exercise more vigorously in the morning, or report to a particular state-run Ministry. In addition, the telescreens are technically capable of detecting subtle changes in an individual’s words, facial expressions, intensity of breathing, or even the heartbeat. If any of those basic factors are not satisfactory to the state inquisitors, whom Orwell pointedly calls the “Thought Police,” the targeted individual may be imprisoned, tortured, or, if confessing to nonexistent crimes against the state and the party, put to death and erased from all records. Big Brother’s picture is displayed all over Oceania: he is the embodiment of the party, the system, and the state. His presence is encountered on public buildings, in the restrooms, above the bed. “Big Brother Is Watching You,” asserts Orwell, adding, “Even from the coin [his] eyes pursued you. On coins, on stamps, on the cover of books, on banners, on posters, and on the wrapping of a cigarette packet—everywhere. Always the eyes watching you and the voice enveloping you. Asleep or awake, working or eating, indoors or out of doors, in the bath or bed—no escape. Nothing was your own except the few cubic centimeters inside your skull.”

Yet even within the people’s minds, privacy is significantly reduced. An individual’s thought process is continuously intruded on by state-imposed rituals such as the “Two-Minute Hate,” a practice where individuals stare and yell at the telescreens showing “prominent” enemies of the state. There is also “Doublethink,” the practice of holding two opposing thoughts at the same time and accepting both of them, the altering of commonsense conclusions (e.g., $3 + 2 = 4$), and the perpetual search for the “internal” and “external enemies” amidst the never-ending state of war. These daily exercises reinforce the fear and mistrust among the population, justifying

surveillance as necessary and defining privacy as obsolete, unpatriotic, and potentially incriminating.

If one's privacy could at least be legally defined, defended, and asserted in a court of law, the reassertion of basic human rights would be possible. However, "in Oceania there is no law," so the actions and behaviors that the state's *apparatchik* machinery monitors are never legally regulated. As a result, every individual's act or behavior is potentially criminal and severely punishable.

Can individuals at least think of privacy in *Nineteen Eighty-Four*? Can they formulate simple thoughts of what it means to have privacy? Even that possibility is tragically decimated in the course of the novel because the vernacular that could express and formulate these thoughts is systematically destroyed. The English language, referred to as "Oldspeak," is systematically replaced with a language referred to as "Newspeak" in which words are reduced to codes without meanings. The result is a society of individuals who are without the capacity to think, or even to contemplate any alternative since there are no words to express such a scenario. While having a lunch with one of the contributors to the latest "Newspeak" dictionary, Winston Smith is told, "Don't you see that the whole aim of Newspeak is to narrow the range of thought? In the end we shall make thoughtcrime [contemplation of a crime] literally impossible because there will be no words in which to express it."

But even without the spoken language, an individual must be able to remember the past, to verify the memories of what it means to be a human, to retain a sense of what it meant to have privacy, based on written records. But alas, not so in Oceania, says Orwell. The entire society is constructed around perpetual falsification, manipulation, adjustment, and surveillance. Who is fighting with whom in the ongoing war changes depending on the alliance at any given time. The records change too, creating the "verifiable" illusion that the past corresponds to the present, whatever that present is determined to be. A person in Oceania does not simply die after incarceration, trauma, torture, confession, and humiliation, but rather is "vaporized" both physically and from all records that would testify as to his or her existence. As one of the protagonists explains to Winston Smith, the entire process of controlling and monitoring the population depends on the simple maxim "who controls the past, controls the future." For Winston Smith, however, "the past was dead, the future was unimaginable."

Even **family** and kinship relationships are scrutinized and controlled. The kids report their parents to the police. Sex is understood to be "dirty" and as having value only as a purely reproductive act. The most intimate conversations between spouses dealing with love, the future, sex, and other such subjects are self-censored. "The family has become an extension of the Thought Police. It [became] a device by means of which everyone could be surrounded night and day by informers who know him intimately." For Winston Smith, this is one of the most devastating developments: without intimacy and privacy, even the sense of tragedy is beyond the realm of human experience, for, as he perceives, "tragedy belonged to the ancient time, a time where there was still privacy."

Orwell's novel unambiguously connects the practice of surveillance and the obliteration of privacy to some technological aspects of modernity. The leaders of previous eras were simply not equipped to enslave populations at the level the

Orwellian society does. Newspaper, film, television, and other technical advances of the modern era, in the hands of a lawless, dictatorial regime, suddenly became surveillance tools canceling the possibility of a private life.

Yet Orwell sees modern phenomena such as class rebellion and rationality based on the fundamental principles of the Enlightenment as the only way out of the totalitarian nightmare. The Proles—constituting the majority of the population in Oceania, kept under loose control by the authorities and ostracized through poverty, disease, and ignorance—is the only group capable of effectively rebelling against the Party if only it could regain the consciousness of its own strength, if only the Proles were to understand that they are “the only remaining humans.” Moreover, if individuals were to unequivocally reestablish the right to assert the basic premises of the everyday truth, the rest would follow and the dictatorship would fall—none of which happens in the novel.

George Orwell died in 1950. More than a half century after his death, *Nineteen Eighty-Four* is still read as fiction, but its message is feared as the tantalizing account of a world we do not want to wake up to, or recognize around us.

See also: **Privacy, definition of; Privacy; Philosophical foundations of; Secrecy**

Suggested Reading: Connelly, Mark. *Diminishing Self: Orwell and the Loss of Freedom*. Pittsburgh: Duquesne University Press, 1987; Cushman, Thomas, and John Rodden (eds.). *George Orwell: Into the Twenty-first Century*. Boulder, CO: Paradigm, 2004; Gleason, Abbott, Jack Goldsmith, and C. Martha Nussbaum (eds.). *On Nineteen Eighty-Four: Orwell and Our Future*. Princeton, NJ: Princeton University Press, 2005; Huber, Peter. *Bye-Bye, Big Brother*. Charles’ George Orwell Links, www.netcharles.com. Online, May 2005; Larkin, Emma. *Finding George Orwell in Burma*. New York: Penguin Press, 2005; Rai, Alok. *Orwell and the Politics of Despair: A Critical Study of the Writings of George Orwell*. New York: Cambridge University Press, 1988.

Uros Petrovic

Bill of Rights. *See* **Constitutional protections**

Biometric identifiers

Biometric identification, or biometrics, is the practice of using physical information to link individuals to databases or to other stored identity information. “Biometric” literally means “bodily measurement” and is increasingly being touted as a solution to security problems in the post-9/11 world. Proponents claim that biometrics has the potential to simultaneously enhance security and privacy. At the same time, biometrics raises Orwellian concerns about facilitating the growth of a “surveillance society.”

Early prison records often recorded an individual’s height and other physical characteristics, and photographs could also be considered a form of biometric information. Perhaps the first full-fledged biometric (called “anthropometric” at the time) identification system was the criminal identification system devised by Paris police official Alphonse Bertillon around 1883. Bertillon applied the tools of anthropometry to the problem of criminal record keeping. His system used 11 precise bodily measurements (such as head length and width, foot length, and even ear

length), detailed physiognomic description, and meticulous notation of “peculiar marks” such as tattoos, birthmarks, and scars. All of this information was entered on index cards, which were filed according to a classification system based on the anthropometric measurements. “Bertillonage,” as it was called, thus contained many of the key features we now think of as constituting a biometric identification system. It was a database of records that were retrievable according to biometric information alone (as opposed to requiring a correct name to be submitted).

A number of different physical attributes have been proposed or used for biometric identification. The most common biometric identifiers are the face, **fingerprints**, iris, anthropometrics, hand geometry, voice, and signature. Less common biometrics include the retina, veins in the palm, skull **x-ray**, tattoos (voluntary or required), gait, body odor, ear shape, skin reflectance, body heat patterns, lip motion, and keystroke dynamics.

James Wayman has proposed that biometric applications be categorized according to how they fall along several dimensions. The user may be cooperative (an employee) or noncooperative (a criminal). The biometric system may be overt (known to the subject) or covert. Users may be more or less well habituated to using the system. The system may be attended (by an operator) or unattended. The use environment may be standard or extreme. The system may be controlled by a public or private entity. And the system architecture may be open (compatible with other systems) or closed.

Biometric applications may usefully be sorted into two categories. In *verification*, a user’s claim to be a particular individual is verified. In *identification*, an individual not claiming particular identity—or whose claim is questionable—has his or her identity determined by comparison of biometric information with that stored in a database.

Potential or existing applications of biometrics include criminal record keeping, immigration control, document security (for driver’s licenses, passports, etc.), voter authentication, protection of access to entitlements or other government payments, creation of databases of political asylum seekers and refugees, medical record keeping, banking (including its use on ATM cards), shopping (including its use on **smart cards**), workplace monitoring, controlling access to secure areas, guarding access to personal property such as an automobile or a laptop computer, and surveillance of airports or other public spaces to identify wanted individuals or potential terrorists. For many of these applications, biometrics is a potential replacement for less secure methods of authenticating identity, such as identification cards or numbers and “secret knowledge,” such as **passwords** or **personally identifiable information** such as one’s mother’s maiden name. There is, in addition, a growing field of “e-world” biometric applications, including such areas as e-commerce.

Biometric identification raises a number of privacy issues. Civil libertarians tend to view biometrics with suspicion. It is seen as having the potential to facilitate the rise of a surveillance society, and possibly even totalitarianism. Covert biometrics, such as face recognition, invokes privacy debates about whether citizens have any reasonable expectation of privacy for readily visible biometric information. These same arguments apply to “shed” biometric information, such as fingerprints or **DNA**. Other criticisms address biometrics’ inherent reduction of the person to stored information as somehow dehumanizing, raising objections on human rights

or even, with reference to the Book of Revelation, religious grounds. (Another religion-based privacy issue is whether women who wear burkhas must unveil their faces for driver's license photographs.) Additional concerns include whether the biometric profile contains information that might be abused by the government, such as heredity, race, ethnicity, **gender**, or behavioral characteristics.

Other experts have argued that biometrics has the potential to enhance both privacy and security. They argue that replacing insecure identification technologies such as identification cards, passwords, and "secret knowledge" with more secure biometric identifiers, which are more difficult to forge or steal, puts individuals' information more securely in their control. Although biometric markers are certainly difficult to forge or steal, there have been reports concerning such potential abuses as creating a rubber mold of another person's fingerprint pattern. Both real and fictional scenarios exist concerning the "stealing" of biometric information by forcibly removing the relevant body part(s). A potential counter-measure to this is requiring the sensor to detect a certain amount of heat.

Given its enormous potential, biometrics is certain to be an important focus of privacy issues for years to come.

See also: **Authentication; Automated Teller Machine (ATM); DNA and DNA banking**

Suggested Reading: Agre, Philip E. *Your Face Is Not a Bar Code: Arguments against Automatic Face Recognition in Public Places*. UCLA Information Studies Department (2003), <http://polaris.gseis.ucla.edu/pagre/bar-code.html>. Online, March 2006; Biometric Consortium. www.biometrics.org. Online, March 2006; Biometrics Institute. www.biometricsinstitute.org. Online, March 2006; Bolle, Ruud, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, and Andrew W. Senior. *Guide to Biometrics*. New York: Springer-Verlag, 2004; National Institute of Standards and Technology. The Biometrics Resource Center, www.biometrics.org. Online, March 2006; Torpey, John, and Jane Caplan (eds.). *Documenting Individual Identity: The Development of State Practices since the French Revolution*. Princeton, NJ: Princeton University Press, 2001; Van Der Ploeg, Irma. *The Machine-Readable Body: Essays on Biometrics and the Informatization of the Body*. Maastricht: Shaker, 2005.

Simon A. Cole

Birth certificate

Birth certificates in the United States, which are issued by the states, have two different sections, and each section involves different privacy concerns. The first section, the legal record of the birth, is always available to the adult whose birth it registers; access by other persons varies widely from state to state, ranging from a short list of specified relatives to the public at large. The second section of the certificate—which records health and medical information about the parents, the birth, and the infant—is used only for data collection and analysis, under regulations that protect the privacy of the registrants and their parents.

It was only in the first half of the twentieth century that birth registration in the United States became both standardized and nearly universal. In colonial times a number of the colonies passed laws requiring government officials to record births and other vital events, but even with the passage of additional regulations over time, these laws and the systems they established were not highly effective. Until



the early 1800s birth certificates were used only for legal and historical purposes, not for the additional public purpose of collecting and analyzing health and demographic data. Birth registration evidently was not a priority in a nation experiencing a high volume of both immigration and internal migration. In the mid-1800s, however, a growing emphasis on the importance of vital statistics for public health purposes led the American Medical Association (AMA) to urge the states to collect vital statistics. By 1859 eight states had established birth registration systems, and after the Civil War more states followed, although under-registration of births continued to be widespread.

Because birth registration was so inadequate, efforts before 1900 to collect data on births focused on the decennial census. After 1900 efforts to obtain birth statistics shifted from the census, which proved unsatisfactory for the purpose, to the ultimately more promising source of birth registration by state and local governments. To develop standards for registration legislation and practices, the Bureau of the Census, which was established as a permanent office in 1902, worked with the American Public Health Association (APHA). In addition to issuing such standards, the bureau in 1903 published a recommended standard birth certificate, which has been followed by 12 revised versions, the latest in 2003. The bureau in 1907, working with the AMA, the APHA, and other organizations, also developed and recommended to the states a model vital statistics law. Four versions of the model law have been issued since then, the latest in 1992.

At first, the Bureau of the Census made great progress in the registration of deaths, but in 1915 it established a national "birth-registration area," a group of 10 states and the District of Columbia in which birth registration was the most complete and therefore the most reliable source of statistics. Significant efforts to improve birth registration at this time resulted in part from an increasing desire to collect statistics that could be used to help reduce infant mortality. In addition, birth certificates were becoming more important to individuals for uses such as establishing age for entering school and obtaining work permits. Ten additional states were found to have sufficiently complete birth registration systems as of 1917 and were admitted to the birth-registration area. By 1933 every state was included. During the 1940s birth certificates became increasingly important to individuals for establishing citizenship for jobs in defense, applying for food ration books, and qualifying for military family allowances. From 1935 to 1948, the estimated prevalence of birth registration rose from 90.7 to 95.5 percent.

Today the responsibility for collecting and publishing birth-related and other vital statistics is vested in the National Center for Health Statistics (NCHS), a part of the Centers for Disease Control and Prevention (CDC), which is part of the U.S. Department of Health and Human Services (HHS). The states generally match the federal government's recommended standard certificate. The demographic information on the birth certificates is provided by mothers at the time of birth, while the medical and health information is drawn from medical records. Typically, the certificates are filed with a local registrar, who in turn files the records with the state vital statistics office. The state office, which maintains files of and issues copies of the certificates, transmits the data to the NCHS for analysis and publication.

The top portion of the 2003 U.S. Standard Certificate of Live Birth, which is the formal title of the legal record of birth, includes the child's name, sex, and time and place

of birth. It also includes the mother's current legal name, her name prior to her first marriage, the date and place of her birth, and her residence. In addition, it includes the father's current legal name and the date and place of his birth. (A section for administrative use includes such information as the mother's mailing address, whether the mother was married at the time of the "birth, conception, or any time between," the mother's and father's **Social Security numbers**, and whether a Social Security number was requested for the child.) A medical professional's or hospital administrator's signature is required. Copies of this portion are used extensively for employment purposes; for obtaining other documents, such as driver's licenses, passports, and Social Security cards; for enrolling children in school; for determining eligibility for public benefits; and for confirming age eligibility for sports and other activities.

The federal government recommends that states provide limited **confidentiality** with regard to the record of birth by restricting access for 100 years after the birth to close relatives and others who have a legitimate need for the information. Restricting access also decreases the possibility of identity theft by fraudulent use of the certificates. A certified copy of the legal record portion, according to the provisions of the most recent Model State Vital Statistics Act and Regulations, is to be considered the same as the original and is to be provided upon application to the person whose birth it registers; or the person's spouse, child, parent, or guardian; or any of these persons' authorized representatives. Relatives doing genealogical research may obtain copies if the registrant is deceased. Other persons may be authorized to obtain copies if they demonstrate that the copies are needed to determine or protect their personal or property rights, and a state may designate regulations that further define who may obtain a copy. Governmental agencies may be provided copies solely for use in conducting official duties, and a court of competent jurisdiction may authorize inspection of the record. When individuals apply for a copy, the state registrar or local custodian may require identification or a sworn statement. The record becomes public 100 years after the date of the birth. Stricter controls than these, and more uniformity among the states, will likely be sought in the future as a result of increasing concern about **identity fraud** and international terrorism.

In many states, law and practice now differ to a greater or lesser degree from the federal recommendations. In a number of states, members of the public can view or purchase an uncertified, informational copy of a birth certificate if they know the name and the birth date of the person whose birth it records. Such public access was available in 14 states according to an HHS Inspector General's report published in 2000. With regard to the security of birth certificates in states with restricted access, this report noted that proof of identification was required for "walk-in requests" for copies in only 30 states in the state's main office and in only 19 states in local offices; proof of identification was required for requests by mail in only 11 states and by local offices in only 7 states.

Among the states with restricted access, there is considerable variety in the particulars of their restrictions. Relatives who may obtain copies range from the registrant's parents only to a list that includes, in addition to the parents, the children, siblings, half-siblings, stepparents, stepchildren, grandparents, great-grandparents, grandchildren, and great-grandchildren. Some states permit greater access if the registrant is deceased and the person applying for the certificate submits proof of the death. Some states permit greater access when the applicant is conducting



genealogical research. Although a number of states have adopted the rule that birth certificates become public after 100 years, many states do not allow certificates ever to become public, whereas others have adopted shorter or longer periods—such as 50, 75, or 125 years—before the certificates become public records. A few states impose special restrictions for access when birth certificates indicate that the child was born to unmarried parents.

The portion of the certificate containing health and medical information was made a separate section in the 1949 revision of the standard certificate, which also placed the information about the child's legitimacy in this more confidential section. Labeled "Information for Medical and Health Purposes Only," the current version of this section includes 29 questions, many with a checklist of possible answers. For the mother and father, the information includes education, race, and type of Hispanic origin. Other questions concern the facility where the birth occurred; the attendant at the birth; and many details about the mother's pregnancy and prenatal care, the delivery, and the condition of the newborn.

The current model federal law and regulations require that when information that identifies individuals is disclosed to researchers, all **disclosures** must be made pursuant to agreements that protect the confidentiality of the information. There are no restrictions, however, on the release of information that does not identify individuals. As is the case with the legal record portion of the certificate, government officials may be furnished with the information for use in conducting their official duties, but this information is not subject to subpoena or court order and is not admissible in court. Although the specific laws and procedures that the states have adopted vary considerably, the laws of all the states are designed to protect the confidentiality of this health and medical information.

See also: **Adoption; Health Privacy; Public Records**

Suggested Reading: Hetzel, Alice M. *U.S. Vital Statistics System: Major Activities and Developments, 1950–95*. Hyattsville, MD: U.S. Department of Health and Human Services, National Center for Health Statistics, 1997. <http://www.cdc.gov/nchs/data/misc/usvss.pdf>. Online, March 2006; National Center for Health Statistics. *Model State Vital Statistics Act and Regulations*. Hyattsville, MD: U.S. Department of Health and Human Services (1994). <http://www.cdc.gov/nchs/data/misc/mvsact92b.pdf>. Online, March 2006; National Center for Health Statistics. *Revisions of the U.S. Standard Certificates of Live Birth and Death and the Fetal Death Report* (2003). http://www.cdc.gov/nchs/vital_certs_rev.htm. Online, March 2006; Office of the Inspector General. *Birth Certificate Fraud*. U.S. Department of Health and Human Services (2000). <http://oig.hhs.gov/oei/reports/oei-07-99-00570.pdf>. Online, March 2006; Shapiro, S. "Development of Birth Registration and Birth Statistics in the United States," *Population Studies* 4 (1950): 86–111.

Elizabeth J. Samuels

Birth control

Birth control, a term coined by Margaret Sanger in the early 1900s, refers to the use of contraception to prevent pregnancy. Decisions about whether or not to use birth control, and what kind, seem to be individual issues and yet have a very public dimension. American's beloved "right to privacy" has its judicial roots in issues

of reproductive rights and birth control. In 1881 the Michigan Supreme Court ruled that a woman “had a legal right to the privacy of her apartment” when she was in labor, after she sued her physician for allowing a jeweler to attend the birth. Furthermore, the “**right to be let alone**” became judicially constituted in 1965 in the historic case of *Griswold v. Connecticut*, 381 U.S. 479 (1965). Prior to that, the dissemination of birth control was illegal.

Birth control, in various forms, has existed for centuries. However, technological advances in the nineteenth and early twentieth centuries pushed the issue into the public sphere. Prior to the nineteenth century, white American women averaged seven births over a lifetime. By 1900 this rate had dropped to three and a half births as a result of increasing medical information regarding conception and contraception. Information about birth control was considered inappropriate, and temperance and anti-vice groups advocated the prohibition of such materials and any associated information. In 1873 their attempts met with some success when Congress passed the Comstock Law. This law declared all information and devices associated with birth control to be obscene and classified the dissemination of birth control information or products via the federal mail as criminal. Anthony Comstock, head of the New York Anti-Vice League, became a special federal agent responsible for preventing the distribution of such “obscene” materials. Additionally, Comstock’s efforts resulted in the passage of anti-contraception laws in 22 states, with the most repressive ones in Connecticut and Massachusetts.

In 1914 Margaret Sanger began publication of *The Woman Rebel*, a monthly feminist magazine devoted to the dissemination of information about birth control methods, many from France. Later, in 1916, Sanger opened the nation’s first birth control clinic in New York City. She recognized the need for immigrant and working women to control their fertility. Sanger was prosecuted for violating New York’s version of the Comstock Law and served 30 days in a federal workhouse. She was also prosecuted for sending contraception to a doctor via the mail. A federal district court ruled that the provision of contraception that promotes the health or saves the life of a doctor’s patient is not covered by the Comstock Law. Sanger’s advocacy for women’s reproductive rights ultimately led to the founding of the American Birth Control League (ABCL) in 1921, which became the Planned Parenthood Federation of America in 1943 and which continues to advocate for reproductive rights today. Sanger’s efforts with Planned Parenthood supported research that led to the creation of the birth control pill in the 1950s.

Debates over birth control dissemination continued into the 1960s. In 1961 Estelle Griswold and Dr. Lee Buxton, a physician and professor at Yale Medical School, were arrested for providing medical advice and instruction related to contraception to married couples in Connecticut. Their conviction was overturned in *Griswold v. Connecticut*, in which the Supreme Court ruled that Connecticut laws prohibiting the instruction or use of contraception by married couples violated a constitutional right to privacy.

In the early 1960s, 28 states still had laws that made it illegal for married couples to use contraception. However, in 1967 President Lyndon B. Johnson approved an annual budget of \$20 million for contraceptive programs, suggesting a growing public acceptance of “family planning.” The revolutionary development of the pill is often associated with a shift in popular sentiment regarding birth control. These



developments paved the way for a more expansive application of the right to privacy with regard to birth control. In 1972 the Supreme Court ruled in *Eisenstadt v. Baird*, 405 U.S. 438 (1972) that the same privacy protections described in *Griswold* must be extended to nonmarried women, thus allowing them access to birth control as well.

Tubal **sterilization**, a permanent form of birth control, became more widespread in the 1960s. Previously, many women desiring sterilization had to meet strict requirements; yet as of 1914 more than 10 states had laws limiting the reproductive options for women deemed socially inadequate, and by 1924 more than 3000 American women had been forcibly sterilized. Many Native American women and other women of color, particularly those on welfare, were encouraged or coerced to undergo this procedure throughout the twentieth century. Today, tubal sterilization is the most popular form of contraception in the United States.

The early 1970s brought additional gains in reproductive freedom as three states repealed their anti-abortion laws and Congress deleted parts of the Comstock Law relating to contraception and **abortion**. During this time, groups such as the American Medical Association, the **American Civil Liberties Union**, and the National Organization of Women publicly support the legalization of abortion. In 1973, a 7-2 ruling legalized abortion in the landmark case *Roe v. Wade*, 410 U.S. 113 (1973). The majority found that a woman's right to privacy included the right to unregulated abortion in the first trimester of pregnancy. At the same time, Congress passed a bill prohibiting the use of Medicaid funds for abortions, unless the mother's life was in danger.

Cost remains a barrier to access to reproductive control. For example, although some American insurance companies are covering the prescription costs for the impotency drug Viagra, only 21 states have contraceptive equity laws that require all FDA-approved birth control to be covered by health plans. From 1980 to 2003, federal funding for clinics providing birth control to low-income women fell nearly two-thirds in constant dollars.

The last decades of the twentieth century saw an increase in reproductive technology to assist fertility as well as continued debate over the roles of birth control and abortion in American society. Birth control pills have become the most common drug used by women of childbearing age; and the emergency contraceptive pill ("Plan B" or "the morning-after pill"), which prevents a fertilized egg from developing if taken within 72 hours after intercourse, was approved for use in the United States in 1998. The widespread use of such contraceptive is estimated to prevent nearly 1.7 million unintended pregnancies and 800,000 abortions annually. However, 40 years after *Griswold*, American women's access to birth control is again being threatened. Some pharmacists around the nation are refusing to dispense monthly birth control pills or emergency contraception. Four states have laws that allow pharmacists to refuse to fill such prescriptions on moral or religious grounds.

Even in contemporary American society, with some forms of birth control available at the local drug store or gas station, reports indicate that nearly half of all pregnancies in the United States are unintended. Access to birth control remains complex and the legality of birth control continues to be contested. Some current Republican politicians, including the third-highest-ranking member of the Senate,

Rick Santorum of Pennsylvania, argue that Americans have no guaranteed right to privacy, and therefore individual states should have the ability to outlaw birth control as they deem fit. The politics of technology, as well as the moral and political climate, influence attempts to limit or challenge reproductive control. Since the late 1880s proponents of birth control have understood it as a central issue behind women's equality in society. In their view, safe and reliable contraception is a prerequisite for women to control their bodies and their lives. Thus, it is important to understand that attempts to control women's reproduction are related to the prevailing social and political climate.

Some women are afforded greater privacy in matters of reproductive control, while others are subjected to limited opportunities. Without access to readily available and legal birth control, American women could expect an average of 12 pregnancies in their lifetimes. Moreover, access to reliable contraception allows women the opportunity to make other informed choices, such as those relating to employment and education. If reproductive freedom is understood as leading to better parenting and citizenship, then access to contraception is an issue of personal autonomy as well as social responsibility.

See also: **Assisted reproductive technologies; Women and privacy**

Suggested Reading: Epigee Women's Health. *Birth Control Guide*. <http://www.epigee.org/guide/>. Online, March 2006; Gordon, Linda. *Woman's Body, Woman's Right: Birth Control in America*, rev. updated ed. New York: Penguin Books, 1990 (1976); Johnson, John W. *Griswold v. Connecticut: Birth Control and the Constitutional Right of Privacy*. Lawrence: University Press of Kansas, 2005; Kranz, Rachel. *Reproductive Rights and Technology*. New York: Facts on File, 2002.

Tori Barnes-Brus

Blood testing

Blood testing is commonly used to detect or "screen for" a wide variety of diseases either present or potential. It is used both in health care settings and in the criminal justice system. When blood tests are used for **DNA** typing as the basis for constructing databases used in criminal investigations, or for detecting behaviors such as substance use, they obviously raise privacy issues similar to those raised by **urine analysis** to test for drugs of abuse. Unlike urine tests, blood tests can reveal a person's current degree of intoxication. The approximate time of drug ingestion can be ascertained by computing the ratio of drug metabolites in the blood to the presence of the drug itself. For these reasons many states permit law enforcement to draw blood in cases of suspected driving under the influence (DUI) if the individual under suspicion refuses to submit to urine testing or a breathalyzer test. In *Schmerber v. California*, 384 U.S. 757 (1966), a case involving a police officer who ordered a treating physician to conduct a test for blood alcohol level, the U.S. Supreme Court held that the blood testing did not violate the Fifth Amendment guarantee against self-incrimination even if results were later used as evidence in a drunk driving conviction. Subsequently the courts have considered blood tests to be legal searches, although any state-compelled blood testing program raises privacy issues due to the Fourth Amendment's clear guarantee against government intrusion.

Public health and safety objectives have occasioned large-scale government intrusions into private life. The "greater good" argument is often invoked to justify

the claim that social responsibility outweighs individual privacy rights in the context of infectious diseases and viral transmission. Syphilis was once a widely feared disease for which there was a relatively accurate and simple blood test. Although gonorrhea was four times as prevalent in the population, there was no straightforward blood test by which it could be diagnosed. The first mass blood testing campaign in the United States occurred within the context of the New Deal, with the launch of a federal public health campaign to contain venereal disease that focused on syphilis. The U.S. Public Health Service began to devote a significant portion of the budget allocated to it by the Social Security Act of 1935 to detecting and treating venereal disease. The U.S. Congress enacted the National Venereal Disease Control Act in 1938, which led to a national infrastructure consisting of 3000 treatment clinics as of 1940. (These clinics were later converted to family planning clinics once the concern about VD had subsided.)

The blood testing campaign against syphilis was conducted in an era when privacy and **confidentiality** were not legally protected. The number of Wasserman blood tests administered for detecting syphilis climbed nearly 300 percent from 1936 to 1940. The city of Chicago tested over 30 percent of its population beginning in 1937, capturing 10,000 to 12,000 individuals a day in its “Wasserman drag-net.” Although these programs likely produced a high number of false positives, the results were used in many cases to deny or delay marriage. Over half of the states had enacted laws prohibiting marriage between infected individuals by 1938.

States also began requiring prenatal blood testing for all pregnant women in 1938 to prevent congenital infection of infants. These laws resulted in reduced infant mortality rates even prior to the use of antibiotics. They also occasioned a large-scale expansion of government **surveillance** into formerly private matters. Public health organizations invented techniques to extract information about all sexual contacts from those who tested positive for syphilis. Case workers invented a term, “shoe leather epidemiology,” to describe how they tracked down those individuals to inform them and bring them in for testing and treatment.

Premarital syphilis testing was instituted by the states, beginning with Connecticut in 1935, but prevalence rates were lower than anticipated. Couples crossed state lines to marry, or they went to physicians reputed to keep the test results confidential. Despite the ineffectiveness of these laws, as evidenced by the low percentage of positive results, many states did not repeal them until the 1970s. A second wave of repeal followed in states where such laws were still on the books: California did not repeal its premarital blood testing law until 1994, and Georgia only did so as recently as 2003. Reasons for repeal included lack of cost-effectiveness and the fact that few cases of syphilis came to light through premarital testing, due to its higher prevalence among groups not seeking to marry or who were legally barred from marriage. The initial assumption behind premarital blood testing was that it would reach the affected population and bring those who tested positive in for treatment. However, this proved not to be the case, and it constitutes a historical lesson that can be extended to human immunodeficiency virus (HIV) testing. The concern is that mandatory testing will in fact deter individuals from seeking treatment.

Blood banks began testing for HIV in 1985 using an initial screen for the presence of HIV antibodies called an enzyme-linked immunosorbent assay (ELISA). A

positive screen must be followed by a Western blot, which is a confirmatory test. Blood banks did not, however, notify individuals of their serostatus, as their main goal was to ensure that the blood supply was not infected. The main focus of the debate over state-compelled HIV testing has been mandatory testing. Given the stigma attached to HIV, which was initially seen as a phenomenon associated with the gay population in the United States, there has been much more scrutiny of state-mandated HIV testing than there was for syphilis testing. The drive to require premarital HIV testing was unsuccessful in the United States: only two states, Illinois and Louisiana, enacted mandatory premarital HIV testing laws, and each has since repealed them. Given the higher rates of heterosexual HIV transmission in the Third World, some governments in south and southeast Asia began to require mandatory premarital HIV testing in the opening years of the twenty-first century.

Mandatory HIV testing has been upheld by the U.S. courts for certain groups. The U.S. Congress passed the Comprehensive Crime Control Act (1990), encouraging states to provide mandatory HIV testing of sex offenders and to make their serostatus known to their victims. Newborns are a second group in which mandatory testing has been permitted. New York and Connecticut both require expedited HIV testing of newborns and notification of their mothers when the serostatus of the mother is unknown. Prenatal HIV testing remains voluntary. Both circumstances in which mandatory HIV testing is applied also involve privacy issues that the U.S. Supreme Court has not yet considered, although it has ruled that the “special needs” exception to the Fourth Amendment applies to compulsory urine testing of certain populations of workers. Urine tests were considered “reasonable” infringements on the privacy of groups associated with “diminished expectation of privacy” in *National Treasury Employees Union v. Von Raab*, 489 U.S. 669 (1989). Similar exceptions may extend to mandatory government blood testing and DNA testing. The privacy question involved in the mandatory collection of blood samples for DNA testing is the extent to which prisoners forfeit their Fourth Amendment rights. Some courts have interpreted this forfeiture expansively, others more restrictively.

Another privacy question concerns **disclosures** of information that includes the results of blood testing. The U.S. Congress passed the Genetic Information Non-discrimination Act of 2003 (S. 1053) in an attempt to prevent genetic discrimination in hiring, firing, and training, as well as insurance discrimination on the basis of results of genetic testing. The concern with maintaining the confidentiality of medical records extends to genetic test results. There are many more mechanisms for protecting individual privacy and guaranteeing the confidentiality of blood test results today. Built-in exceptions to the privacy rules of the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** allow disclosure of certain kinds of information to public health authorities, such as history of disease or injury, child abuse, birth, death, and the conduct of public health surveillance, investigation, or intervention programs.

See also: **DNA and DNA banking; Health privacy**

Suggested Reading: Brandt, Allan M. *No Magic Bullet: A Social History of Venereal Disease in the United States since 1880*. Oxford: Oxford University Press, 1985; Okezie, Justin A. “The Presumption of Guilt and Compulsory HIV Testing of Accused Sex Offenders: A Case Study of *State ex rel. J.G., N.S., and J.T.*,”



American University Journal of Gender and the Law 6 (1998): 557–582; Wailoo, Keith. *Drawing Blood: Technology and Disease Identity in Twentieth Century America*. Baltimore: Johns Hopkins University Press, 1997.

Nancy D. Campbell

***Bowers v. Hardwick*, 478 U.S. 186 (1986)**

When does the mere description of one's action not impinge the basic interest of any other person? This traditional Millian notion of a self-regarding or private action has had the most difficult time in the American courts. Although the U.S. Supreme Court did say in *Roe v. Wade*, 410 U.S. 113 (1973), that a woman's right to obtain an **abortion** was such an action, at least within the first two trimesters (with the woman's physician playing a significant decision-making role only in the second trimester), in *Bowers v. Hardwick* the Court let stand a Georgia sodomy statute that made certain adult consensual homosexual sex acts a crime, even if performed behind closed doors in the home. The effect of the case was to hold outside constitutional privacy protection matters of same-sex sexual intimacy among consenting adults for the reason that they simply were not thought to be private.

The case involved the unchallenged legal entry of a Georgia police officer into the home of Michel Hardwick on the evening of August 3, 1982. There the officer found Hardwick and another adult male engaged in an act of oral **sodomy** in Hardwick's bedroom. Hardwick was subsequently charged with violating O.G.C.A. §16-6-2 (1984), a Georgia criminal statute that made it a crime to engage in sodomy with another person (male or female), even in one's home, punishable by not less than 1 and up to 20 years in prison. The Georgia statute stated that "[a] person commits the offense of sodomy when he or she performs or submits to any sexual act involving the sex organs of one person and the mouth or anus of another." The statute did not distinguish between heterosexual and homosexual sodomy. The case went to the U.S. Supreme Court, where the statute was challenged on Fourteenth Amendment substantive due process grounds, which in this case were privacy grounds.

The Supreme Court, in upholding the statute, distinguished that portion of the statute pertaining to homosexual sodomy from the remainder of the act, which addressed heterosexual sodomy. Specifically, the Court, referring to the portion of the statute making homosexual sodomy a crime, ruled, per Justice White, that its prior case law did not put adult consensual homosexual sodomy in the home beyond state proscription. The basis of the Court's rationale was that "[n]o connection between **family**, marriage, or procreation on the one hand and homosexual activity on the other [was] demonstrated." Nor did the Court's prior privacy cases protect any form of private sexual conduct between consenting adults. In effect, the Court said that the privacy of an act is determined by whether such a connection is shown. Absent such a demonstration, no privacy is at stake.

It is important to understand that the Court did not find that the state had a more compelling interest than upholding privacy to protect in this case; rather, the Court saw no privacy interest at all. And although sodomy statutes are seldom prosecuted, the effect of the *Bowers* holding was an unintended justification of state laws that discriminated on the basis of sexual orientation in matters of employment, housing, public accommodations, parenting, marriage, foster care, and military

service. Here the rationale came to be that if the underlying conduct that defined the discriminated class could be made criminal, little could be said that would persuade courts that the class might deserve a heightened degree of protection from discrimination.

When the Supreme Court decided *Bowers*, no American privacy case was directly on point in dealing with homosexual sodomy. However, the American Law Institute, a think tank of legal scholars, had by this time put forth a Model Penal Code, which a number of states had already adopted, that removed same-sex sodomy from the list of crimes. The Court's failure to assign credence to the code's adoption combined with the breadth afforded to privacy protection in several of its own prior decisions makes the Court's proffered rationale in *Bowers* untenable. Indeed, it suggests a deep-seated cultural prejudice against homosexuals on the part of some of the justices who participated in the decision. This was particularly clear from Justice Burger's concurring opinion: "Decisions of individuals relating to homosexual conduct have been subject to state intervention throughout the history of Western civilization. Condemnation of those practices is firmly rooted in the Judeo-Christian moral and ethical standards."

Interestingly, the set of privacy principles that could have decided this case—and no doubt would have, had the prejudices implicit in the above-quoted passages not existed—have their foundation in three different areas of the law: Fourth Amendment, tort, and constitutional liberty.

In the Fourth Amendment, the privacy principle protects persons, information, and places against unreasonable searches and seizures. What makes a search unreasonable is the presence of a reasonable expectation of privacy coupled with the absence of a **search warrant** based on probable cause that a crime was about to take place. This right to privacy of information and protection of places like the home was specifically aimed at preventing the government's pursuit of a criminal investigation from becoming a mere fishing expedition for possible criminal activity. A perhaps antiquated example of this rule would be the person in a glass-walled telephone booth who has a reasonable expectation of not being overheard, but no such expectation of not being seen.

In contrast to the Fourth Amendment privacy principle was the development of the **privacy tort** in civil law. Here the issue, as described in a famous law review article from the turn of the last century, was protecting against unreasonable invasions into personal affairs by the press and other persons. Professor William Prosser describes this tort as involving four separate concerns: (1) intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; (2) public disclosure of embarrassing private facts about the plaintiff; (3) publicity that places the plaintiff in a false light in the public eye; and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

Like the Fourth Amendment, the civil law privacy tort was to serve as a means of protecting information and places. However, this tort is directed against other persons rather than against the government. In this way, privacy law became, in addition to a protection against certain governmental intrusions, a safeguard of individual personhood and autonomy from the prying eyes of others. These were not the only sources of privacy protection that had been recognized prior to the Court's decision in *Bowers*, however. Beginning in the 1960s, with *Griswold v. Connecticut*, 381 U.S. 479

(1965), the Supreme Court began to set out constitutional privacy law jurisprudence based on a liberty right to engage in private actions.

In *Griswold*, the Court upheld the constitutional privacy rights of a married couple to use contraceptives and of physicians to advise their use against a state law that prohibited both. In *Eisenstadt v. Baird*, 405 U.S. 438 (1972), the Court extended that right to include unmarried persons. In *Carey v. Population Services International*, 431 U.S. 678 (1977), the Court extended the right still further, striking down a law that made it a crime to distribute contraceptives to minors. In *Roe v. Wade*, the Court extended constitutional privacy protections to a mother's choice to have an abortion, noting that the fetus was not a person under the law.

The Supreme Court's jurisprudence in this area was not confined to physical activity that was arguably self-regarding. The Court had also upheld, in *Stanley v. Georgia*, 394 U.S. 557 (1969), the right of a person to possess "obscene matter" in the home. In that case too the Court stated, "This right to receive information and ideas, regardless of their social worth, is fundamental to our free society. Moreover, in the context of this case—a prosecution for mere possession of printed or filmed matter in the privacy of a person's own home—that right takes on an added dimension. For also fundamental is the right to be free, except in very limited circumstances, from unwanted governmental intrusions into one's privacy."

All the precedent that might suggest the contrary—the fact that the Court had previously recognized a constitutional privacy right of married persons, unmarried persons, and minors to obtain contraceptives and receive physician advice on their use; a women's right to obtain an abortion with no recognized interest in an unborn fetus in the first two trimesters of a pregnancy; and the right to possess obscene materials in the home—indicates its decision in *Bowers* to be mistaken. The Court refused to find constitutional privacy protection for two consenting adults to engage in same-sex sodomy in the home. It is true that prior to *Bowers*, two cases—one New York Court of Appeals case, *People v. Onofre*, 415 N.E.2d 936 (N.Y. 1980), and a Virginia federal district court case, *Doe v. Commonwealth's Attorney*, 403 F. Supp. 1199 (E.D. Va. 1975), *aff'd mem.*, 425 U.S. 901 (1976)—had gone in opposite directions on whether a fundamental right to privacy covers and protects such activities. But it is also true that five years before *Bowers* was decided, the European Court of Human Rights (ECHR) had found, in a case similar to *Bowers* arising in Ireland, that the Irish statutory prosecution violated the privacy guarantee of the European Convention on Human Rights. According to many legal scholars, the Supreme Court's failure in *Bowers* to acknowledge the ECHR case reflects the parochial attitude of some of the justices that the Court still has difficulty managing.

Bowers was thus not a "very hard" case at the time the Supreme Court decided it because the Court had a sufficient indication of society's political morality both from its own past privacy decisions and based on what was happening elsewhere in the Western world to render a decision against such statutes based on their self-regarding nature, although it chose not to do so. Nor should the decision be dismissed on the ground that the courts have long recognized government's right to prohibit certain seemingly self-regarding behaviors such as the private use of recreational drugs in the home. In this case, one might argue that a compelling state interest exists to prevent the harmful effects of such drugs on society, which cannot

be reasonably addressed absent a blanket proscription on their possession. A similar argument might be made for prohibiting prostitution on the basis of protecting poor women from exploitation. No such similar interest existed in *Bowers*, however. For the only interest that stands out there is the protection of traditional morality. But that interest would open the door to much subjectivity when no other harm can be shown. Consequently, it is fair to say that at the time when the Court heard the case of *Bowers v. Hardwick*, its own constitutional jurisprudence had already been sufficiently developed to afford protection to Michael Hardwick.

The same precursory precedent that was available to the Court in *Bowers* was also available to guide the Court's more recent decision in ***Lawrence v. Texas*, 539 U.S. 558 (2003)**, which overruled *Bowers*. The only difference, other than that society itself had become more tolerant of gay and lesbian people, was that now the Court would render a proper decision that was consistent with its own constitutional precedent.

See also: Constitutional protections; Privacy, definition of; Privacy, philosophical foundations of; Private parts

Suggested Reading: Allen, Anita, and Erin Mack. "How Privacy Got Its Gender," *Northern Illinois University Law Review* 10 (1990): 441–454; Allen, Anita, and Erin Mack. "Taking Liberties: Privacy, Private Choice and Social Contract Theory," *University of Cincinnati Law Review* 56 (1987): 461–491; Allen, Anita, and Erin Mack. *Uneasy Access: Privacy for Women in a Free Society*. Totowa, NJ: Rowman & Littlefield, 1988; Allen, Anita, and Erin Mack. *Why Privacy Isn't Everything: Feminist Reflections on Accountability for Private Life*. Lanham, MD: Rowman & Littlefield, 2003; Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Garrow, David J. *Liberty and Sexuality: The Right to Privacy and the Making of Roe v. Wade*. Berkeley: University of California Press, 1998; Mill, John Stuart. *On Liberty*. London: Longman, Roberts & Green, 1869; www.bartleby.com/130/. Online, March 2006; Prosser, William L. "Privacy," *California Law Review* 48 (1960): 383; Samar, Vincent J. "Gay Rights as a Particular Instantiation of Human Rights," *Albany Law Review* 64 (2001): 983; Samar, Vincent J. *The Right to Privacy: Gays, Lesbians and the Constitution*. Philadelphia: Temple University Press, 1991.

Vincent J. Samar

***Boyd v. United States*, 116 U.S. 616 (1886)**

Boyd v. United States is a landmark case in the development of privacy protections, establishing a relationship between the Fourth and Fifth Amendments to the United States Constitution. In *Boyd* the Supreme Court ruled that the seizure or compulsory production of a person's personal papers to be used as evidence against that person is the same as compelling self-incrimination. Ultimately, this broad interpretation of the amendments was severely limited by subsequent Supreme Court cases.

E. A. Boyd & Sons, an importing company, was accused of importing 35 cases of plate glass into New York City without paying a duty required under an 1874 customs act. The two partners in *Boyd* attempted to import the 35 cases to furnish



glass needed in the construction of a government building. The glass specified was foreign glass. The partners understood that if part or all of the glass was furnished from the partnership's existing duty-paid inventory, it could be replaced by duty-free imports. Pursuant to this arrangement, 29 cases of glass were imported duty free. The partners then claimed they were entitled to the duty-free entry of an additional 35 cases, which were soon to arrive. The forfeiture action concerned these 35 cases.

The case as filed was civil in nature, but the Supreme Court ruled that the 1874 customs act, which allowed the imposition of both fines and prison sentences, was essentially criminal in nature. Boyd was accused of committing fraud under that act. To prove his case, the prosecuting attorney needed Boyd's records of a previous shipment involving 29 cases of plate glass. The district attorney obtained an order from the district judge requiring Boyd to produce the invoice for the 29 cases. Boyd produced the invoice and was found guilty, and the government seized the 35 cases of plate glass. Although he complied with the order, Boyd complained and appealed, arguing his constitutional rights were denied. The Supreme Court ruled in the partners' favor.

In reaching its decision, the Court spent significant time analyzing the origins of the 1874 act at issue. That act was an amendment of an 1867 act that itself was an amendment of an 1863 act. The original amendments of the act allowed "[t]he district judge, on complaint and affidavit that any fraud on the revenue had been committed by any person interested or engaged in the importation of merchandise, to issue his warrant to the marshal to enter any premises where any invoices, books, or papers were deposited relating to such merchandise, and to take possession of such books and papers." The Court noted that the act "was the first legislation of the kind" ever enacted. It was "adopted at a period of great national excitement [during the Civil War], when the powers of the government were subjected to a severe strain to protect the national existence." In 1874 the act was amended to allow the Court to order the defendant in the action to produce the books or papers.

The first step in the Court's consideration of Boyd's argument was to find that the requirement that Boyd produce documents in response to a court order was still a "search and seizure" and fell "within the scope of the fourth amendment." The more difficult question for the Court was whether the search was "an 'unreasonable search and seizure' within the meaning of the fourth amendment of the constitution."

The Court distinguished searches for "stolen or forfeited goods" and "seizure of a man's private books and papers for the purpose of obtaining information therein contained." The simple answer: "In one case, the government is entitled to the possession of the property; in the other it is not," the Court ruled. Using a historical approach, the Court examined the use of "writs of assistance" in England and the colonies before the American Revolution. Basically, a writ of assistance allowed a revenue officer collecting taxes for the crown to search any home or building for smuggled goods. Colonists, who were smuggling a wide variety of goods to avoid taxes imposed by the king, hated the practice. The Court noted that in 1761 Boston patriot James Otis called the writs "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book, since they placed 'the liberty of every man in the hands of every petty officer.'" The Supreme Court noted that Otis's comments

occurred during a debate that was “perhaps the most prominent event which inaugurated the resistance of the colonies to the oppressions of the mother country.” In other words, opposition to the writs, and the searches they allowed, was a fundamental cause of the Revolutionary War.

To show the impropriety of the legislation under consideration in the case, the Supreme Court then discussed two cases that essentially resulted in the end of general warrants in Britain. General warrants, like writs of assistance, allowed officers to seize persons or papers and, more specifically, were frequently issued to allow searches of private homes for books or papers that could be used to convict the home owner of libel.

The first case was that of John Wilkes, publisher of the *North Briton*, a newspaper that frequently denounced the crown and was considered “heinously libelous.” In April 1763 Wilkes published an article in his paper lambasting the king for a message presented in Parliament. After that, Lord Halifax, the British secretary of state, issued a general warrant and Wilkes’s home was searched. Wilkes was arrested and temporarily imprisoned in the Tower of London. After charges were dismissed, Wilkes sued for trespass. He won. The officer who searched Wilkes’s home was ordered to pay £1000 and Halifax was ordered to pay £4000.

The second case was *Entick v. Carrington and Three Other King’s Messengers*, decided in 1765. Lord Halifax had again issued a general warrant, and the resulting search of John Entick’s home found no libelous materials. In concluding his decision, Lord Camden noted, “It is very certain that the law obligeth no man to accuse himself; because the necessary means of compelling self-accusation, falling upon the innocent as well as the guilty, would be both cruel and unjust; and it should seem, that search for evidence is disallowed upon the same principle. There too the innocent would be confounded with the guilty.”

The importance of these old English cases for the Supreme Court lay not in the holdings alone but in the fact that “every American statesman, during our revolutionary and formative period as a nation, was undoubtedly familiar” with the principles expressed in those decisions. In other words, when the Founding Fathers incorporated the right against self-incrimination into the Constitution, they were incorporating the principles that had been decided in British courts almost two decades before the Constitution and the Bill of Rights were drafted. The Court concluded that the drafters of the Constitution would never have approved of the series of statutes under consideration in *Boyd*: “The struggles against arbitrary power in which they had been engaged for more than 20 years would have been too deeply engraved in their memories to have allowed them to approve of such insidious disguises of the old grievance which they had so deeply abhorred.”

For the Supreme Court, the critical questions addressed by British courts in the cited cases were at the very foundation of the concepts of “constitutional liberty and security.” Following its review of that history, the Court concluded that “any forcible and compulsory extortion of a man’s own testimony, or of his private papers to be used as evidence to convict him of crime, or to forfeit his goods” should be condemned.

The next step in the Court’s analysis was to consider the statutory history leading up to the customs act of 1867. The Court found that the first congress, in creating the Judiciary Act of 1789, granted courts the power to compel persons to turn over books

or documents in their possession, provided such documents would have been ordered to be produced under the “ordinary rules of chancery.” The Court then noted, “Now it is elementary knowledge that one cardinal rule of the court of chancery is never to decree a discovery which might tend to convict the party of a crime, or to forfeit his property. And any compulsory discovery by extorting the party’s oath, or compelling the production of his private books and papers, to convict him of crime, or to forfeit his property, is contrary to the principles of a free government.”

Then the court examined the language of the Fourth and Fifth Amendments to the constitution:

We have already noticed the intimate relation between the two amendments. They throw great light on each other. For the “unreasonable searches and seizures” condemned in the fourth amendment are almost always made for the purpose of compelling a man to give evidence against himself, which in criminal cases is condemned in the fifth amendment; and compelling a man “in a criminal case to be a witness against himself,” which is condemned in the fifth amendment, throws light on the question as to what is an “unreasonable search and seizure” within the meaning of the fourth amendment.

The Court concluded there simply is no rational difference between the “seizure of a man’s private books and papers to be used in evidence against him” and “compelling him to be a witness against himself.” The Court then warned that in order to protect against the erosion of “constitutional provisions for the security of person and property,” the courts must liberally construe those freedoms rather than apply a strict construction that “deprives them of half their efficacy, and leads to gradual depreciation of the right, as if it consisted more in sound than in substance.”

Several of the *Boyd* Court’s holdings have not stood the test of time. Perhaps the most critical shortcoming is the failure of subsequent courts to follow the recommendation that protections of liberties be liberally construed.

Specifically, the application of the Fourth Amendment to subpoenas was limited by *Hale v. Henkel*, 201 U.S. 43 (1906). Purely evidentiary (but “nontestimonial”) materials, as well as contraband and fruits and instrumentalities of crime, may now be searched for and seized under proper circumstances (*Warden v. Hayden*, 387 U.S. 294 (1967)). Also, the Supreme Court has eliminated the idea that “testimonial” evidence may never be seized and used in court (see *Katz v. United States*, 389 U.S. 347 (1967), establishing a **reasonable expectation of privacy** test for admission of tape-recorded conversations; and *Osborn v. United States*, 385 U.S. 323 (1966), on admissibility of tape-recorded conversation between attorney and client).

It is also clear that the Fifth Amendment does not independently prohibit the compelling of every sort of incriminating evidence but applies only when the accused is compelled to make a *testimonial* communication that is incriminating. The courts have therefore declined to extend the protection of the privilege to the provision of blood samples (*Schmerber v. California*, 384 U.S. 757, 763–764 (1966)), handwriting exemplars (*Gilbert v. California*, 388 U.S. 263, 265–267 (1967)), or voice exemplars (*United States v. Wade*, 388 U.S. 218, 222–223 (1967)) or to the donning of a blouse worn by the perpetrator (*Holt v. United States*, 218 U.S. 245 (1910)). Furthermore, despite *Boyd*, neither a partnership nor the individual

partners are shielded from the compelled provision of partnership records on self-incrimination grounds (*Bellis v. United States*, 417 U.S. 85 (1974)).

The conclusion in *Boyd* that a person may not be forced to produce private papers has nonetheless often appeared as dictum in later Supreme Court decisions. To the extent, however, that the rule against compelling the production of private papers rested on the proposition that seizures of or subpoenas for “**mere evidence**,” including documents, violated the Fourth Amendment and therefore also transgressed the Fifth, the foundations for the rule have been washed away. In consequence, the prohibition against forcing the production of private papers has long been a rule searching for a rationale consistent with the proscriptions of the Fifth Amendment against compelling a person to give “testimony” that is self-incriminating.

The Supreme Court has noted that the act of producing evidence in response to a subpoena has communicative aspects of its own, wholly unrelated to the contents of the papers produced. Compliance tacitly concedes the papers’ existence and their possession or control by some party. It could also indicate a party’s belief that the papers are those sought (*Curcio v. United States*, 354 U.S. 118, 125 (1957)). Elements of compulsion are present, but the more difficult question is whether the “tacit averments” of the party are both “testimonial” and “incriminating” under the Fifth Amendment.

It is unlikely that admitting the existence and possession of papers will rise to the level of testimony afforded protection under the Fifth Amendment. When the existence and location of the papers are a foregone conclusion, a party adds little or nothing to the sum total of the government’s information by conceding that he in fact has the papers. Under these circumstances, by enforcement of the summons “no constitutional rights are touched. The question is not of testimony but of surrender” (*In re Harris*, 221 U.S. 274, 279 (1911)).

The historical and statutory history relied on by the Supreme Court in *Boyd* have great appeal to those concerned with finding privacy rights in the Constitution. But with subsequent Supreme Court rulings on specific evidentiary questions and with the denial of any convergence between the Fourth and Fifth constitutional amendments, the holding in *Boyd* has effectively been reversed.

See also: **Constitutional protections**

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black’s Law Dictionary*, 7th. ed. St. Paul, MN: West, 1999; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hall, Kermit L. *Conscience, Expression and Privacy: The Supreme Court in American Society*. New York: Garland, 2000; Hubbard, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley



Heights, NJ: Enslow, 2000; Smith, Robert Ellis. *Compilation of State and Federal Privacy Laws*. Providence, RI: Privacy Journal, 1992.

David J. Brown

Brandeis, Louis D. (1856–1941)

Louis Dembitz Brandeis was born in Louisville, Kentucky, on November 13, 1856. His family was from Prague. Brandeis excelled in his studies in high school and then at school in Dresden. Brandeis attended Harvard Law School and graduated at the top of his class in 1877. He became a successful lawyer in Boston and a leading advocate of social and political reform. President Woodrow Wilson named Brandeis to the Supreme Court in 1916. Following a contentious battle, he became the first Jewish member of the Supreme Court. He retired from the Court in 1939 and died in 1941.

No person in the United States has had a greater influence on the development of privacy law than Louis Brandeis. This is all the more remarkable in view of the fact that Brandeis published only a single article on privacy (which was rejected by the first court that considered his argument) and a single judicial opinion (which appeared as a dissent and was largely ignored for almost 40 years). But today that article, “The Right to Privacy,” and the dissent in *Olmstead v. United States*, 277 U.S. 438 (1928), are routinely cited by scholars, judges, policymakers, and privacy advocates all around the world.

“The Right to Privacy” appeared in the *Harvard Law Review* in 1890. Brandeis and his co-author and close friend, Samuel Warren, argued forcefully that the common law should evolve in response to new technology and new business practices to recognize a new right: “**the right to be let alone.**” Significantly, the authors focused on the injury caused by private persons and not by government since tort law is generally concerned with private wrongdoing.

By many accounts, the article is one of the most influential in American law. It is also a model for legal scholarship. Brandeis and Warren described an emerging social challenge. They discussed how current law failed to provide adequate protection. They examined similar claims in other jurisdictions, including courts in England and France, and they set out an argument for a new approach that eventually transformed law in the United States. The article is purposeful, ambitious, timely in its publication, and timeless in its ongoing influence.

The Brandeis-Warren article also considered possible limitations on the claim of a right to privacy. They said first that the right to privacy “does not prohibit any publication of matter which is of public or general interest.” This important qualification anticipated that the claim of privacy would, at times, come into conflict with freedom of the press and the public’s right to know. Brandeis and Warren also suggested that limitations included communications that would otherwise be privileged (such as communications in legislative or judicial proceedings), oral communications, or information that has been published by the individual or with his or her consent. Brandeis and Warren said that truth would not provide a defense—an important distinction from the law of defamation—nor would the absence of malice.

A New York state court first considered the argument for the Brandeis-Warren tort in the 1902 case of *Roberson v. Rochester Folding Box Co.*, 171 N.Y. 538, 64

N.E. 442. In that case, a company displayed the image of a young woman on an advertising flyer without her consent. She claimed that her privacy was violated. Although the court rejected her argument, it did say that a legislative body could establish law preventing the use of a person's picture or name for advertising purposes without that person's general consent. The following year, the New York state legislature passed such a law. Two years later, a Georgia court considered a case similar to the one in New York and held instead for the plaintiff. Georgia thus became the first state to recognize a common law tort action for privacy invasion.

Claims under the common law tort of privacy continued in state courts throughout much of the twentieth century. Legal scholars outside the United States described the tort as the "American tort," in part because the common law courts of Britain had rejected similar claims.

In 1960 Dean Prosser examined over 300 **privacy tort** cases and concluded that they fell into four categories: public **disclosure** of privacy facts, intrusion upon seclusion, false light, and appropriation. Prosser's taxonomy became a popular way to describe the privacy right first set out by Brandeis and Warren, although some legal scholars suggested that the original formulation relied on a unified concept of human dignity that could not easily be divided into separate categories.

Throughout the latter part of the twentieth century, the common law tort of privacy increasingly confronted challenges from media organizations claiming that the right to privacy infringed on the public's right to know. Nonetheless, state courts continued to adopt the legal theory. In 1998 the Minnesota Supreme Court recognized the privacy tort in *Lake v. Wal-Mart*, 582 N.W.2d 231 (1998). The case is significant also because it arose from the unapproved publication of photographs, which several legal scholars believe was the reason for the original article.

Another sign of the ongoing vitality of the Brandeis-Warren article is that it was cited in *Bartnicki v. Vopper*, 532 U.S. 514 (2001), a case involving the disclosure of a private telephone conversation, by the Court majority, the justices in concurrence, and even those in dissent. Although the justices could not agree as to the outcome of the case before them, they all seemed to agree that it was important to cite Brandeis in their opinions.

The dissent of Justice Brandeis in *Olmstead* is the cornerstone of modern privacy law. In that case, which concerned the investigation of a popular bootlegger during prohibition, the Supreme Court was asked to determine whether the Fourth Amendment **search warrant** requirement applied to the interception of a telephone communication. Much of the evidence in the case was obtained by **wiretapping**.

The Court, in an opinion by Chief Justice Taft, held that because no physical intrusion upon a protected space had occurred, there was no search and therefore no warrant was required. Justice Taft noted that Congress could establish privacy protection for telecommunications by legislation if it chose to do so. Justice Holmes wrote in dissent that the wiretap by federal officials, which violated state law, was a "dirty business." But it was the dissent of Justice Brandeis that came to shape modern-day privacy law.

Brandeis said first that the application of the Constitution required considering not only what "has been, but of what may be." Brandeis said that because the privacy of mail communications was already protected and because tapping into a telephone



communication is an intrusion far greater than tampering with the mails, the Constitution should recognize the protection of this new form of communication.

Brandeis concluded, in one of the most widely cited phrases of modern privacy law, that the right of privacy is “the most comprehensive of rights and the right most valued by civilized men.” The gender-specific reference, although not surprising, was unfortunate. Feminist scholars would later criticize Brandeis for harboring a paternalistic view.

It is often claimed that the Brandeis dissent in *Olmstead* was adopted by the Supreme Court in *Katz v. United States*, 389 U.S. 347 (1967), another case involving a telephone interception and the question of whether a warrant was required. It is true that the Court relied on the *Olmstead* dissent to reach its conclusion that a search had occurred and that a warrant should have been required. However, the “**reasonable expectation of privacy**” test, introduced by Justice Harlan in a concurrence in that case, took the law down the path of trying to determine whether there was an expectation of privacy based not only on one’s subjective expectation but also on a socially objective expectation. Not surprisingly, as technology advanced, courts became less willing to recognize an expectation of privacy as objectively reasonable.

It seems unlikely that Brandeis would have endorsed this view of the Fourth Amendment. His opinion in *Olmstead* relied in part on a nineteenth-century case, *Boyd v. United States*, 116 U.S. 616 (1886), that flatly prohibited the government from securing access to certain types of information. Brandeis viewed the Fourth Amendment limitation on searches as closely interwoven with the Fifth Amendment prohibition of government incursions into the person. It is an approach to privacy that does not simply establish procedures to regulate government conduct but sets certain aspects of the person beyond the reach of government.

A German constitutional court embraced this view of privacy in 2004. That court found that federal wiretapping laws infringed upon the guarantees of human dignity and the inviolability of the **home**. The court held that an absolute area of intimacy where citizens can communicate privately without fear of government **surveillance** protects certain communications.

Brandeis’s defense of the First Amendment and his contribution to modern First Amendment doctrine is also noteworthy as critics of privacy often charge that privacy and the First Amendment are at odds. With Justice Holmes, Brandeis set forth a robust view of the First Amendment that was later embraced by the Supreme Court in such cases as *Times v. Sullivan*, 376 U.S. 254 (1964), and *Brandenburg v. Ohio*, 395 U.S. 444 (1969). The Brandeis opinion in *Whitney v. California*, 274 U.S. 357 (1927), is considered one of the most eloquent expressions of First Amendment values in all of American law. In that opinion, Brandeis set forth a broad view of the right to protest, the right to assemble, and the right to challenge government as essential to the functioning of an effective democracy. At other times, Brandeis set forward expansive views of open government and the broad dissemination of public information, and he argued for greater public participation in government decisionmaking.

Louis Brandeis engaged in many of the popular legal and social causes that emerged in the United States in the early twentieth century. Associated with the progressive movement, the founding of the state of Israel, and many social and

political reform efforts, Brandeis embraced a view of law as a public service and a means of social change. He supported the New Deal programs of the Roosevelt administration but also argued against concentration of power in the government and the private sector. Brandeis campaigned for workers' rights, for consumer protection, against corruption in government and against persistent poverty.

Brandeis's expertise as a lawyer as well as his views about American government also influenced the modern privacy movement. Perhaps in response to the growing formalism in American law following the adoption of Langdell's scientific approach to legal education, Brandeis prepared a brief in a case concerning working conditions that relied almost exclusively on empirical data gathered from experts in social science. Instead of presenting legal arguments about the appropriate scope of liberty of contract, Brandeis chose to present evidence on the impact of long hours for working women. The Brandeis Brief, as it came to be known, became a critical tool for litigators and political reformers. Modern-day **privacy advocacy organizations**, such as the Electronic Privacy Information Center (EPIC), often have followed the model of the Brandeis Brief in their cases. For example, in *Hibel v. Sixth Judicial District*, 542 U.S. 177 (2004), EPIC submitted an amicus brief to the Supreme Court that included detailed reports on computer databases that would be accessible to police officers if a Nevada state law compelling the disclosure of personal identity was upheld.

Brandeis was also a fierce defender of federalism. In *New State Ice v. Liebmann*, 285 U.S. 262 (1932), Brandeis defended state regulation of business activity, arguing that the states were "laboratories of democracy." Brandeis's views of federalism came to the aid of modern-day privacy advocates when those who opposed state regulation of commercial **data brokers** argued for federal preemption that would limit the ability of the states to safeguard privacy. Privacy advocates, arguing as Brandeis did many years earlier, supported the regulatory "experimentation" of the states

As lawyer, social reformer, and jurist, Louis Brandeis was one of the most influential Americans of the twentieth century. Although privacy was never a central focus of Brandeis's work, his contributions to the development of the law of privacy, his innovative work as a lawyer, and his basic regard for the rights of the individual in a modern, industrial democracy provided the foundation for many future privacy efforts.

In recognition of his contributions, the organization Privacy International bestows the Brandeis Award to "those have done exemplary work to protect and champion privacy."

See also: **Constitutional protections; Privacy, Definition of; Privacy, philosophy of**

Suggested Reading: EPIC and Privacy International. *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* (2004). <http://www.privacyinternational.org>. Online, March 2006; Lief, Alfred. *The Social & Economic Views of Mr. Justice Brandeis*. New York: Vanguard Press, 1930; Mason, Alpheus Thomas. *Brandeis: A Free Man's Life*. New York: Viking Press, 1946; Mason, Alpheus Thomas. *Brandeis & The Modern State*. Princeton, NJ: Princeton University Press, 1933; McGraw, Thomas. *Prophets of Regulation: Charles Francis Adams, Louis D. Brandeis, James M. Landis, Alfred E. Kahn*.



Cambridge, MA: Harvard University Press, 1984; Purcell, Edward A., Jr. *Brandeis and the Progressive Constitution*. New Haven, CT: Yale University Press, 2000; Solove, Daniel, Marc Rotenberg, and Paul Schwartz. *Information Privacy Law: Cases and Materials*. New York: Aspen, 2005; Strum, Philippa. *Brandeis: Beyond Progressivism*. Lawrence: University Press of Kansas, 1993.

Marc Rotenberg

C



Cable Communications Policy Act of 1984

The Cable Communications Policy Act of 1984 (CCPA) dictates the privacy practices of cable companies. Under the act, default privacy protections are minimal. For example, although customers must sometimes give consent for their cable companies to collect **personally identifiable information**, consent is easily obtained and is often not required. First, nothing in the act prevents a cable company from obtaining the required consent via the standard cable agreement or via another standardized process such as a “click-through” agreement on the company’s website. Second, even without such consent, cable operators may collect such information in order to “obtain information necessary to render a cable service or other service provided by the cable operator to the subscriber” or to “detect unauthorized reception of cable communications.”

Personally identifiable information may include account information such as name, address, **electronic mail** address, telephone number, driver’s license number, **Social Security number**, bank account number, and other account information. It may also include information regarding your viewing habits, for example, how much time you spend watching programs, which menu screens you use most often, and which pay-per-view programs you order. Under the CCPA, personally identifiable information does not include “any record of aggregate data which does not identify particular persons.” At least one court has ruled that personally identifiable information also does not include information stored in the cable converter box. As technology advances and as cable companies are able to offer ever more sophisticated program options, the amount of personal information collected by cable companies may become enormous.

Beyond collection of personal information, cable companies also have wide latitude in disclosing personal information. Even if a customer does not consent, cable companies can disclose that customer’s personally identifiable information if it is “necessary to render, or conduct a legitimate business activity related to a cable service or other service provided by the cable operator to the subscriber.” Thus, cable operators may disclose customers’ personal information to third parties such as marketing companies, collection agencies, and companies that specialize in warehousing personal



information and creating personal profiles; indeed, this “legitimate business activity” exception means that personal information can be disclosed to almost anyone. Moreover, because of the legitimate business activity provision, cable companies are permitted to combine customers’ personal information with personal information obtained from third parties to construct enhanced databases and customer profiles.

Cable companies are required to give customers **privacy notices** and privacy policy statements at the time a customer enters into a cable agreement. After this, a privacy policy must also be sent to each customer at least once a year. The policy must inform the customer of what personal information is collected by the cable company, how this information will be used, what the disclosure practices of the company are, how long the customer’s personal information will be retained, instructions on how and where to access the personal information that the cable company has collected, and the limitations on the company’s legal collection of and disclosure of personal information.

If a third party requests a cable subscriber’s personally identifiable information pursuant to a court order, the cable company must notify the subscriber. If a governmental entity requests such personal information pursuant to a court order, that entity must show by clear and convincing evidence that the customer is reasonably suspected of engaging in criminal activity and that the information would be material evidence in the case; in addition, the customer must be given the right to appear in court and contest any claims made in support of the court order. However, this notice requirement has been deemed inapplicable if the cable operator provides both **Internet** access and cable access to the customer, because the **Electronic Communication Policy Act of 1986** bars companies that provide electronic communications services from notifying customers that their personal information has been requested by a governmental entity via a court order.

A cable customer has the right to access all the personally identifiable information that the cable operator has collected on the customer at a convenient place designated by the cable company. If the customer finds errors in his or her personal information, the customer must be given a reasonable opportunity to correct any errors. Personally identifiable information must be destroyed by the cable company if the information is no longer necessary for the purpose for which it was collected, and if there are no pending requests or court orders for such information. The CCPA allows aggrieved customers to collect actual damages, which cannot be less than \$100 per day of a violation or \$1000—which ever is higher. The court may also award punitive damages, reasonable attorneys’ fees and reasonable litigation costs. Finally, the act permits states and franchising authorities to enact or enforce laws consistent with the act.

See also: **Fair information practices; Opt-in vs. opt-out**

Suggested Reading: Cate, Fred H., Robert E. Liton, Michael Staten, and Peter J. Wallison. *Financial Privacy, Consumer Prosperity, and the Public Good*. Washington, DC: Brookings Institute, 2003; Federal Communications Commission. <http://www.fcc.gov>. Online, January 2006; Fischer, Richard L. *The Law of Financial Privacy*. Washington, DC: A.S. Pratt & Sons, 2002; Gandy, Oscar. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press, 1993; Garfinkle, Simson. *Database Nation*. New York: O’Reilly, 2000; Rubin, Paul H., and Thomas M. Lenard. *Privacy and the Commercial Use*

of Information. Amsterdam: Kluwer Academic Publishers, 2002; Smith, Jeff H. *Managing Privacy: Information Technology and Corporate America*. Chapel Hill: University of North Carolina Press, 1994.

Marcy E. Peek

***Cady v. Dombrowski*, 413 U.S. 433 (1973)**

Dombrowski was a member of the Chicago police force and owned a 1960 Dodge **automobile**. On September 9, 1969, Dombrowski visited West Bend, Wisconsin, located over a hundred miles northwest of Chicago. He visited two taverns near West Bend that evening and in the early morning of the next. Around noon of the second day, Dombrowski's car became disabled, and he had it towed to his brother's farm. He then borrowed his brother's car and drove back to Chicago.

Once back in Chicago, Dombrowski rented a Thunderbird at the airport around midnight, and drove back to his brother's farm, where a tenant witnessed the Thunderbird pull alongside of the Dombrowski's Oldsmobile at 4 a.m. On the morning of September 11, Dombrowski purchased two towels from a nearby department store. That evening he ate and drank heavily in a restaurant for over three hours, and then he attempted to return to his brother's farm. On his way, Dombrowski had an accident and smashed the rented Thunderbird into a bridge abutment. A passing motorist saw Dombrowski and gave him a ride back to town, where Dombrowski called the police. The police picked Dombrowski up at a tavern and took him to the scene of the accident. On their way, the officers determined Dombrowski to be drunk since he offered three different stories of how the accident happened.

When the police arrived at the scene, they took several measurements relevant to the accident. Dombrowski informed the officers he was a Chicago law enforcement officer. At the time, the Wisconsin officers believed that Chicago police officers were required to carry their service revolvers at all times. Therefore, before the tow truck arrived, the officers searched Dombrowski as well as the front seat and glove compartment of the car for his service revolver, but did not find it. The car was towed to a private garage in Kewaskum, Wisconsin, and no guard was posted at the garage. Dombrowski was interviewed at the West Bend police station and subsequently arrested for drunk driving. Later, because his condition was not improving, Dombrowski was taken to a local hospital where he lapsed into a coma and was placed under guard for observation.

One of the Wisconsin police officers, an Officer Weiss, returned to look for the service revolver in the car, following the standard procedure of the West Bend police department. In his search of the vehicle, Weiss discovered blood in the car and several items in the trunk, including a nightstick with Dombrowski's name on it, two pairs of trousers, a raincoat, a towel, and a floor mat with fresh blood on it. When confronted with these items and with the assistance of counsel, Dombrowski informed the officers that he believed there was a body to be found at the north end of his brother's farm.

Upon investigation, officers found the half-dressed decedent's body near the disabled Dodge on the farm. Looking through one of the windows of the vehicle, the officers observed a pillowcase, the backseat, and a briefcase covered in blood. The officers returned with **search warrants** and orders to impound both of the vehicles. The laboratory discovered and seized the front and back seats, a sock covered



in blood, a rear floor mat partially covered with blood, the briefcase, and a front floor mat. The return of the warrant was filed, but it failed to list the sock and floor mat as having been seized.

The issue presented in this case concerns whether the warrantless search of the Thunderbird violated Dombrowski's Fourth Amendment rights, and whether the seizure of the sock and floor mat was invalid, having not been listed in the warrant's return. In the decision, the Supreme Court made several key distinctions regarding the search of the wrecked Thunderbird. The Court admitted that generally there is a **reasonable expectation of privacy** regarding a vehicle, but in certain circumstances, that expectation is trumped by public concern. Moreover, cars are ambulatory and often noncriminal conduct will bring officers in plain view of evidence, fruits, or instrumentalities of a crime or contraband. The Court pointed out two important factual findings in this case that support its reasoning. First, the Thunderbird represented a nuisance since it had been left on a public highway, and Dombrowski had been unable to make arrangements to move the vehicle. The car was not adjacent to a dwelling or momentarily unoccupied on a street, and therefore there was no reasonable expectation of privacy. Secondly, it was standard procedure to check a vehicle for a revolver in order to protect public safety. It was constitutionally reasonable to believe that someone could happen upon the revolver and retrieve it. Therefore, the police officer took action designed to protect the safety of the general public, and not to intrude on Dombrowski's rights. The Court then reasoned that the seizure of the sock and floor mat from the Dodge was not invalid, because the Dodge automobile was the item particularly described in the warrant as the subject of the search. Therefore, it was not significant that the items were not listed in the warrant return, and the warrant was valid at the time the articles were discovered.

See also: Carroll v. United States, 267 U.S. 132 (1925); Schmerber v. California, 384 U.S. 757 (1966); South Dakota v. Opperman, 428 U.S. 364 (1976); Terry v. Ohio, 392 U.S. 1 (1968)

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Feinman, Jay M. *Law 10: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow Publishers, 2000.

Matthew M. Dwyer

California v. Ciraolo, 476 U.S. 207 (1986)

In standard analyses of the Fourth Amendment, which was designed in part to protect individuals' right to privacy, whether a person has a constitutionally

protected expectation of privacy is based on two levels of inquiry. The first is whether a person has demonstrated an expectation of privacy, and the second is whether society will accept that expectation as reasonable. Although these appear to be straightforward standards, cases such as *California v. Ciraolo* illustrate the complexities involved in the analysis of the Fourth Amendment.

In this case, the respondent, Ciraolo, had marijuana growing in his back yard, which was protected from sight at ground level by a 10-foot-high inner fence and a 6-foot-high outer fence. The **home** itself was directly in front of the yard and provided one edge of the fence's perimeter. This tall barrier, however, was no match for the Santa Clara, California, police department. After receiving an anonymous tip reporting the respondent's illegal activity, the police department dispatched two officers, both of whom were trained in marijuana identification, to fly over the respondent's property in a private plane. The officers, flying at an altitude of 1,000 feet, within publicly navigable airspace, identified and photographed the marijuana growing on the respondent's property. In addition, they photographed the outside of the respondent's house as well as other homes and yards in the surrounding region. One of the officers filed an affidavit on the basis of the anonymous tip and his naked-eye observations. He attached the photograph of the respondent's home and surrounding area to the affidavit and obtained a **search warrant**. As a result of the search, 73 plants were seized from the respondent's property.

The respondent pleaded guilty to cultivating marijuana after the trial court denied his plea to withhold the evidence of the search. The California Court of Appeals, however, reversed the trial court's decision to deny the respondent's motion. It ruled that the aerial observation of the respondent's yard, which occurred without a warrant, violated the Fourth Amendment to the Constitution of the United States. Finally, in May of 1986, the Supreme Court granted a writ of certiorari and again reversed the appellate court's verdict. It ruled that the respondent's motion to withhold the evidence was properly denied, and that there had been no violation of the Fourth Amendment.

To properly apply the Fourth Amendment, it was necessary for the Court to first decide whether the respondent, Ciraolo, clearly had attempted to demonstrate his expectation of privacy with respect to his property. None of the courts disagreed that the fences surrounding the yard were obvious evidence that the respondent had demonstrated this expectation. The Supreme Court, however, addressed the second question, which was whether his expectation of privacy was reasonable. Although the respondent's yard was considered to be part of his home, and the respondent had an expectation of privacy in his home, the Court determined that this did not restrict all police **surveillance**. While the respondent took measures to prohibit views of his property from ground level, the officers who observed the illegal cultivation of marijuana were in a public area that happened to be in the air, and they possessed every legal right to be there. Therefore, according to the Court, the respondent knowingly exposed his property to public sight. In addition, anyone who flew above the respondent's yard and happened to look down could have viewed what the officers viewed. Therefore, the Court ruled that for the respondent to hold the expectation that his yard was protected from all observation was not an expectation that society was willing to accept as reasonable.



In his dissent, Justice Powell referred to the period of the Fourth Amendment's passage and the original intention of the framers of the Constitution to protect citizens' right to security and freedom from surveillance. Powell pointed out that scientific and technological advances had made it possible for police officials to devise strategies for surveillance that did not constitute physical intrusion on privacy. Thus, the Fourth Amendment gives individuals the right to be in their homes and in the areas directly surrounding their homes, free from any governmental intrusions, yet does not protect these same individuals from intrusions made possible with modern technology. In this instance, police officers observed the respondent's activities by means of a private airplane, a product of modern technology. Powell questioned why this method of surveillance was permitted without a warrant, yet, if the officials had climbed a tree or the respondent's fence in order to view the yard, the Court would have deemed this method of search as unreasonable.

The Court's inquiry as to whether society would view the respondent's expectation to privacy as reasonable was also flawed in Powell's opinion. The Court held that the respondent could not expect privacy from aerial observations taken from public airspace, and that society would not recognize this expectation as reasonable either. Powell observed that commercial flights are not taken with the purpose of observing one specific home and one specific person's activities, as was the case for the officers flying above the respondent's home. At most, people aboard a public aircraft may have only seconds to view what is going on below them as they pass over, and the chances of them connecting what they see to any one specific person are slim to none. Therefore, contrary to the majority opinion, the respondent did not knowingly expose his property to governmental surveillance any more than any other person who had not constructed a roof to cover his yard.

Overall, Powell found it difficult to imagine that society would permit individuals to be subjected to this type of police surveillance of their homes and yards without a warrant and concluded that there should be some recognition of a violation of the Fourth Amendment in this case.

See also: Chimel v. California, 395 U.S. 752 (1969); **Constitutional protections; Curtilage; Payton v. New York**, 445 U.S. 573 (1980); **Reasonable expectation of privacy; Trespass; United States v. Dunn**, 480 U.S. 294 (1987); *Warden v. Hayden*, 387 U.S. 294 (1967); *Weeks v. United States*, 232 U.S. 383 (1914)

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow Publishers, 2000.

Sean M. Peek

***Camfield v. City of Oklahoma City*, 248 F.3d 1214 (2001)**

In *Camfield v. City of Oklahoma City*, the Tenth Circuit Court of Appeals adjudicated a videotape renter's contention that an official policy to remove a famous foreign film from public access violated numerous **constitutional protections** and provisions. At issue was the policy by the Oklahoma City Police Department to confiscate the Academy Award-winning film *The Tin Drum* from the public following a state judge's decision that the video violated Oklahoma's child pornography statute. The state court judge's controversial decision was made *ex parte*, which means that no parties to the case were present or allowed to make arguments. Because the statute was amended amid the proceedings, the Supreme Court held that the renter's challenge to Oklahoma's child pornography statute was moot. However, the Court did rule that the police department's policy of complete removal of the foreign film without a prior adversarial hearing did impose an unconstitutional prior restraint under the First Amendment (and the Fourteenth Amendment as applied to the states).

The facts of the case were highly touted at the time. Michael Camfield, who was heavily involved with the **American Civil Liberties Union (ACLU)**, had his copy of the movie taken from his apartment by three Oklahoma City Police Department officers. He sued the city of Oklahoma City, several members of the Oklahoma City Police Department, and two state prosecutors under 42 U.S.C. §1983, alleging violations of his First, Fourth, and Fourteenth Amendment rights.

The Tin Drum, a German film, received the 1979 Academy Award for best foreign language film, among numerous other awards and acclaim. The Court recalled an earlier interpretation of the film "as a complex allegorical fantasy intended to symbolize the rise of Nazism and the corresponding decline of morality in Nazi Germany." At the time of the case, the movie had been circulating in the public domain for over 20 years and had been widely discussed in academic articles in books devoted to film.

In 1997, a citizen complained to the Oklahoma City Police Department that *The Tin Drum* contained child pornography. The police obtained a copy of the movie and submitted it to a state judge to receive a judicial ruling on the matter. The judge confirmed the allegation that the movie contained child pornography as defined by the Oklahoma child pornography statute, although his opinion was given orally and not as a formal written opinion.

Upon the judge's oral ruling, the Oklahoma City Police Department instituted a policy to remove the objectionable film from public access. Police officers visited numerous video stores throughout Oklahoma City and obtained copies of the tape. They also requested and received the names and addresses of people who were renting the movie at that time. One of those customers in possession of a rental tape was Michael Camfield, the development director of the ACLU of Oklahoma. Upon hearing of the recent controversy over *The Tin Drum*, he was watching the film to devise rebuttal strategies for his organization "when the officers knocked on his door." Mr. Camfield handed over the tape to the police officers, contributing to a total of nine voluntary surrenders of tapes to the Oklahoma City police. Those nine renters later requested that their tapes be returned, but the Oklahoma City Police Department refused their requests.

While Mr. Camfield's legal challenge to the Oklahoma City Police Department's policy of removing the tape was being addressed, the Oklahoma state legislature narrowed its definition of child pornography within its child pornography statute. Thus, the statute no longer criminalized material involving a minor who was merely "portrayed, depicted, or represented as engaged in" sexual acts. The Supreme Court found that this substantial narrowing of the statute made Mr. Camfield's challenge to the statute moot. As the Court explained, a challenge is moot when there is no longer "a live case or controversy" as required by Article III of the United States Constitution.

Mr. Camfield's challenge to the Oklahoma City Police Department's policy of removing the tape, however, remained intact. Although the legislature narrowed the statute after the tapes were removed, this did not change the state of affairs at the time the police officers had removed the tapes from public domain without an adversarial judicial hearing. The Court held that the policy of having video renters voluntarily surrender their copies of the tape "imposed an unconstitutional prior restraint on speech" under the First and Fourteenth Amendments. Deciding whether the tape included images of child pornography at the time of the policy was a legal determination that required an adversarial hearing. Thus, because no such hearing involving arguments by both sides had occurred, the policy was deemed unconstitutional. This violation, however, was limited to the First and Fourteenth Amendments. The Court rejected Mr. Camfield's Fourth Amendment claim because he failed to demonstrate either a search or a seizure.

See also: **Constitutional protections; Video Privacy Protection Act of 1988**

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed, St. Paul, MN: West, 1999; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow Publishers, 2000.

Ryan C. Hudson

Carnivore

Carnivore, also referred to as the Carnivore Diagnostic Tool or the Carnivore Electronic Communication Collection System, is the name of a series of suites of software developed by the **Federal Bureau of Investigation (FBI)** for authorized collection of electronic data for law enforcement purposes. It is an example of packet-sniffing software. Carnivore was designed by the FBI to intercept and copy data packets to and from suspects at the site of an **Internet** service provider (ISP) with the cooperation of the ISP. The term "Carnivore" is also commonly used to describe the successors to that series of software, even though the FBI dropped the name Carnivore in 2001 to adopt the more neutral name of DCS1000 to describe

the intercept suite. Unlike furtively employed and developed tools, Carnivore has been openly discussed by the FBI on its website and by other U.S. government institutions. For example, it has been subject to congressional review, and there was even an appraisal of the software under the auspices of the Department of Justice carried out by the Illinois Institute of Technology Research Institute.

With the advent of widespread public use of the Internet as a communications network, it became clear to the FBI that for law enforcement purposes agents would have to use tools to intercept network data traffic in much the same way that phone taps are used to gather evidence of criminal activity. This need for data-intercept tools led to the development of Carnivore's predecessors during the 1990s.

The FBI is reputed to have developed its first packet capture system in the mid-1990s, but little is publicly known about this first system. The second incarnation, Omnivore, was developed in 1997 for the Solaris x86 platform at a cost of around \$900,000. It was designed to give government agencies the ability to capture Internet traffic based on users' identities and to print captured **electronic mail** in real time. In addition, Omnivore was configured to save the captured e-mail to an 8 mm tape backup. Through a project named Phiple Troenix, the FBI developed Carnivore to replace Omnivore. This redevelopment was driven by the need for a more modern system that could be run on personal **computers**, and this project led to the development of the Carnivore suite at a cost of \$800,000 to run on the Microsoft Windows NT operating system.

From Omnivore to DSC1000, the Carnivore-type systems seem to have operated in fundamentally the same way. A system is installed in the machine room of an ISP under the administration of an FBI agent. All the Transmission Control Protocol/Internet Protocol (TCP/IP) data (the way in which information is coded and packaged to communicate on the Internet) traveling past the Carnivore insertion point are captured as a copy of the data stream. There is not an interruption of the data; rather, the data are merely mirrored as they flow past. As the TCP/IP data are captured, they are written to a buffer in order to temporarily store the copies of the packet data, typically to a shared memory area of the system. As the memory area begins to fill, the Carnivore software sifts through the information collected, applying user-defined filters to the buffered packet data. Thus, if Carnivore were configured to collect all e-mails to mperry@uwo.ca, all the packet data to that address would be written from the buffer to a more permanent storage medium (such as a Zip drive or hard drive), while all other data would be flushed from the buffer. In essence the system replicates all the traffic passing the insertion point but discards anything that does not meet the search criteria. However, Carnivore is more configurable than simply being able to search for an e-mail address, for it can be set to capture sets of data based on fixed or dynamic Internet Protocol (IP) addresses, and can collect all the packets to and from a particular address, or, in "pen-mode," only the to/from header information. Thus, not only e-mails but also the web pages browsed, the file transfer protocol, or indeed any transfers from a particular computer or suspect can be captured by the system.

In recent years, the FBI seems to have begun to move away from using its own software to using commercially available software. Taking into account the ongoing support and development costs of a home-grown system in a rapidly developing

environment, it may be that using a commercial system that can be tailored for a particular enforcement purpose is more effective. The FBI's Carnivore/DCS1000 report to Congress at the end of 2003 states that during that year the agency deployed **surveillance** software eight times but did not deploy Carnivore or DCS1000 at all.

There are a number of commercial packet analysis packages available, such as EtherPeek, Ethertest, and Ethereal. These are often employed by network technicians in order to detect network problems and determine network performance. They can also be used in the same way as Carnivore to capture packet data information, and other law enforcement agencies have used EtherPeek. The main weakness with this type of software is that the use of a simple encryption package can defeat content collection, and this has led to the development of **keystroke logging** software such as Magic Lantern. By inserting a key logging program onto the computer of a suspect, such as by the use of a Trojan horse, which is a surreptitiously installed computer program, enforcement agencies can record the keys typed by the computer user. However, the use of IP masking, IP spoofing, anonymizing proxy servers, and other security techniques, which are all perfectly legal and have legitimate uses, can prevent the easy identification of the target suspect. As with many other areas of computer security, it is essentially an "arms race" between those who wish to obfuscate their data, for legitimate or illicit reasons, and those who seek to use code to uncover the data transmissions and content of others, which may also be legal or illegal.

The history of Carnivore and its successors illustrates that legitimately deployed law enforcement tools that copy targeted digital transmissions have a useful role to play in the law enforcement environment, and they will continue to be used, whether developed by enforcement agencies themselves or by private companies that offer off-the-shelf packages that allow government entities to tailor programs meet their objectives.

See also: **Cryptography; Electronic surveillance; Wiretapping**

Suggested Reading: Electronic Privacy Information Center. *Carnivore*. <http://www.epic.org/privacy/carnivore/>. Online, March 2006; Federal Bureau of Investigation. *Carnivore Diagnostic Tool*. <http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm>. Online, March 2006; Nabbali, Talitha, and Mark Perry. "Going for the Throat: Carnivore in an Echelon World: Part 1," *Computer Law and Security Report* 6 (2003): 456–467; Nabbali, Talitha, and Mark Perry. "Going for the Throat: Carnivore in an Echelon World: Part 2," *Computer Law and Security Report* 20 (2004): 84–97.

Mark Perry

***Carroll v. United States*, 267 U.S. 132 (1925)**

The National Prohibition Act, also known as the Volstead Act, was passed by Congress in 1919 and prohibited the manufacturing, transportation, and sale of alcoholic beverages. On January 16, 1920, the Volstead Act came into force as the Eighteenth Amendment, later repealed in 1933 by the Twenty-first Amendment.

George Carroll and John Kiro were indicted and convicted for transporting intoxicating spirituous liquor in an **automobile** in the amount of 68 quarts of whiskey and gin in violation of the National Prohibition Act. Carroll and Kiro contended that the search of their automobile and the discovery of the alcohol was the

product of an illegal search and seizure in violation of their Fourth Amendment rights.

On September 21, 1921, three men, Carroll, Kiro, and Kruska entered an apartment in Grand Rapids, Michigan, and met three undercover federal prohibition agents, Cronewett, Scully, and Thayer. Cronewett, using an alias, was introduced to Carroll and Kiro, and stated he wanted to buy three cases of whiskey. Carroll and Kiro stated that they had to go east of Grand Rapids to obtain the alcohol and would be back in about an hour. After the time had passed, Kruska returned in an Oldsmobile roadster, the registration number of which Cronewett noted, and stated they could not get the alcohol that night but would return the following day to deliver it. The sellers never returned.

Cronewett and his colleagues maintained patrol on the road between Grand Rapids and Detroit, looking for violators of the National Prohibition Act as part of their regular duties. On October 6, 1921, Carroll and Kiro passed Cronewett and Scully, who were breaking for lunch, in the same Oldsmobile Roadster the agents had noticed a month prior. The agents engaged in a pursuit, but lost the men in East Lansing. More than two months later, on December 15, 1921, Carroll and Kiro again passed the agents. This time the agents were able to catch the two men east of Grand Rapids. Upon stopping them, the agents searched the roadster and found 68 bottles of liquor behind the upholstery of the seats. The two men were arrested.

The question before the Supreme Court was whether the search and seizure of the alcohol in this case violated Carroll and Kiro's Fourth Amendment rights. Chief Justice Taft delivered the opinion of the Court, including an extensive review of statutory and case law. These references demonstrated that the guaranty of the Fourth Amendment right against illegal search and seizures had long recognized a distinction between the search of a home or structure and that of a vehicle or ship. The distinction is based on the practicability of obtaining a **search warrant**. The Court demonstrated that it was easier to obtain a warrant for a structure, whereas it was not practicable to secure a warrant for a moveable object like a vehicle, because the vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought.

Next the Court determined under what circumstances a warrantless search of a vehicle might be made. The majority stated that it would be intolerable and unreasonable if a prohibition agent were authorized to stop every automobile on the chance of finding liquor, and thus subject all persons lawfully using the highways to the inconvenience and indignity of such a search. Those entitled to use the public highways have a right to free passage without interruption or search unless probable cause for believing that their vehicles are carrying contraband or illegal merchandise is known to a competent official who is authorized to make searches. In this case, the agents had probable cause or reasonable basis to believe that Carroll and Kiro were transporting alcohol. They appeared in the same vehicle that they had used in October; were followed into a neighborhood notorious for manufacturing and importing illegal spirits; and, had been seen on different occasions making the trip between Detroit and Grand Rapids. It was clear, according to the Court, that in this case the officers had justification for the search and seizure. The facts and circumstances within their knowledge and the trustworthy information were sufficient in themselves to establish a reasonable belief that liquor was being



transported in the automobile which they had stopped and searched. Therefore, in this case, Carroll and Kiro's Fourth Amendment rights were not violated. The search and seizure of the vehicle were warranted by the inherent mobility of the vehicle and by the probable cause the officers had that the two men were transporting alcohol.

See also: **Automobile search; Cady v. Dombrowski, 413 U.S. 433 (1973); Schmerber v. California, 384 U.S. 757 (1966); South Dakota v. Opperman, 428 U.S. 364 (1976); Stop and frisk; Terry v. Ohio, 392 U.S. 1 (1968)**

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hubbard, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow Publishers, 2000.

Matthew M. Dwyer

CCTV. *See* Surveillance cameras

Cellular telephone

The privacy issues surrounding cellular telephones (alternatively, "cell phones," "wireless," or "mobile phones") are in some ways simply the union of the issues of telephony and radio communications generally. While enabling long-distance voice communication and data transfer, these antecedent technologies simultaneously opened up the potential for eavesdropping, particularly by state law enforcement and intelligence-gathering organizations. However, the inherent mobility of the cellular phone has both complicated these issues and introduced new ones. Since their earliest deployment in the 1980s, cell phones and their supporting infrastructure have proliferated around the globe, making them the most common personally carried electronic device. Their impact on communication has powerfully reshaped social mores and the boundaries between public and private space, so that today cell phones are iconic of the tension intrinsic to mobile communications: an almost constant connection to a pervasive information network, favoring individuated, electronically mediated experience over physically proximate social interaction. Cell phones (and related devices such as personal digital assistants, or PDAs) are and will continue to be pivotal indicators of the interdependence of privacy norms and information technology.

The broad adoption of cell phones by the consumer market (and the privacy implications therein) depended on the solution of three crucial technical challenges: portability, bandwidth limitations, and integration with existing telephone networks. As with many information technologies generally, innovations in electronics manufacturing—in particular chip microminiaturization and the gradual increase in power density of small, dry-cell batteries—allowed cell phones to be

reduced to an easily portable size. While previous generations of “mobile” radio communication equipment could be moved or even mounted in vehicles, in general they were far too unwieldy to be carried personally and were limited in range. Just as importantly, however, fixed telephones relied on wires and offered duplex communication (i.e., simultaneous transmission and reception). For a radio-based system, this meant two frequencies or channels were required per user (one to transmit, one to receive), and as the density of users in a given area increased, so did the demand for available channels (or bandwidth). This issue was solved through the development of cellular networks, whereby a geographic region was segregated into cells, each having its own central relay tower and using a range of radio channels distinct from adjacent cells. The arrangement allowed for the reuse of channels within nonadjacent cells, and more than two decades of new cell establishment and further innovations in digital signal processing have sought to match commercial providers’ call-handling capacity with increasing consumer demand. Finally, despite significant differences in the underlying technology, cellular systems had to be integrated with existing telephone networks, both technically and culturally. For example, users had to be able to call fixed phones from cell phones (and vice versa), and the phones themselves had to have a familiar “user interface” (that is, their operation had to strongly resemble that of fixed phones).

As a direct descendant of previous telecommunication technologies, cell phones have inherited from them their fundamental privacy challenges, significant advances in signal encryption notwithstanding. In the nineteenth century, the signaling and communication demands of railroads, steam-powered ocean vessels, the news media, and big business brought the dawn of the telecommunications era: the telegraph and Morse Code in the 1840s and 1850s; the telephone and telephone exchanges in the 1870s and 1880s; and “wireless,” or radio, after the turn of the century. While these developments significantly extended the physical distance over which instantaneous communication could occur, they also incurred the possibility of electronic eavesdropping or **wiretapping** (in the cases of telegraphy and telephony) or broadcast interception (in the case of radio). Early on, communications security was primarily a concern of large state and commercial users engaged in business or intelligence gathering, but as telecommunications proliferated and became culturally accepted in private residences, surveillance of citizens by the state became an attractive possibility to law enforcement agencies. In recent decades, the growing value of contact information as a commodity (e.g., for **telemarketing** or fundraising) has made the privacy status of telephone *numbers* (including cell phone numbers) an important controversy.

The true innovation of the cell phone from the users’ perspective—communications *mobility*—has opened new, explicitly spatial dimensions in privacy discussion. Cell phone technology is commonly described as having gone through three generations: analog cellular or “first generation” systems, digital or “second generation” systems, and multimedia or “third generation” systems. Beginning with the first generation, cell phones have reshaped the culturally negotiated boundary between public and private space. Once a somewhat intimate practice restricted to the **home**, office, or phone booth, telephone conversation has moved into subways, grocery stores, and many other public venues. Requests to curb cell phone use are often made explicitly to preserve the character of previously well-defined social spaces, protecting privacy and limiting distraction in hospitals, theaters, classrooms, and other places.

Newer generations of cell phones have compounded this spatial reconfiguration by integrating other technologies. Ostensibly required to ensure seamless switching between cells, a cell phone's location can be determined using a number of techniques (such as a **global positioning system** (GPS), for example), with or without the user's knowledge. While this offers clear advantages for some relatively benign applications (e.g., the automatic localization of emergency callers), the **Federal Bureau of Investigation (FBI)** and other agencies have recently lobbied to have such information available for **surveillance** and also incorporated into permanent phone records for law enforcement purposes. Along with other "location-aware" technologies, this has resulted in an entirely new privacy regime: that of *locational* privacy (i.e., the right to limit knowledge of a person's specific whereabouts). Challenging the public/private boundary even further, third-generation cell phones have integrated digital cameras or video recorders, allowing instant image collection and transmission. The significant privacy concerns introduced with closed-circuit television and other imaging systems are extended via this ubiquitous personal device, making "public spaces" just as often *surveilled* spaces.

Communications mobility yields several other shifts in the landscape of privacy concern. When restricted to the home, telephones were largely a *household* property, and their use by children and young adults was administered by the older adults of the household. Today, cell phones and accounts are typically considered *individual* property and often get distributed to children by parents concerned with their safety. On the one hand, this has made it more difficult to constrain what information children give out over the phone; on the other, it contributes to the broad sublimation of constant parental surveillance, a distinct shift in privacy norms. In another example, the poor quality and coverage of telephone and other ground lines in developing countries has made cell phones an enormously popular alternative, creating differentials in the acceptance and proliferation of cell phone use (and in culturally inflected understandings of "privacy"). Also, the integration of identification technologies such as caller ID (more common to cell phones than to fixed phones) has incrementally eroded the privacy of a previously anonymous act, while the very recent availability of inexpensive, limited-time "disposable cell phones" provides a counter example of privacy *enhancement*. As the digital information employed by cell phones is expanded, standardized, and more fluidly exchanged (e.g., through technologies such as Voice-Over-Internet Protocol, or VoIP), these small devices will continue to have broad and varied privacy implications.

See also: **Electronic Communication Privacy Act of 1986; Do-not-call registry; Internet; Manners; Public/private dichotomy; Telecommunication Act of 1996**

Suggested Reading: Diffie, Whitfield, and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press, 1999; Electronic Privacy Information Center. *Privacy*. <http://www.epic.org/privacy>. Online, March 2006; Katz, James E. *Perpetual Contact: Mobile Communication, Private Talk, Public Performance*. Cambridge: Cambridge University Press, 2002; Levinson, Paul. *Cellphone: The Story of the World's Most Mobile Medium and How It Has Transformed Everything!* New York: Palgrave Macmillan, 2004; Ling, Rich. *The Mobile Connection: The Cell Phone's Impact on Society*. San Francisco:

Morgan Kaufmann Publishers, 2004; Spiked Online. *Do Mobile Phones Invade Our Privacy?* <http://www.spiked-online.com/>. Online March 2006.

Lane DeNicola

Central Intelligence Agency (CIA)

The Central Intelligence Agency is part of the American intelligence community, which is led by the director of national intelligence. Primarily, the CIA is responsible for collecting, analyzing, and reporting information about foreign governments, corporations, individuals, and multinational or para-national groups to U.S. government agencies and branches. The CIA describes its mission as being “the eyes and ears of the nation.” The second aspect of the mission of the CIA is to furnish relevant and objective analysis of international intelligence. The third aspect of the agency’s mission is to be the government’s “hidden hand” in conducting covert action to preempt threats to U.S. security or to achieve national policy objectives. Those covert operations are conducted at the direction of the president under the supervision of the director of the CIA.

After World War II and in the face of the increasing threat of Communism and the beginning of the Cold War, the U.S. Congress created the Central Intelligence Agency as the successor to the OSS (Office of Strategic Services), which ceased to exist in October 1945. The CIA came into existence with the signing of the National Security Act of 1947. While the CIA is charged with the task of collecting intelligence, it has no police power, no power of subpoena, no law enforcement powers, and no internal security functions within the United States. Its focus on foreign governments, businesses, and individuals places its activity *outside* the United States, since Congress created the agency to protect the privacy and security of U.S. citizens. The areas that are of greatest importance in the work of the CIA include international organized crime, narcotics trafficking, counterterrorism, counterintelligence, nuclear nonproliferation, the environment, and arms control intelligence.

The agency is organized into several departments, the most notable of which are the Directorate of Intelligence, which analyzes intelligence from all sources on key foreign issues; the National Clandestine Service, which undertakes covert collection of foreign intelligence; and the Directorate of Science and Technology, which creates and applies new technology to collect intelligence.

The standard euphemism for the CIA is the “other government agency.” That veiled reference is used when the CIA is involved in a situation but the United States cannot confirm the CIA’s involvement. Other colloquial names for the CIA are “the Agency” and, most commonly, “the Company.” People who work for the CIA are often called “spooks” or “spies,” as are persons who work for other intelligence agencies throughout the world. Because the headquarters of the CIA is located in Langley, Virginia, which was open farmland when the agency was formed and the headquarters was constructed, employees of the agency are often called “Virginia farm boys.”

Documentation indicates that at the time of the CIA’s creation in 1947, many former Nazi operatives were recruited to be agents. In return, those operatives were promised immunity from prosecution for war crimes committed during World War II (Operation Paperclip). In 1949 Congress passed a law that essentially allowed

the CIA to operate in complete **secrecy** and without the limitations generally applied to the use of federal funds. That law also created a program that permitted defectors from other countries and persons considered essential to national security to be admitted to the United States without going through the normal immigration processes, to be provided with new identities, and to be provided financial support.

Within that Congressionally sanctioned secrecy, the CIA began the first “structured behavioral control program” in the early 1950s. At the time, there was little involvement or oversight of the CIA’s activities by other government agencies. That was generally explained on the basis of the need to maintain secrecy to protect the agents, sources, and methods employed by the agency. The CIA was also trying to match the capabilities of the KGB, the agency of Russian spies, in an effort to keep ahead of the Communist group. The early 1950s was also a time of rapid expansion of the reach of the agency.

Throughout the Cold War and under the Communist threat, the CIA was allowed to carry out its operations without much oversight or interference until the early 1970s. The eruption of the Watergate scandal and the efforts of Congress to exercise its oversight power over the executive branch of the government began to expose the activities of the CIA. When Watergate became a national issue, President Nixon tried unsuccessfully to have the CIA convince the **Federal Bureau of Investigation (FBI)** that an investigation of Watergate would reveal too much about the involvement of the CIA in such past activities as the Bay of Pigs invasion. At about the same time, James Schlesinger, who was then director of central intelligence, authorized a series of reports that brought to light vast wrongdoing by the CIA. Those reports were often referred to as “the family jewels.” The general public probably would have known nothing of that sordid history had not a *New York Times* reporter published a story documenting the involvement of the CIA in the assassination of certain foreign leaders. The story also revealed that the CIA had been keeping files on thousands of American citizens who had been involved in the peace movement during the Vietnam War and those opposing nuclear proliferation.

In light of those revelations, by 1975, after intensive Senate and House investigations, the CIA was prohibited from future assassinations of foreign leaders, and the agency was notified that a prohibition against spying on Americans would be enforced. That trend has been reversed, however. After the September 11, 2001, attacks on the World Trade Center and the Pentagon, many restrictions on the tactics of the CIA were removed. At the same time, the Intelligence Reform and Terrorism Prevention Act of 2004 instituted a number of changes in the structure of the government’s management of domestic and foreign intelligence.

Over the past 60 years or so, the CIA has conducted a number of operations that have become quite famous. Those that have reached public awareness include:

- A mind-control program called MKULTRA that was conducted in the United States in the 1950s and 1960s;
- A “false flag” operation in Italy designed to discredit leftist groups by conducting terrorist operations for which they would be blamed;
- Numerous efforts in Eastern Europe to limit the scope of Soviet influence;
- The overthrow of the Mossadegh government in Iran in 1953;

- The overthrow of the democratically elected government of Guatemala in 1954;
- The Bay of Pigs invasion of Cuba in 1961;
- Efforts to assassinate Fidel Castro, head of state in Cuba;
- Involvement in a secret war in Laos between 1962 and 1975;
- Involvement in the Nicaragua “contra” conspiracy and sale and trafficking of cocaine; and,
- Involvement in the coup in Chile in 1973.

The CIA and its activities, particularly its covert activities, have been the source of controversy since the agency’s creation. The CIA is criticized for breaking the laws of other nations, attempting assassinations, and disseminating propaganda. More recently, a great deal of public attention and ensuing controversy have surrounded accusations of torture against prisoners and the existence of secret prisons in foreign countries to which prisoners are taken in circumvention of American legal restrictions and Geneva Convention restrictions against the use of torture. However, the defenders of those practices believe that they are necessary to protect national security.

Historically, the CIA has abrogated the privacy of foreign citizens to protect the privacy and security of U.S. citizens. Recently, many critics and many American citizens have voiced the opinion that the lack of controls on the intelligence gathered by the CIA, the FBI, and other intelligence agencies abrogates the right to privacy that is constitutionally guaranteed to American citizens. Key issues in the debate over the authority to violate personal privacy concern racial or ethnic profiling, wiretapping, monitoring of personal communications via **cellular telephones**, access to personal records that show the reading habits of private citizens, monitoring of **electronic mail** and other **Internet** use, monitoring of personal movement via the **Global Positioning System (GPS)**, and the use of **radio frequency identification (RFID)** chips to track the movement of pets, personal goods, and items shipped, among others.

In addition, questions on the legality of spying on American citizens who are not under investigation for a crime, and without a court order or **search warrant**, are arising. If there are no controls over spying against Americans or foreigners, there is also no control over the type of information collected or the way it is used. Although many Americans have been willing to relinquish certain rights to privacy in the post-9/11 climate of concern for national security, it has not been established that those same Americans are willing to relinquish all personal rights in favor of uncontrolled access by government agencies.

Some argue in favor of controls, noting that an attack by terrorists or another government requires months of planning, which would provide ample opportunity for government agencies to obtain the necessary warrants before initiating spying or **surveillance** activity. They point to a larger concern that, without warrants defining the information that can be obtained or the means by which it can be obtained, it becomes possible for any government agency to collect any kind of information on any individual residing within the United States.

The CIA, which serves as the “eyes and ears of the nation,” is in danger, according to some, of turning its surveillance activities on U.S. citizens. The current



debate over the scope and limitations of CIA power, especially in this age of electronic snooping, may well define the agency's role in American government for the coming decades.

See also: **Constitutional protections; Electronic surveillance; Foreign Intelligence Surveillance Act of 1978 (FISA)**

Suggested Reading: Baer, Robert. *See No Evil: The True Story of a Ground Soldier in the CIA's War on Terrorism*. New York: Three Rivers Press, 2003; Blum, William. *Killing Hope: U.S. Military and CIA Interventions since World War II*. Monroe, ME: Common Courage Press, 2003; Central Intelligence Agency. *About the CIA*. www.cia.gov. Online, April 2006; Chomsky, Noam. *Hegemony or Survival*. New York: Henry Holt, 2003; Darling, Arthur B. *The Central Intelligence Agency: An Instrument of Government, to 1950*. State College: Pennsylvania State Press, 1990; Hulnick, Arthur. *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century*. Westport, CT: Greenwood, 1999.

Gregory M. Duhl

Children's Online Privacy Protection Act of 1998 (COPPA)

In 1998 Congress passed the Children's Online Privacy Protection Act, 15 U.S.C. §§6501–6505 (COPPA), in response to a 1998 Federal Trade Commission (FTC) report that described the widespread collection and use of **personally identifiable information** of children without their parents' knowledge or consent. The FTC was charged with enforcing the act and issuing COPPA rules. The final COPPA Rule was issued in 1999 and became effective in April 2000.

COPPA aims to protect the personal information of children (persons under the age of 13) online. The final COPPA rule requires parental consent before a commercial website or an online service directed at children (or a website or online service that has knowledge that it collects personal information from children) collects, uses, or discloses personal information about a child. The COPPA rule also requires that websites and online services "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children." In addition, entities subject to this act must allow parents to access any personal information on their child and delete it or opt out of future collection, and such entities must limit their collection of children's personal information to that which is reasonably necessary to participate in the activity. Furthermore, site operators cannot condition participation in an online activity upon the disclosure of more personal information than is necessary to participate in that activity. COPPA also requires that websites subject to the act must post a privacy policy informing parents of their privacy practices and the contact information for each operator of the website. The required privacy policy must be linked to a conspicuous place on the website's homepage and on any page on which a child is asked to provide personal information.

COPPA does not apply to **Internet** service providers or nonprofit entities, but it does apply to domestic websites and foreign websites directed at children in the United States. The types of personal information that are regulated by COPPA include a child's full name, physical address, **electronic mail** address, **Social Security number**, telephone number, and a persistent identifier—such as a cookie—that is combined with personal information. COPPA includes a "safe harbor"

provision that allows entities and industry groups to request FTC approval of self-regulatory guidelines.

Violators of the act may be subject to an injunction and civil penalties of up to \$11,000 per violation. Although the FTC has enforcement authority for COPPA, the commission has brought few cases under the act. However, the FTC has issued warning letters to dozens of website operators. In addition to FTC enforcement, COPPA empowers states and select federal agencies to enforce the act within their jurisdictions.

Many criticisms have been leveled at COPPA. Some critics argue that the various parental consent mechanisms outlined by the FTC are too cumbersome, too slow, and too expensive. Furthermore, these critics argue, the parental consent mechanisms are inadequate to protect children's privacy because children can simply fabricate information to access sites, and sites can evade COPPA regulation by stating that they do not sell products to children. Other critics have argued that defining a child as a person under the age of 13 is arbitrary and unjustified, inasmuch as children over the age of 13 may also need online privacy protection. Finally, some commentators have argued that COPPA may not pass constitutional muster because requiring children to divulge personal information or verify that they are entitled to access information as a condition to accessing the information results in the chilling of speech and, thus, a violation of the First Amendment. Similarly, critics argue that the forced relinquishment of the right to anonymous communication may run afoul of the First Amendment.

Suggested Reading: Allen, Anita L. "Minor Distractions: Children, Privacy & E-Commerce," *Houston Law Review* 38 (2001): 751–776; Federal Trade Commission. <http://www.ftc.gov>. Online, March 2006; George, Joey F. (ed.). *Computers in Society: Privacy, Ethics and the Internet*. Upper Saddle River, NJ: Pearson Prentice Hall, 2004; Gurak, Laura. *Persuasion and Privacy in Cyberspace: The Online Protests over Lotus Marketplace and the Clipper Chip*. New Haven, CT: Yale University Press, 1997; Savitt, Nancy L. "A Synopsis of the Children's Online Privacy Protection Act," *St. John's Journal of Legal Commentary* 16 (2002): 631–640.

Marcy E. Peek

***Chimel v. California*, 395 U.S. 752 (1969)**

One afternoon in 1965, three police officers arrived at Chimel's California **home** with a warrant authorizing them to arrest Chimel for the burglary of a coin shop. Chimel's wife ushered them in, where they waited for 10 or 15 minutes before Chimel arrived home from work. When he arrived, one of the officers handed him the arrest warrant and asked if they could look around. Chimel objected, but the officer advised him that on the basis of the lawful arrest they would nevertheless conduct a search. The officers did not have a **search warrant**.

Accompanied by Chimel's wife, the officers searched the entire three-bedroom house, including the attic, the garage, and a workshop. In two of the rooms, the officers had Chimel's wife open drawers and physically move contents so that they "might view any items that would have come from the burglary." The officers seized a number of items: primarily coins, but also several medals, tokens, and other objects. The entire search took between 45 minutes and an hour. At Chimel's trial, these items were admitted as evidence against him over his objection that they



had been unconstitutionally seized. He was convicted, and the conviction was affirmed by both the California Court of Appeals and the California Supreme Court. Both courts conceded that the arrest warrant was invalid because it was set forth in conclusory terms, but that because the officers had procured it in good faith and their actions were based on probable cause, the arrest was nevertheless lawful. Therefore, the courts found that the search incident to the valid arrest was justified.

The United States Supreme Court granted certiorari; it accepted the California courts' findings that the arrest was valid, and it considered only whether the warrantless search of Chimel's house could be constitutionally justified as a search incident to that arrest. In its decision, the Supreme Court reversed the California Supreme Court. The Court began its analysis by reciting the progression of case law leading from the limited suggestion found in the dicta of *Weeks v. United States*, 232 U.S. 383 (1914), which upheld the search of the person incident to a lawful arrest, to the expansive holdings of *Harris v. United States*, 331 U.S. 145 (1947).

Both *Harris* and *United States v. Rabinowitz*, 339 U.S. 56 (1950), extended the search incident to the surroundings within the person's possession or control. It was upon these cases that the state had relied in its argument that the search was lawful. The dubious progression of these cases led the Supreme Court to find that the doctrine as pronounced in *Rabinowitz* could withstand neither historical nor rational analysis. The warrant requirement serves a high function, protecting privacy from government invasion as guaranteed in the Fourth Amendment. The Court affirmed that when an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect an escape. It is also reasonable, the court held, for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction. The area into which an arrestee might reach in order to grab a weapon or evidentiary items is also governed by a like rule: a gun on a table or in a drawer in front of the arrestee. The court explicitly overruled *Harris and Rabinowitz*, however, to the extent that those cases allowed officers to engage in warrantless searches not justified by probable cause. Here, the search went far beyond Chimel's person and the area from within which he might have obtained a weapon or some piece of evidence that could have incriminated him. The Court held that this search was unlawful and reversed Chimel's convictions.

Mr. Justice Harlan concurred in the opinion but questioned the Court's overruling of *Harris* and *Rabinowitz*, expressing concern about the workability of the expanded warrant system inherent in the majority's opinion. Justice White, joined by Justice Black, dissented. The dissent expressed concern that Fourth Amendment jurisprudence was changing all too rapidly, and that it would be unwise to abandon the latest rulings in this area. Like the concurrence, the dissent argued that the holding in this case, and the explicit overruling of *Harris* and *Rabinowitz*, would unreasonably require police to leave the scene of an arrest in order to obtain a search warrant when they may already have probable cause. It argued that Chimel's life and privacy had already been disrupted by the arrest; the officers' subsequent search of his premises was a "relatively minor intrusion." The dissent held with the most recent cases: once probable cause exists, the fact that there is no warrant does

not make a search incident to a lawful arrest unreasonable or unlawful, and the dissent did not limit this holding, as did the majority, to a search only of the person and the immediate and accessible surroundings.

See also: California v. Ciraolo, 476 U.S. 207 (1986); *Payton v. New York*, 445 U.S. 573 (1980); *United States v. Dunn*, 480 U.S. 294 (1987); *Warden v. Hayden*, 387 U.S. 294 (1967)

Suggested Reading: Barteo, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow Publishers, 2000.

Larkin R. Evans

Civil liberties. *See* Constitutional protections

Civil service laws

Civil service laws dominate public employment in the United States. The principles of selection based on merit and of the personal accountability of government employees on which these laws rest may conflict with personal privacy. Therefore, courts and government officials have struggled to accommodate civil service laws with personal privacy.

Based in part of reforms in New York state, the Civil Service Reform Act of 1883 created the modern federal civil service. Civil service in the federal government and in the states rests on selection by competitive examination and on protections for career employees from arbitrary personnel actions. Civil service laws implicate issues regarding the protection of the personal privacy of public employees. Some concerns about privacy arise from the selection of public employees. For example, the interests of the public employer in hiring some categories of public employees, such as police officers, may outweigh the privacy interests of employees. Private information sought could include medical and psychological information; polygraph tests; financial information; and information regarding drinking, gambling, and arrest records, including those of relatives. In some instances, the interests of the public employer in the selection of categories of public employees can outweigh even strong interests in privacy.

Selection procedures often require inquiry into the past conduct of persons seeking government employment, conduct that reflects on their honesty, integrity, and qualifications. This inquiry requires the cooperation of persons with information about these candidates. Privacy provisions, however, such as those in the **Privacy Act of 1974**, give persons access to records about themselves. Such access reduces the likelihood that third persons will candidly respond to inquiries. Therefore, the



Privacy Act of 1974 contains an exemption from its access provisions for investigatory material compiled for the purpose of determining the suitability, eligibility, and qualifications for civilian federal employment. This exemption, however, only protects a confidential source providing information under an express promise of **confidentiality**.

Some concerns about privacy arise from the principle of personal accountability in civil service laws. Civil service laws hold employees accountable through the investigation and punishment of misconduct and poor performance. Such accountability implicates personal privacy. For example, the constitutional protection against unreasonable searches and seizures applies to government employees. Depending upon the circumstances, a public employee may have a reasonable expectation of privacy regarding the workplace. The Supreme Court, however, has dispensed with the requirement of a warrant based on probable cause in public employment. Instead, the Court decided that all work-related searches of public employers need only meet the standard of reasonable under all the circumstances.

Moreover, the Supreme Court permits some searches without a suspicion of wrongdoing by a specific public employee. For example, the Court has approved random **drug testing** of categories of employees whose use of illegal drugs pose particular risks. Examples of such categories of employees include customs employees seeking transfer or promotion to positions involving drug interdiction, employees carrying firearms, guards, police, employees flying or maintaining aircraft, chemical and nuclear workers, firefighters, and motor vehicle operators.

Statutory provisions, like the Privacy Act of 1974, may affect the conduct of investigations of federal employees. The act provides that to “the extent practicable,” information be acquired from the subject of an inquiry. This requirement encourages managers to seek information from employees first. In some cases, however, it is not practicable to do so because the inquiry would alert employees to an ongoing investigation.

Because the Privacy Act of 1974 gives persons the right to access and review records regarding them, this right may influence civil service investigations. Although access and review help guarantee the accuracy of government information identified with a particular person, these rights may also give employees premature access to investigative files and may identify witnesses. The exemptions to the act temper interference with civil service discipline. Exemptions to the right of access and review regarding criminal investigations or regarding information compiled in the reasonable anticipation of “a civil action or civil proceedings” are likely to apply to many civil service investigations.

Accountability may require dissemination to the public of information regarding the misconduct, performance, and punishment of public employees. Particularly when the misconduct is egregious or places the public at risk, disclosures assure the public of the integrity and effectiveness of the civil service. This assurance supports public confidence and trust in the operations of government. These disclosures, however, may also threaten privacy.

See Also: **Constitutional protections; Disclosures; Open meetings laws; Public records**

Suggested Reading: Lee, Yong S., and David H. Rosenbloom. *A Reasonable Public Servant: Constitutional Foundations of Administrative Conduct in the*

United States. New York: M.E. Sharpe, 2005; Vaughn, Robert G. *United States Merit Systems Protection Board: Rights and Remedies*. New York: Law Journal Press, 2006; Vaughn, Robert G. *Principles of Civil Service Law*. New York: Matthew Bender, 1976.

Robert G. Vaughn

Click stream data. See Internet

Clinton-Lewinsky scandal

The Clinton-Lewinsky scandal dominated news headlines in the United States, with reverberations heard around the world, throughout the second term of President William J. Clinton. The scandal centered on a consensual, sexual affair involving the president and a young White House intern named Monica Lewinsky. Facts about the affair were made public in the course of Independent Counsel Kenneth Starr's far-reaching inquiry into what began as accusations of financial improprieties in the Whitewater land deal. Starr's probe culminated in a vote on December 19, 1999, by the U.S. House of Representatives to approve two articles of impeachment against the president on charges that included perjury and obstruction of justice in connection with Clinton's efforts to suppress information about his relationship with Lewinsky. The events surrounding the revelation of the Clinton-Lewinsky affair elicited widespread concern about dwindling privacy protections for public figures and private citizens in the contemporary United States. Frequently likened to a form of "new **McCarthyism**," the Starr probe in particular came to emblemize the pathologies of a society that no longer respects the right to privacy. The media was also widely condemned for what many considered to be excessive coverage of the details pertaining to a private affair.

The origins of the scandal lie in two other legal imbroglios that dogged Clinton throughout his presidency: the investigation of the Whitewater land deal and the Paula Jones sexual harassment lawsuit. In 1994, during Clinton's first term in office, Attorney General Janet Reno appointed Robert Fiske, Jr., as independent counsel to investigate the financial dealings of the Whitewater property company. The president and his wife, Hillary Rodham Clinton, were accused of colluding with their friends and business partners, James and Susan McDougal, to reap profits, tax breaks, and financial favors from the deal. The Clintons denied any wrongdoing, emphasizing throughout the investigation that they had in fact lost money on the Whitewater venture.

In August 1994, Fiske was replaced as special prosecutor by Kenneth Starr, a well-known conservative who had served as the solicitor general for the Justice Department under President George H. W. Bush. At about this time, a former Arkansas state employee named Paula Jones filed a sexual harassment lawsuit against Clinton, charging that in 1991 he had ordered a pair of Arkansas state troopers to escort her to a hotel room where then-governor Clinton had made unwelcome sexual advances. Jones claimed that she filed her suit in an effort to salvage her reputation after conservative journalist David Brock had published an article naming Jones as a participant in one of Clinton's many extramarital affairs.

Meanwhile, in July 1995, 22-year-old Monica Lewinsky joined the White House staff as an unpaid intern, and in November 1995 she took a paid position at the White



House Office of Legislative Affairs. Two days later, a sexual relationship between the President and Lewinsky began during the government furlough. According to later testimony, the affair continued intermittently for the next 18 months.

In May 1996 the first Whitewater trial ended, and both of the McDougals were convicted of fraud. A month later, a Senate hearing on Whitewater ended inconclusively. Shortly thereafter, Starr announced that he would step down, but four days later he suddenly changed his mind and decided to continue his investigations. It soon became clear that Starr had shifted the focus of his investigation from a concern with financial affairs to an interest in intimate ones. Following on the heels of a story published in *Newsweek* magazine detailing the president's alleged sexual advances toward White House staffer Kathleen Willey, Lewinsky was subpoenaed in December 1997 by lawyers for Paula Jones; in a sworn affidavit, Lewinsky denied having an affair with the president. Soon thereafter, Lewinsky confidante Linda Tripp turned over to Starr over 20 hours of taped telephone conversations with the unwitting Lewinsky that contained admissions of Lewinsky's sexual relations with the president. In January 1998, Matt Drudge published Lewinsky's name on his website, as well as a report that *Newsweek* had obtained the Tripp-Lewinsky tapes but had pulled a story about them under pressure from Starr, who feared it would jeopardize his investigation. On January 21, 1998, following a *Washington Post* report on his relationship with Lewinsky, Clinton told a television interviewer that "there is no improper relationship." One week later, before an invited media audience at the White House, Clinton insisted, "I want you to listen to me. I did not have sex with that woman, Monica Lewinsky."

Several months later, Lewinsky's lawyers struck an immunity deal with Starr, in which she agreed to provide "full and truthful testimony" in exchange for full immunity from prosecution. For the next 15 days, Lewinsky was questioned by the grand jury. Shortly thereafter, the president was asked to provide a blood sample for **DNA testing** to determine if it was a match with semen stains found on a blue dress Monica Lewinsky had kept in her closet following a sexual encounter with the president. Two weeks later, President Clinton admitted to the grand jury that he had had "inappropriate intimate contact" with Ms. Lewinsky, although he continued to hold that his earlier statements had been accurate, explaining at one point that his answer to the question about the nature of his relationship with Lewinsky "depends on what the meaning of 'is' is."

In September 1998, Starr submitted his report to Congress, and despite its graphic sexual content, the report was immediately posted on the congressional website, with particularly salacious portions reprinted in newspapers and on websites around the world. One month later, the House of Representatives voted to hold an impeachment inquiry. In November Clinton settled the Jones lawsuit for \$850,000 without acknowledging guilt. In December, the House Judiciary Committee approved four articles of impeachment. The full House approved two of the articles, and Clinton became only the second sitting president in the history of the United States to be impeached. The Senate trial began in January 1999, and a month later the President was acquitted.

The Clinton-Lewinsky scandal spawned widespread reconsideration of the meaning and extent of privacy rights in the contemporary United States. Throughout the ordeal, many suggested that the real scandal lay not in the fact that the president had had an extramarital affair, but rather in the invasion of the president's

privacy by the independent counsel's office and the media. While scandals are nothing new in U.S. politics—nor is the tendency for presidents from Jefferson to Kennedy to stray from the terms of the marital oath—the Clinton-Lewinsky scandal set a new standard in terms of the public's sense of its right to know personal details about public figures.

In the wake of the scandal, no clear consensus emerged about who to blame for the breakdown of respect for the principle of privacy. Special Prosecutor Starr was frequently chastised in the media for his tactics, which included the subpoena of records of sale from a local Washington, D.C., bookstore and the reliance on methods of intimidation in interrogating Lewinsky. Such seeming abuses of prosecutorial discretion led to calls for a repeal of the statute authorizing special prosecutors, as well as demands to curtail prosecutorial discretion in an investigation of sexual harassment charges.

The media was charged with violating privacy as the scandal unfolded. The president's affair with Lewinsky dominated headlines in the mainstream media for an extended period, leading to complaints that journalists had abdicated their responsibility to guard the public interest. The scandal also raised concerns about the growing influence of alternative and nontraditional media, including web-based news sites such as the *Drudge Report* and AM-frequency talk radio stations, which appeared to hold themselves to lower standards of verification and professional comportment when gathering and reporting the news than had been expected of more traditional news outlets.

Throughout the scandal, the feminist movement was frequently identified as a cause of the breakdown of privacy norms in the United States, with second-wave feminism's embrace of the motto "the personal is political" held culpable for the corrosion of the boundary between public and private. At the same time, many self-described feminists rose to Clinton's defense, urging chastened members of the movement to rethink the meaning and limits of the imperative to politicize the personal, and to dedicate themselves to re-conceptualizing privacy rather than abandoning the ideal altogether.

See also: **Journalism; Public/private dichotomy; Sexual harassment; Women and privacy**

Suggested Reading: Apostolidis, Paul, and Juliet A. Williams (eds.). *Public Affairs: Politics in the Age of Sex Scandals*. Durham, NC: Duke University Press, 2004; Berlant, Lauren, and Lisa Duggan (eds.). *Our Monica, Ourselves: The Clinton Affair and the National Interest*. New York: New York University Press, 2001; Howe, Peter. *Paparazzi: And Our Obsession with Celebrity*. New York: Artisan Books, 2005; Maurer, Paul J. "Media Feeding Frenzies: Press Behavior during Two Clinton Scandals," *Presidential Studies Quarterly* 29 (1999): 65–80; Wattier, Mark J. "The Clinton Factor: The Effects of Clinton's Personal Image in 2000 Presidential Primaries and in the General Election," *White House Studies* 4 (2004): 467–488.

Juliet Williams

Clipper and Capstone chips

On April 16, 1993, just a few months after President William J. Clinton took office, the White House proposed the Escrowed Encryption Standard (EES) for the



encryption of voice, fax, and **computer** information transmitted over circuit-switched telephone systems. EES was to be used for the protection of sensitive but unclassified information. The standard, which was nominally a National Institute of Standards and Technology (NIST) effort, included a tamper-proof hardware encryption chip (Clipper) and a key-escrow system. Each hardware chip would have its own key; these keys were to be split and registered at birth—escrowed—with two agencies of the U.S. government (NIST and the Department of Treasury Automated Systems Division were the initial escrow agencies). In other words, this was an encryption system in which the federal government held the private keys.

Keys would be released to law enforcement agents armed with proper authorization. This would enable law enforcement to decrypt intercepted communications. A more advanced chip, Capstone, included additional cryptographic components for **authentication** and integrity checking: Clipper plus a public-key key exchange algorithm, the Secure Hashing Algorithm, the Digital Signature Standard, a high-speed exponentiation engine, and a random number generator.

EES—or Clipper, as it came to be known—is a method for encrypting voice and fax communications that enables easy decryption for legally authorized wiretaps. Such a description badly misses the point. In 1993 the world was on the verge of a communications revolution. Protocols for easy access and display of information on the **Internet** had been developed and were being deployed. This network had been opened for commercial traffic. The World Wide Web was about to burst forth. In very short order, the Internet was transformed from a medium used primarily for scientific communications to a major player in world economic activity. The Escrowed Encryption Standard, which provided a government backdoor into encrypted communications, was proposed at a crucial moment.

The Clipper program was voluntary, but there were many objections anyway. In particular, there was public concern that the U.S. government might seek to prevent the use of non-escrowed systems. In response, the White House stated that there was no intent to require key escrow. Executive Branch activities belied that statement. The U.S. **Communications Assistance for Law Enforcement Act (CALEA)**, first proposed in 1992 and eventually passed in 1994, required that digitally switched telephone networks be built according to **wiretapping** standards determined by the U.S. Department of Justice. In 1992 National Security Advisor Brent Scowcroft described the digital-telephony bill as a “beachhead [that] we can exploit for the encryption fix.”

The government posited that Clipper was an encryption system providing both security and privacy, while enabling government access under legal authorization; however, there were immediate objections to the government’s key-escrow proposal. Of the 320 letters submitted to NIST regarding the Clipper proposal, all but a handful were negative. Civil liberties organizations expressed concerns about threats to privacy. Computer security experts observed that the establishment of escrow agencies was a dangerous concentration of resources, and thus that Clipper diminished rather than increased security. Business, unhappy with export controls on encryption, did not find EES a useful substitute. Nonetheless, in 1994 EES became an official federal information processing standard.

The Escrowed Encryption Standard specifies the use of Skipjack, an encryption algorithm developed by the **National Security Agency (NSA)**, and the creation of a Law Enforcement Access Field (LEAF) to be implemented on a tamper-proof

hardware device. Skipjack uses 80-bit keys, and initially specifics of the algorithm were not made public. Each Clipper chip has an 80-bit device-unique key used by the escrow system.

When two participants with Clipper-enabled telephones establish a connection, they set up a “session key” for that communication, including a phone call and a fax transmission. This session key is used to encrypt the communication. This key is passed to the Clipper chip of the device doing the communicating, which encrypts it using the chip’s device-unique key. This information is combined with the chip’s identifier and other information to form the LEAF, or Law Enforcement Access Field, and is shipped to the other participant’s device. The system is set up so that only if the LEAF decrypts properly can encrypted communications begin. The communication is encrypted with the session key; because the two participants know the key, they can communicate securely. An eavesdropper would need the device keys in order to decrypt the communication. Given the setup of the system, law enforcement would have access to the keys under authorization.

In a strong algorithm, each additional bit of key length increases the security by a factor of two, so unless the government’s backdoor escrowed keys were used for decryption, data encrypted using Skipjack was nominally 2^{24} —or 16 million—times more secure than data encrypted using the Data Encryption Standard, the 1977 federal standard for protecting secure but unclassified data. The increased security was one reason the government hoped for a strong positive reaction to EES. This was not to be. Just months after EES was made into a standard, Matt Blaze, a researcher at AT&T, discovered a way to defeat law enforcement access to the keys during a Clipper-enabled communication (Blaze’s attack did not defeat the EES encryption, just law enforcement access to the encryption keys). The attack was easy to program and demonstrated that Clipper did not fulfill the government’s claims of secure communications and easy government access (under proper legal authorization).

Two years after the approval of EES, only AT&T was producing secure telephones with Clipper chips. The company found few purchasers. U.S. business was not interested. Neither were foreign companies: the issue of law enforcement access to keys for devices used outside the U.S. had never been fully worked out, and this contributed to foreign unease about Clipper. U.S. law enforcement bought some Clipper-enabled phones but was not particularly enamored of the product. Despite extensive U.S. government efforts to encourage other nations to adopt an escrowed approach for encrypted civilian communications, there was little buy-in from abroad. Few wanted secure communications with the U.S. government holding the keys.

Key escrow was part of a larger effort by the U.S. government to slow civilian deployment of strong encryption. By the end of the 1990s, however, the U.S. government changed its direction. Seeing important advantages to the deployment of strong **cryptography** throughout civilian infrastructure, the Clinton administration simplified export-control laws and embraced the use of non-escrowed encryption in the civilian sector, including the adoption of the Advanced Encryption Standard, a strong, symmetric-key algorithm that replaced the aging—and much weaker—Data Encryption Standard.

Suggested Reading: Computer Professionals for Social Responsibility. *Clipper Chip* October 1994. <http://www.cpsr.org/prevsite/program/clipper/clipper.html>.



Online, March 2006; Diffie, Whitfield, and Landau, Susan. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press, 1999; Electronic Privacy Information Center. *Clipper Chip*. <http://www.epic.org/crypto/clipper/>. Online, March 2006; Garfinkel, Simson. *Web Security, Privacy and Commerce*, 2nd ed. New York: O'Reilly Media Inc., 2002; Singh, Simon. *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*. New York: Doubleday, 1999.

Susan Landau

Communications Assistance for Law Enforcement Act (CALEA)

The Communications Assistance for Law Enforcement Act (CALEA) is a federal law passed in 1994 that creates a legal duty for all private telecommunications carriers to ensure that all their equipment and networks have the capability to conduct wiretaps if ordered to do so by the appropriate law enforcement agencies. The law does not change the limitations and restrictions on **wiretapping** procedures originally set out in 1968 by Title III of the Omnibus Crime Control and Safe Streets Act and subsequently amended by other statutes, such as the **Electronic Communication Privacy Act of 1986** and the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)**. CALEA is codified at 47 U.S.C. 1001–1010.

CALEA is a significant milestone in the evolution of the relationship between law enforcement agencies conducting wiretaps and the telecommunications industry carrying out the communications the agencies seek to intercept. In this context, a “wiretap” is defined as an interception of a communication’s content as well as **pen registers** and trap-and-trace devices that seek to trace the destination of outgoing and incoming calls. In 1969, immediately after Congress set out the rules governing wiretapping procedures, a telecommunications company refused to assist the **Federal Bureau of Investigation (FBI)** in conducting a wiretapping operation. This refusal was upheld by a federal appellate court, and a few months later, Congress amended the federal wiretapping statute to require all telecommunications companies to assist law enforcement with any legal wiretapping activity. The new amendment did not create any duty for these private companies to change or upgrade their equipment or networks, primarily because the existing technology used by the telecommunications companies at the time was able to adequately meet the needs of law enforcement officials when they sought to conduct wiretaps.

This began to change during the revolution in telecommunications technology in the 1980s and early 1990s, a revolution that included the gradual switch from analog to digital telephony and the dramatic increase in the use of **cellular telephones**. These emerging technologies posed new challenges to law enforcement agencies seeking to wiretap telephone communications. For example, many cellular phone networks had a limited capacity to conduct multiple wiretaps at the same time, while speed dialing and voice-dialing features sometimes made it impossible to trace the number that had been dialed. In response, Congress passed CALEA, which required telecommunications companies to retrofit all of their equipment and networks to ensure that the companies could, upon request, isolate and deliver to law enforcement the content of communications as well as the destinations and origins of all phone calls for a target telephone. The law also authorized payments

to the private companies to reimburse them for the costs of these upgrades, and the companies were given four years to comply with the CALEA requirements.

On August 5, 2005, the Federal Communications Commission (FCC) issued new rules expanding CALEA's reach to include certain broadband and voice-over Internet Protocol (IP) services, even though such networks fall outside the traditional definition of "telecommunication carrier." The FCC argued that these networks were increasingly being used as replacements for local telephone usage, and so CALEA requirements had to be imposed in order to maintain the ability of law enforcement to conduct effective wiretaps. This move was not without controversy, as numerous privacy groups claimed that CALEA did not and should not be used to cover **Internet** communications.

Suggested Reading: Ask CALEA. *Communications Assistance for Law Enforcement Act of 1994*. <http://www.askcalea.net/>. Online, March 2006; Dempsey, James X. "Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy," *Albany Law Journal of Science & Technology* 8 (1997): 70–71; Froomkin, A. M. "The Death of Privacy?" *Stanford Law Review* 52 (2000): 1461–1544.

Ric Simmons

Communications Decency Act (CDA)

The Communications Decency Act (CDA) was Title V of the United States **Telecommunication Act of 1996**. As passed by Congress, Title V affected the **Internet** and online communications in two significant ways. First, it attempted to regulate both indecency and obscenity in cyberspace that could be available to children. Second, Section 230 of the act declared that operators of Internet services were not to be construed as publishers, and thus were legally liable for the words of third parties who used their services.

The CDA imposed broadcast-style content regulations on the open, decentralized Internet and severely restricted the First Amendment rights of all Americans. There was strong opposition to this legislation because it threatened the very existence of the Internet as a means for free expression, education, and political discourse.

The most controversial portions of the CDA were those relating to indecency and obscenity on the Internet. The relevant sections of the act were introduced as a response to fears that Internet pornography was on the rise. Indecency in television and radio broadcasting had already been regulated by the Federal Communications Commission: broadcasting of offensive speech was restricted to certain hours of the day, when minors were supposedly least likely to be exposed. Violators could be fined and potentially lose their licenses. The Internet, however, had only recently been opened to commercial interests by the 1992 amendment to the National Science Foundation Act and thus was not addressed by many previous laws. The CDA, which affected the Internet and cable television, marked the first attempt to expand regulation to this new sphere.

The CDA prohibited posting "indecent" or "patently offensive" materials in a public forum on the Internet, including web pages, newsgroups, chat rooms, and online discussion lists. The CDA, however, was not about child pornography, obscenity, or using the Internet to stalk children since these activities were already illegal under current law. Free speech advocates, however, worked diligently and



successfully to overturn the portion relating to indecent, but not obscene, speech. They argued that speech protected under the First Amendment, such as printed novels or the use of the “seven dirty words,” would suddenly become unlawful when posted to the Internet. Critics also claimed the bill would have a chilling effect on the availability of medical information.

In Philadelphia, Pennsylvania, on June 12, 1996, a panel of federal judges blocked part of the CDA, saying it would infringe upon the free speech rights of adults. On July 29 a U.S. federal court struck down as too broad the portion of the CDA intended to protect children from indecent speech. A year later, on June 26, 1997, the Supreme Court upheld the lower court’s decision in *Reno v. American Civil Liberties Union*, stating that the portion concerned was an unconstitutional abridgement of the First Amendment right to free speech because it did not permit parents to decide for themselves what material was acceptable for their children, extended to noncommercial speech, and did not define “patently offensive,” a term with no prior legal standing.

See also: **Constitutional protections**

Suggested Reading: Center for Democracy and Technology. *Communications Decency Act (CDA)*. <http://www.cdt.org/speech/cda/>. Online, March 2006; Cohen, Henry. *The Communications Decency Act of 1996* (CRS report for Congress). Congressional Research Service, Library of Congress, 1996; Cohen, Henry. *Internet Indecency: The Supreme Court Decision on the Communications Decency Act* (CRS report for Congress). Congressional Research Service, Library of Congress, 1997.

Sarah K. Parkinson

Computer-Assisted Passenger Prescreening System (CAPPS II) and Secure Flight

The Computer-Assisted Passenger Prescreening System (CAPPS II) was developed by the Department of Homeland Security’s (DHS) Transportation Security Administration (TSA) to allow the comparison of airline passenger names with names in private- and public-sector databases to assess the level of risk a passenger might pose. The program’s goals bore a strong resemblance to the **Multi-State Anti-Terrorism Information Exchange Program (MATRIX)**, which is run by a private company and sponsored by many states, but CAPPS II served the more limited mission of supporting airline security. When privacy and effectiveness issues were widely raised, former Secretary of Homeland Security Tom Ridge announced his intention to dismantle the program in July 2004. The program was dismantled, reinvented, revised, and reintroduced as Secure Flight in September 2004.

The Secure Flight program embodies the layered strategy employed by DHS to secure air traffic safety by using several levels of security to protect air passengers. The Secure Flight program includes use of federal air marshals, federal flight deck officers, and a streamlined version of the CAPPS II database-comparison methodology. The CAPPS II component of the program requires TSA to conduct preflight comparisons of airline passenger information with federal government watch lists.

With Secure Flight, passenger name records from domestic flights are compared to names maintained by the terrorist screening database in the newly named Office

of Transportation Vetting and Credentialing (DHS/TSA 2004). This database includes the “no-fly” and “selectee” lists of persons known or suspected to be engaged in terrorist activity. Secure Flight compares these two lists for the exclusive purpose of identifying suspected terrorists. Information on passengers is disseminated on a strictly need-to-know basis. A redress mechanism for alleged abuse is included within the program. Further, no **Privacy Act of 1974** exemptions are invoked under the revamped program, and passenger name records are released to individuals who request them. Homeland Security has embraced these precautions and changes in order to address the privacy concerns that befell the CAPPS II and MATRIX Programs.

Suggested Reading: Department of Homeland Security, Transportation Security Administration. *Secure Flight Test Records System*. <http://www.tsa.gov/public/display?content=09000519800cf3a7>. Online, March 2006; Etzioni, Amitai. *How Patriotic Is the Patriot Act? Freedom versus Security in the Age of Terrorism*. New York: Routledge, 2004; Goldberg, Carole. *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security*. New York: W. W. Norton, 2002.

Jill Joline Myers

Computer cache. *See* **Computer; Internet**

Computer Fraud and Abuse Act of 1986

Information technology has become very valuable to businesses and government alike. Interconnectivity allows different **computers** to communicate over a seamless web, sending packets of data that comprise databases and files. However, many companies are losing millions of dollars through unauthorized access, interception, and fraudulent dissemination of proprietary information. Such unauthorized access can lead to computer fraud and a variety of other computer crimes, commonly referred to as “hacking.” The Computer Fraud and Abuse Act, 18 USC 1030 (CFA), criminalizes unauthorized access into or theft of protected computer data and thus helps preserve rights to privacy.

Companies use various security devices to protect their ability to collect, store, retrieve, and disseminate information. Companies also use computers to collect and maintain **personally identifiable information** about their customers in order to verify identities, such as **Social Security numbers**, **home** phone numbers, **fingerprints**, and voiceprints. The positive effect of collecting personal data is that it reduces infringement and computer abuse. The negative effect is that such information cannot only reveal the identities of persons, but it can also track individuals’ activities and habits.

Service providers, such as **Internet service providers (ISP)**, telephone companies, and cable companies, maintain and often sell proprietary information about subscribers and customers. Such information includes bank account numbers, driving records, criminal background, employment history, and credit history, all of which can be sold to third parties without the knowledge or consent of subscribers and customers. Much of this information is collected as part of legitimate business activity and stored in centralized computers; it is often more expensive to delete these pieces of information than to maintain them.



There is a growing concern about dissemination of private facts about persons to third parties and the ability to develop profiles of persons through compilation of information retained in computer databases. Previously, this information was decentralized and posed little risk. Today, however, as industries converge or data services are outsourced to private companies, much of this information is stored on centralized computers and more readily accessible by law enforcement for a variety of reasons.

The CFA covers computer espionage, theft of specific types of information, computer **trespass**, computer fraud, damage to a protected computer, trafficking in passwords, and computer extortion. The act has broad coverage and is designed to prevent access to classified national defense or foreign relations information, financial information or consumer-reporting agency records, information on a computer operated on behalf of the United States, and any computer used in interstate or foreign commerce.

There are four general elements necessary to establish a violation under this act. First, there must be unauthorized access. Unauthorized access includes someone who steals another's identity to hack into a protected computer. It can also include access by someone who would otherwise have authority to access a computer network, but who exceeds that authority. Second, the perpetrator must intend to hack into the system or to gain access. Intent to harm or cause damage is not required for prosecution under the act. Third, the perpetrator must access a protected computer. Protected computers include all government computers, computers operated on behalf of the government, computers used in interstate or foreign commerce or communications, financial institution computers, and foreign computers. In short, almost any computer is covered under the act. Finally, the perpetrator's actions must cause some damage. The damage element can be satisfied if the actions impair the integrity or availability of data, a program, a system, or affect information such that costs exceeds \$5000 in one year; impair medical records, regardless of the value; cause physical injury to a person, regardless of value; or threaten public health and safety.

The statute was first tested in *United States v. Morris*, 928 F.2d 504 (1991), 502 U.S. 817 (1991). Robert Tappan Morris was a computer programmer with authorized access to government computers who introduced a software worm into the system that spread to and damaged computers at numerous installations, including leading universities, military sites, and medical research facilities. In response to a defense that Morris was authorized but merely exceeded his authority, the Supreme Court held that the scienter or "intentional" requirement of the statute applied only to the access—the corresponding damage, however unintentional, still satisfied the statute.

In 1996 the act was amended to codify the rule. Today, a person is liable under the statute who (1) knowingly engages in conduct that intentionally causes damage, (2) engages in intentional access that recklessly causes damage or (3) engages in intentional access that causes damage. The statute applies to unauthorized access as well as to instances in which someone exceeds his or her authority.

After September 11, 2001, Congress passed the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)** in part in order to expand the law

enforcement and investigative tools available under CFA. Specifically, the act was designed to include “cyberterrorism” offenses that might threaten public health or safety, and authorized the U.S. Secret Service, the **Federal Bureau of Investigation (FBI)**, and other agencies already empowered under CFA to investigate computer fraud. In addition, under the revisions, the length of punishments was increased up to 20 years, and the term “damage” was broadened to mean “any impairment to the integrity or availability of data, a program, a system, or information.” However, under the revised statute, damage that resulted from “the negligent design or manufacture of computer hardware, computer software, or firmware” was no longer actionable.

Under the revised CFA, the damage element requiring a minimum of a \$5,000 loss impairment can “include any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or other information to its conditions prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred by an individual or corporation because of interruption of service.” Subsequent cases have used these broader standards to assess culpability in civil cases to limit access to data or systems, such as commercial espionage as well as hacking into a city’s emergency communication system or a hotel and airline communication systems.

See also: **Cable Communications Policy Act of 1984**

Suggested Reading: Harrington, Susan J. “The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions,” *MIS Quarterly* 20 (1996): 257–278; Office of the Chief Information Officer, U.S. Department of Energy. *Computer Fraud & Abuse Act*. <http://cio.doe.gov/Documents/cfa.htm>. Online, March 2006; Straub, Detmar W., Jr., and William D. Nance. “Discovering and Disciplining Computer Abuse in Organizations: A Field Study,” *MIS Quarterly* 14 (1990): 45–60.

Andrea L. Johnson

Computer Matching and Privacy Protection Act of 1988

The Computer Matching and Privacy Protection Act of 1988 (CMPPA) amended the **Privacy Act of 1974** by adding provisions that federal agencies must implement when performing computerized comparisons of certain collections of administrative records. Such a comparison seeks to identify an individual who appears on two lists but should not, or who, appearing on one list, should not appear on a second.

Computer matching first came to public attention in 1977 following an initiative called “Project Match,” in which the then Department of Health, Education, and Welfare (HEW) compared recipients of Aid to Families with Dependent Children (the major federal welfare program) with federal payroll records, intending to identify individuals improperly collecting both welfare payments and a government paycheck. Although the comparison yielded 33,000 “raw hits,” only 35 convictions resulted, all for minor offenses with less than \$2000 in fines. The program was criticized not only for its lack of financial gain compared to the costs, but also because it caused some payments to be interrupted based solely on a raw hit, without verification by a human being or due process controls.



These concerns continued throughout the 1980s, and the CMPPA was enacted to address some of them. However, CMPPA does not prohibit any particular type of matching program. Instead, it adds procedural safeguards for matches that seek to establish or verify an individual's eligibility for federal benefit or loan programs, recoup payments or delinquent debts arising from these programs, or compare federal personnel or payroll systems with other federal or state records. The CMPPA does not: cover matches designed to produce aggregate statistical data; support research where the results will not be used to make adverse decisions about the subjects; advance a criminal investigation of a named subject, foreign counterintelligence purpose, or background investigation for a security clearance; conduct tax administration; or, perform routine personnel administration. In addition, it does not cover matches where an agency uses only its own records.

As a statute amending the Privacy Act, CMPPA only applies to systems of records as defined by that act: collections of records about U.S. citizens or legal, permanent resident aliens, in the custody of a federal agency, connected to an identifier of the individual, and retrieved by that identifier. The major provisions of the CMPPA require an agency to: conclude an agreement with a partner matching agency describing the records that will be matched and the procedures to be followed before, during, and after the match; analyze the costs and benefits of matching programs; publish notice of new matching programs in the *Federal Register*; include individual notices to potential subjects of a match at the time of collecting information; conduct independent verification of "hits;" and, notify individuals and provide them the opportunity to refute any adverse information before denying or terminating a benefit or loan. The CMPPA also requires agencies participating in matching programs to set up data integrity boards to oversee the programs, and assigns the Office of Management and Budget to provide guidance, assistance, and oversight to the other federal agencies.

In 1990, Congress enacted Computer Matching and Privacy Protection amendments to clarify details of the due process provisions of the original CMPPA. These amendments permit an agency to substitute its own due process and independent verification procedures following computer matching if its procedures are similar and were in existence and working well prior to passage of CMPPA. For example, a program that provides monthly payments to beneficiaries and has been relying on an advance-notice period shorter than the 30 days required by CMPPA would be permitted to take adverse action after the shorter period in order to avoid making overpayments.

See also: **Data mining; Public records**

Suggested Reading: Clarke, Roger. "Dataveillance By Governments: The Technique of Computer Matching," *Information Technology & People* 7 (1994): 46–85; Gandy, Oscar. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press, 1993; Office of Management and Budget. "The Computer Matching and Privacy Protection Amendments of 1990 and the Privacy Act of 1974 (proposed guidance)," *Federal Register* 54 (1991): 18599–18601; Office of Management and Budget. "Privacy Act of 1974: Final Guidance Interpreting the Provisions of Public Law 100–503, the Computer Matching and Privacy Protection Act of 1988," *Federal Register* 54 (1989): 25818–25829; Office

of Management and Budget. *Privacy Guidance and Privacy Reference Materials*. <http://www.whitehouse.gov/omb/inforeg/infopoltech.html>. Online, March 2006.

Maya A. Bernstein

Computers

Most computer users entrust their respective computers with vast amounts of very sensitive and **personally identifiable information**. Even if such computers are never connected to any network, such as the **Internet** or even a local network, they retain that sensitive information long after the user thinks that it was deleted. When a computer is connected to a network, be it the Internet or some internal corporate or other network, it is as if there were a person sitting right behind the user, taking precise notes of everything that the user does with the networked workstation.

Computer hard disks contain mirrors of people's lives. **Electronic mail**, love letters, tax returns, and privileged communication with lawyers are all saved in the computer for the user's benefit and, unless the user take measures to protect his or her privacy, for the benefit of anyone who steals the computer or of any computer forensics investigator. In a business setting, proprietary information, marketing plans, and lists of current and prospective clients constitute every commercial business's lifeblood. If these fall into competitors' hands, the commercial entity will likely go bankrupt; if it is a publicly held company, its stockholders will claim negligence and will rightly sue. Similarly, in a medical setting, healthcare professionals are legally required under the **Health Insurance Portability and Accountability Act of 1996 (HIPPA)** to safeguard the **confidentiality** of patient data under penalty of jail time in many cases. Government users of computers are similarly required to ensure that the data entrusted to them cannot fall into unauthorized hands.

Despite all the foregoing, the reality of life is that laptops do get forgotten in taxicabs and airplanes, and almost all computers are eventually sold, donated, recycled, or thrown in the trash. At a minimum, computers regularly get sent to repair shops, almost invariably with their hard disks in place. What about the sensitive data in those hard disks? Law enforcement has been quite successful in promulgating the self-serving fiction that only criminals with something to hide would have an interest in ensuring that sensitive data in their computers are rendered inaccessible by all others. In fact, quite the opposite is true: individuals and organizations can be held legally liable for failing to ensure that sensitive data cannot be accessed by third parties. It is technically impossible to hide data from all except law enforcers; as such, one must either hide it from all or from nobody. Given the legal obligations of businesses, individuals, and professionals to prevent unauthorized disclosure of sensitive data, a computer user must hide sensitive data from all. Achieving this result is very difficult.

And if that were not difficult enough, computer users and owners have to worry about new vulnerabilities introduced by the fact that most new computers, especially laptops, come with an already enabled wireless connectivity known as "Wi-Fi." In the default, unmodified mode, as soon as such a laptop is turned on, it dutifully searches for and tries to establish communications with any commercial or private Wi-Fi "access point." A rogue access point nearby can then connect with such a laptop and access all its files. Similarly, if any Wi-Fi-enabled laptop user

connects to the Internet through a legitimate access point at an airport, coffee shop, or hotel, all communications can be readily intercepted by another suitably configured laptop nearby; worse yet, a suitably configured laptop can masquerade as the legitimate wireless access point to which the hapless user wants to connect, and then act as a go-between connecting the unsuspecting user and the legitimate Wi-Fi access point, thereby intercepting all traffic to and from the unsuspecting user. In short, the privacy threat extends far beyond the concern of unauthorized access to computer files. Remote interceptors can gain access to a computer and files through wireless paths that are enabled by default—for the convenience of the user—by computer manufacturers.

As far as the confidentiality of the files that reside in the computer is concerned, even if the computer owner went to the heroic measures needed to make a sensitive file truly disappear from magnetic media, there is a high likelihood that copies and earlier versions of that file would exist in numerous other places in the same magnetic media; these copies can have unrecognizable names and/or have names that are invisible in the normal default directory lists. To make things worse, chances are that there will be fragments of earlier copies of files scattered all over the user's magnetic media. Furthermore, even though the computer's screen and printer show the latest version of a document, the electronic version of it in the computer will most likely contain the full history of how it evolved from the very first draft onward, and this history can be seen by anyone with the know-how.

Unbeknownst to the user, most Windows-based applications create temporary files on the hard disk at unadvertised locations and use unrecognizable names, so that should the computer crash for any reason such as a power failure, the user will not have lost the file he or she had created. Since Windows and its application software are not clairvoyant and cannot tell if a computer will crash or not, they usually create and save such temporary files; if the computer does not crash—as is usually the case—these temporary files remain in the computer. Additionally and independently, Windows stores information about a user's computer activities in numerous files on the hard disk; most of these locations, such as the "Registry" and the "Swap file" are very difficult to find and even harder to remove because they have been merged with information that the computer needs to operate; if that entire merged file were removed, the computer would not work at all.

In addition, the names of files created by the user are stored separately from the files themselves. Even if the user manages to remove a file, its name will still be discoverable and, if it is particularly revealing, could haunt the computer's user. Secure deletion of any one file and its name is not a simple proposition; it must be viewed only as part of the secure cleanup of an entire disk and never as just the secure removal of the latest copy of a single file. It follows that what must be eliminated is not just a sensitive file itself, but also copies of the file that have been created by the computer's software as well as all information *about* that file, such as the file's name (ideally chosen to be nondescript and not incriminating), the date it was created, the date it was last accessed, the date it was renamed, and the folder it was moved from and to—all of which are stored separately on the computer's hard disk.

Using the "delete" command to remove a file achieves absolutely nothing. The file remains in the disk and is merely marked as "no longer wanted." Using "format" or

even the “fdisk” partitioning command does not remove sensitive files either. The only way to remove a sensitive file and its separately stored name and date stamp is to overwrite them. Overwriting a known file is easy, assuming that there is only one copy with no temporary or other copies of it, and no evidence of it in the many system-level files used by Windows; unfortunately, copies of the file and of segments of that file are typically stored by Windows all over the hard disk.

“Disk wiping,” or the process of overwriting all sensitive data on a hard disk so that such data cannot be retrieved by others, is a very complex business. Windows offers no means for users to overwrite their sensitive files; rather, Windows makes it extremely difficult to remove sensitive files because of the many ways that it leaks sensitive information into assorted obscure places in the computer’s storage media. As a result, numerous software packages have evolved that have varying degrees of success in eliminating sensitive data from computers. The problem is that even the best of them do not work very well for the following technical reasons: (1) Windows and Windows-based application software create and use files that cannot be removed from within Windows (e.g., the Swap file) while Windows is running; (2) disk-wiping software has no way of knowing which legitimate-looking files created by assorted application software should be eliminated; (3) disk-wiping software usually does not touch the Registry files—yet this is precisely where, for example, Microsoft’s Internet Explorer stores the user’s web-browsing activity; (4) Windows stores the names of files and data about those files in a different place than the files themselves, and treats those names differently even if a file has been deleted; and (5) the typical high capacity hard disks of today come with a number of sectors held in reserve. When a data-containing sector in the disk is deemed by the hard drive’s “smart” firmware to be marginal (e.g., when there are occasional errors in reading the data from it), the hard disk’s own firmware copies the data from the marginal sector to one of the sectors held in reserve, assigns the logical address of the marginal sector to the new sector where those data were copied, and “mothballs” the marginal sector without overwriting the data in it after those data were copied onto the new sector.

No disk-wiping software can touch the now-mothballed sector, since it no longer has an address and hence it does not exist as far as any software is concerned. On the other hand, a forensics investigator with access to the disk drive manufacturer’s firmware can readily access those sectors and all data in them.

Disk wiping, then, is a very complicated task, and all software that purport to do it fail quite miserably. Particularly because of reason five above, computer users are advised not to depend on any such software for wiping hard disks clean, and are encouraged to physically destroy the storage media before selling, donating, or disposing of magnetic storage media. The only secure fix is to physically destroy the magnetic media. Given the low cost of hard disks today, there is no excuse for not destroying the old one and getting a new one if the user is concerned about the confidentiality of computer data contained in the old hard disk.

Unlike conventional analog data, such as the shade of grey or the subjective recollection of a witness, digital data that takes one of two very unambiguous values (zero or one) is misperceived by the average person as being endowed with intrinsic and unassailable truth. In fact, quite the opposite is true. Unlike tampering with conventional analog data and evidence, which can often be detected by experts

with the right equipment, digital data can be manipulated at will and, depending on the sophistication of the manipulator, the alteration can be undetectable regardless of digital forensics experts' competence and equipment. The potential for a miscarriage of justice is great, given that many defense lawyers, judges, and juries may be unaware of the esoteric details of computer science. This aspect of digital evidence may not be addressed by the computer forensics industry and by the prosecution, both of which focus on the other aspects of the process of collecting, preserving, and presenting digital data evidence, which are indeed unassailable, such as the "chain of custody" portion of handling digital evidence.

A common example of computer evidence can illustrate this point. A suspect's hard disk is confiscated and subjected to forensics analysis; a report is generated for the court stating that the hard disk contained certain files, with certain dates, and that these files were renamed or printed on various dates, thereby negating the suspect's claim that he or she did not know of the existence of these files.

A typical judge or jury will accept these facts at face value. However, the data found on someone's hard disk (or other mass storage media) could indeed have entered that hard disk through any one or more of the following ways without the suspect's knowledge, let alone complicity. For example, the hard disk may not have been new when the suspect purchased it, and it may have contained files from before the suspect took custody of it. This applies even in the case of purchases of supposedly new computers, because they could have been resold after being returned by a previous buyer. Spy-ware could have secretly installed unadvertised files as well as a capability for the software maker to snoop on the individual's computer through the Internet. If this snooping capability were exploited by a third-party hacker who routinely scans computers for this kind of back-door entry, then files could be inserted on the suspect's computer at will. Obtaining full control of anyone's computer through existing security flaws in its operating systems and applications, especially its Internet Explorer, might allow anyone to insert files in it without the knowledge of the owner. This can happen through an unsecured broadband Internet connection or a wireless access point. In addition, when a user browses the Internet, it is not uncommon to mistype an address and end up inadvertently and unintentionally on an "adult" website. Alternatively, one can still end up at an incriminating site because hackers have often doctored up entries in the domain name servers (DNS), which amounts to doctoring-up the directory that is accessed every time a user types the name of a website he or she wants to see.

Advertising in the form of pop-up ads, scrolling text, and images from unsavory advertisers or purveyors of pornography may get stored ("cached") in the hard disk drive. Over a period of time, enough to these ads collect in the computers and create the appearance of frequent activity. Of course, others in the household or workplace could have visited websites that the owner did not patronize. Unsolicited e-mail and their attachments can remain on a hard disk for some time. Few users will go to the trouble of overwriting the offensive attachment because Windows does not include any provision to overwrite anything. And even if a user did attempt to overwrite a file with specially purchased software, the name of the file, which could be quite incriminating in and by itself, would remain on the hard drive.

Computers crash sooner rather than later. The typical course of action is to take the computer to a technician in an effort to access personal and business

data. Computer technicians, like other outsiders, have the opportunity to place data into the repaired computer. A few years later, the owner of the computer is likely to have forgotten about the repair altogether. Computer forensics examiners like to substantiate their findings by pointing out the time/date stamp associated with different computer files. Yet, the time/date stamp, as well as every single bit of data in a computer's magnetic media can be altered undetectably with a disk editor. Additionally, images can be altered. Unlike images from conventional film-based photography, which can usually be identified as doctored by a competent investigator, digital images (such as those taken by any surveillance camera) can be altered in a manner that no expert can detect, as long as the alteration is done professionally enough. Likewise, unlike analog sounds (e.g., the infamous gap in the tape recording made during President Nixon's term in office), where a careful study of the background noise can detect alterations of analog recordings, digitized files of sounds can be altered at will; if the alteration is done professionally enough, it will be undetectable even by a forensics examination of the digital file.

The use of digital evidence has created a new phenomenon in today's courtrooms. Computers store more and more information about people's lives and activities. This has resulted in an explosive increase in the use of computer forensics techniques on confiscated or subpoenaed computers, based on the incorrect assumption that what is in the computer is what the user put into it. An entire cottage industry of computer forensics investigations has sprung up to service the appetite for such services. The legal and societal problem with this situation is that individuals in the legal and law enforcement professions may be unaware of at least some of the many ways whereby the data they present as evidence are really not evidence of anything because these data may have been placed in a computer without the knowledge or complicity of the owner of the computer. In addition, evidence that is based on a computer user's Internet Service Provider's records is, similarly, evidence of nothing. A person's Internet account can be accessed by third parties without that person's awareness or complicity, even if that person had been the only one at home when the alleged Internet access occurred.

In the end, digital evidence should be viewed with extreme suspicion, regardless of the competence or qualifications of the computer forensics expert witness. While the chain of custody portion of how the evidence was handled may have been impeccable, the raw digital data itself on which a forensics analysis was based can be easily and undetectably tampered with by anyone with the right background.

See also: **Anonymity; Authentication; Computer Fraud and Abuse Act of 1986; Computer Matching and Privacy Protection Act of 1988; Cryptography; Data mining; Health privacy; Library records; Workplace privacy**

Suggested Reading: Caloyannides, Michael. *Desktop Witness: The Dos & Don'ts of Personal Computer Security*. Hoboken, NJ: John Wiley & Sons, 2002; Computer Professionals for Social Responsibility. <http://www.cpsr.org>. Online, March 2006; Easttom, Chuck. *Computer Security Fundamentals*. Upper Saddle River, NJ: Prentice Hall, 2005; Electronic Privacy Information Center. <http://www.epic.org>. Online March, 2006; Gandy, Oscar. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press. 1993; Harrington, Susan J. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly* 20 (1996):

257–278; Smith, Jeff H. *Managing Privacy: Information Technology and Corporate America*. Chapel Hill: University of North Carolina Press, 1994; Straub, Detmar W., Jr., and William D. Nance. “Discovering and Disciplining Computer Abuse in Organizations: A Field Study,” *MIS Quarterly* 14 (1990): 45–60.

Michael Caloyannides

Confessional culture

The term “confessional culture” is used to describe aspects of popular culture and shifts in social relations taking place in the United States from the late twentieth century to the present. At the heart of confessional culture lies a will to countenance **disclosures** that infects everything from casual encounters between strangers to popular television programs that revolve around intimate revelations. The mass media plays an essential role in enabling and sustaining confessional culture by providing a crucial venue for publicizing the personal. Most often used as a term of aspersion, confessional culture is commonly associated with a breakdown in **manners** and norms of propriety, as well as the proliferation of television and radio shows that revolve around the disclosure of trivial, and often salacious, personal details of private lives.

The term has been traced to Michel Foucault’s discussion of confession in *The History of Sexuality*. Arguing that confession lies at the heart of Western conceptions of sexuality, Foucault suggests that confession forms the basis for Western legal systems, medical practice, education, family connections, and romantic relations, and that social life is organized around institutions that rely on the confession of crimes, sins, and desires to enable practices of normalization.

Foucault emphasizes the wide variety of social institutions implicated in the confessional imperative, while the contemporary discourse of confessional culture tends to **privilege** psychotherapy as the exemplary site of confession, one which provides both a vocabulary and the implicit model for confession as it is enacted interpersonally and in popular culture. The late twentieth century saw the emergence of an array of television and radio programs that revolved around confession, from daytime talk shows, to prime-time reality TV programs, to call-in radio shows. These increasingly popular genres highlight the close connection between the will to confess on the one hand and the rise of voyeurism as a dominant social modality on the other. A confessional culture critically depends not just on subjects who are willing to tell all, but also on the presence of an audience that regards revelations as entertainment.

Confessional culture has been held accountable for a variety of social ills, including the displacement of serious news and other programming by shows that venerate disclosure above all else. The news media have been subject to special sanction for encouraging the idea that the public has the right to know everything it can about the private lives of public officials. Daytime talk shows using the style of hosts such as Phil Donahue or Ricki Lake, where hosts ask personal questions and guests share private and often intimate details, have been dismissed as modern-day freak shows, and the ascendance of reality TV has been read as another sign of a decline in public taste.

Confessional culture has also been linked to a breakdown in the social norms that were seen at one time to provide welcome protection against violations of

personal privacy, particularly against those who otherwise would extend overtures of intimacy in an indiscriminate manner. The popularization of the phrase “too much information” in the early years of the new millennium may be a sign of a nascent backlash against such uninvited intimacies.

Those who defend confessional culture suggest that confession is a powerful tool for challenging social norms and practices that “closet” or silence sexuality and social deviance. The very distaste elicited by a confessional culture suggests the transgressive power of revelation to break down established social norms and force confrontations with ideas and people who are otherwise repressed or silenced.

See also: **Public/private dichotomy; Secrecy**

Suggested Reading: Cummings, Dolan. *Editor’s Note: Confessional Culture*. <http://www.culturewars.org.uk/2004-02/dec04.htm>. Online, March 2006; Foucault, Michel. *The History of Sexuality: An Introduction*. New York: Vintage, 1990 (reissue).
Juliet Williams

Confidentiality

Confidentiality is the state of having information kept secret. Confidentiality is treating information as private and protecting it from unauthorized access, **disclosure**, or publication. Confidentiality generally pertains to information that is not generally available to the public. Maintaining confidentiality ensures that information is accessible only to those authorized to access it and disclosed only to those authorized to receive it. Confidentiality is an essential component of information security.

Confidentiality is a term widely used to imply a sense of trust and **secrecy** regarding information shared with another. Confidentiality also encompasses a relationship of trust, loyalty, and reliance between two communicating parties. In a confidential relationship, the disclosing party (discloser) expects the receiving party (recipient) to protect and keep secret any shared information and disseminate it to third parties only with the consent of the discloser or when required by law. In a confidential relationship, a duty of confidentiality attaches, the breach of which may be punishable by law. Confidentiality also embraces the ethical principles that support certain professions in which relationships of trust are formed, such as medicine, law, and **journalism**.

Confidentiality is derived from the Latin word *confidentia*, or “confidence,” and the Latin root *fid* or *fidere*, which means “faith.” “Confidence” and other forms of the word have been in use since the fifteenth century with semantics related to the idea of trust. When information is shared within a relationship of trust and with an expectation of secrecy, the recipient must take adequate precautions and safeguards to control and protect the information from access by or disclosure to any other entity. While there may be written agreements between the discloser and recipient to guarantee confidentiality, there is also an implied duty on the part of the recipient to act in good faith to prevent any harm that may result from disclosure of the information.

Confidentiality does not apply to all information shared with the expectation of secrecy. For example, if an individual shares personal information with a friend or co-worker, the obligation of confidence depends upon the circumstances, expectations,



and personal relationship between the two individuals. However, in situations where there are written contracts or agreements that govern information sharing between two parties, there may be a duty to keep all information confidential. These agreements can be legally enforced. Injunctive relief, monetary compensation, and other remedies may be available if the discloser can prove that the recipient has made unlawful disclosures. Under exceptional circumstances, the recipient can disclose confidential information if disclosure is mandated by court order or statute. Information that is deemed confidential is not limited to written documents. Confidentiality may extend to oral communications, video, voice recordings, and any form of communication that was used to convey private information. Ownership of the information generally resides with the discloser, and permission may have to be obtained from the discloser for the recipient to use the information.

In certain circumstances, where there is a special relationship between two parties, additional rights may be granted by law to preserve the privacy of information communicated between the two parties. This right to confidentiality is termed **privilege** and belongs to the discloser. Privileged communications are protected by law from compelled disclosure in judicial proceedings. Some protected or privileged associations include doctor-patient, attorney-client, priest-confessor, and husband-wife relationships. The obligation to maintain confidentiality may also extend to the recipient's heirs, successors, and representatives. The concept of privilege is much narrower than that of confidentiality.

In 1977 the U.S. Supreme Court, in *Whalen v. Roe*, indicated that confidentiality or informational privacy was one of the two branches of the constitutional right of privacy (the other being autonomy or decisional privacy). Other courts of appeal have indicated that this constitutionally protected right of confidentiality may provide a discloser with a cause of action against the government for the wrongful dissemination of private or confidential information. However, in most cases, the courts have not found the government liable.

Recognition of the duty of confidentiality can be found in several federal statutes. For example, the **Privacy Act of 1974** expressly mandates that federal agencies "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records" as pertaining to individuals' records that are collected and maintained by the agencies. The federal **Freedom of Information Act** provides another example. It recognizes that confidential matters should not be made public by government agencies.

The medical profession provides an example of confidentiality within a confidential relationship. All newly licensed physicians take the Hippocratic Oath, which requires physicians to protect the personal and private information of patients. In short, medical ethics require that doctors keep patients' personal or health information confidential. In most instances, doctors must seek consent in order to disclose a patient's medical information to third parties. However, medical confidentiality has become more problematic given the development of new health care business models, including health maintenance organizations (HMOs). Now, patient data is shared with more individuals and entities in the course of treatment and payment for medical services than ever before. In addition, advances in information technologies make it easier, faster, and more convenient to share patient

information with relevant parties, thus increasing the possibilities for unauthorized access and disclosure. The **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** contains provisions that protect a patient's confidential information by restricting some disclosures of health information without authorization.

The financial industry is required to comply with certain legal obligations to protect the confidentiality and accuracy of the information it collects and disseminates. The **Fair Credit Reporting Act (FCRA)** requires consumer-reporting agencies to institute reasonable procedures to ensure "the confidentiality, accuracy, relevancy, and proper utilization" of an individual's financial, credit or other **personally identifiable information**. The **Financial Services Modernization Act of 1999**, also known as the Gramm-Leach-Bliley Act (GLBA), recognized that "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."

The employee-employer relationship may be a confidential one. In the context of employment, an employee, potential employee, or business associate may have access to information that is integral to the company's existence. Such information includes customer lists, financial performance, proprietary technology, and trade secrets. A trade secret could be any process or practice that gives a company a competitive advantage in an industry. Those who are privy to trade secrets may have a legal obligation to keep them confidential, either by virtue of their confidential relationships or by contract. Every state recognizes some form of trade secret protection, either through common law or statute (many states have adopted the Uniform Trade Secrets Act). Trade secret law allows an owner of a trade secret to prevent those who are bound either by a duty of confidentiality or by contract from disclosing the trade secret to others.

A confidential relationship can be created by contract through a confidentiality or nondisclosure agreement. Here, parties agree to protect the confidentiality of trade secrets or other confidential information disclosed during employment or business transactions. Breach of a confidentiality agreement is punishable by law. Injured parties may request a court to stop further disclosures or otherwise compensate them for the breach.

Under the principles of agency law, an employee owes duties of loyalty, obedience, and care to an employer. An employee cannot compete with his or her employer in the same area of business, even if the employee works outside employment hours. In research institutions or in employment positions involving the development of scientific or technological innovations, employees do not necessarily have ownership rights to their work product. Employees may generate ideas for improving existing work products or create brand new innovations and discoveries, both of which may belong to their employer. Typically, employers execute the confidentiality, nondisclosure, and invention assignment agreements to protect a company's work product investment. Even in the absence of contractual obligations, state tort law provides for causes of action to prevent an employee from exploiting specialized skills obtained during the course of employment in order to benefit others.

See also: **Gossip**

Suggested Reading: Alderman, Ellen, and Caroline Kennedy. *The Right to Privacy*. New York: Alfred A. Knopf, 1995; Allen, Anita L. *Why Privacy Isn't*



Everything: Feminist Reflections on Accountability for Private Life. Lanham, MD: Rowman and Littlefield, 2003; Black, Henry C. *Black's Law Dictionary*, 7th ed., St. Paul, MN: West, 1999; Ruebner, Ralph, and Leslie Ann Reis. "Hippocrates to HIPAA: A Foundation for a Federal Physician-Patient Privilege," *Temple Law Review* 77 (2004): 505–576; Smith, Robert Ellis. *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*. Providence, RI: Privacy Journal, 2004; Westin, Allan. *Privacy and Freedom*. New York: Atheneum, 1967.

Leslie Ann Reis

Constitutional protections

The United States Constitution establishes a minimum of privacy to which government officials may add but from which they may not subtract. **Louis Brandeis** and Samuel Warren, his co-author and law partner, are generally credited with introducing privacy as a legal concept in their heralded law review article published in 1890. That article focused on tort law, but decades later as a Supreme Court justice, Brandeis spoke grandly of a constitutional "**right to be let alone**" in *Olmstead v. United States*, 277 U.S. 438 (1928).

Consistent with Brandeis's proclamation, many popular accounts speak of a unitary constitutional right of privacy. Supreme Court jurisprudence since Brandeis wrote makes it more accurate and helpful to understand constitutional privacy initially in terms of two distinct sets of rights. One set, which includes the Fourth Amendment's ban against unreasonable searches and seizures, protects what may be called informational privacy and restricts the government's access to information about an individual. Another set of rights, which includes the unenumerated right of privacy at stake in the Court's highly publicized **abortion** decisions, protects individual autonomy by giving individuals freedom to make certain decisions about the course of their lives. It is true that informational privacy and individual autonomy both entail an individual's "right to be let alone" by government. But the scope, constitutional basis, and debates over these two principles are sufficiently distinct as to merit separate discussion.

I. Informational Privacy

The Constitution protects informational privacy by regulating the means by which the government collects information. The Fourth Amendment bans unreasonable searches and seizures and the Fifth Amendment's **privilege** against self-incrimination precludes any person from being "compelled in a criminal case to be a witness against himself."

At the outset, it is important to distinguish the method at work in these provisions from another common method, which protects privacy by focusing on the information's subject matter. A legal regime might choose to designate certain subjects as inherently private and as presumptively beyond the government's purview. The government could be prohibited or restricted from accessing or using information about, for instance, an individual's medical treatment, sexual orientation, or religious affiliation. Much is to be said in favor of such an approach. Information pertaining to such highly personal subjects is frequently irrelevant to any legitimate public concern, its public disclosure can be extremely damaging to the individual, and even the threat of disclosure can deter desirable conduct. Although some state

and federal privacy laws adopt the approach of designating private subject matters, the Constitution's provisions concerning informational privacy do not.

The Constitution instead restricts the means by which information about any subject may be collected. Provided that information is not obtained through proscribed means, the government may use information everyone would regard as presumptively private. For example, that an individual has a highly embarrassing scar in an intimate area is private in its subject matter. But when the government learns about this fact from the voluntary statement of a third-party witness, the Constitution's protections of informational privacy do not bar the government from using this fact. Conversely, the government may not obtain through proscribed means information that no one would regard as "private" in its subject matter. The privilege against self-incrimination, for example, permits a criminal suspect to refuse to answer whether she or he murdered another person on a public street in broad daylight.

It is not clear that any single coherent theory underlies the Constitution's protections of informational privacy. Consider the Fifth Amendment's privilege against self-incrimination. From one view, the privilege exists because of doubts about the truthfulness of statements obtained through coercion. Even if this were the Fifth Amendment's rationale, it cannot explain the Fourth Amendment. The Fourth Amendment does not rest on doubts over whether, for example, the illegal drugs stashed in a person's kitchen drawer are that person's or whether a person's authentic beliefs are expressed in the private diary found next to the bedstead. If anything, the information's private location actually tends to strengthen rather than weaken its reliability.

It is also problematic to link constitutional protections of informational privacy with the notion that certain subjects are inherently private. The link cannot be a direct one. As mentioned above, constitutional protections restrict access to public information and permit access to private information. As an indirect protection of private subject matters, informational privacy is not very effective. Informational privacy, by itself, permits government to regulate any subject matter. By regulating subject matters that might reasonably be thought private, government can generate the justification needed to overcome Fourth Amendment barriers to accessing private areas. Government can obtain information from sources other than through a search, a seizure, or a compelled statement by a suspect. It may then use such information to establish probable cause that a violation of law in question has occurred and, if necessary, acquire a warrant to undertake a search or seizure or make an arrest.

The **home** is the archetypal private place and is explicitly mentioned in the Third and Fourth Amendments. Government nonetheless remains able to, and uncontroversially does, enforce prohibitions against violence and abuse in the home. Informational privacy likewise does not create an effective barrier against regulation of activity occurring in the home that might reasonably be thought private. Consequently, it is difficult to understand the Fourth Amendment's restrictions on gathering information from homes as an indirect means of protecting the private activities that occur there.

If the Fourth Amendment indeed does aim to protect private subject matters, then it would seem that government must be precluded from regulating certain private matters altogether. The Fourth Amendment, however, has not been so interpreted.



Instead of resorting to a unifying theoretical rationale, courts sometimes interpret the Constitution's protections in light of the particular governmental abuses the founders had in mind.

The Fourth Amendment grew out of the colonists' antipathy for the writs of assistance used by the British to enforce revenue laws. These court-issued writs authorized British officials to enter any house or other place to search for and seize prohibited and untaxed goods. Once issued, a writ remained in force throughout the lifetime of the sovereign and six months thereafter.

Construed narrowly as confined to this abuse, the Fourth Amendment condemns only unlimited court-authorized searches. The Fourth Amendment's text explicitly addresses this abuse, requiring that warrants be based "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The first clause of the Fourth Amendment, however, does not confine itself to judicially authorized searches and seizures and speaks more generally of the people's right to be free of "unreasonable searches and seizures." The Supreme Court thus has interpreted the Amendment as addressing both warrantless and warrant-based searches and seizures.

The privilege against self-incrimination found in the Fifth Amendment developed as a reaction to the perceived excesses of the British Courts of Star Chamber, which sat from 1487 to 1641. These courts required that accused persons answer any and all questions put to them and became a vehicle for the suppression of political dissent. By the eighteenth century, British law had rejected the inquisitorial practice of the Star Chamber in favor of the principle that no man should be compelled to accuse himself. It forbade the use of testimony compelled during trial or obtained before trial through torture. Nine state constitutions had a privilege against self-incrimination when the Fifth Amendment became law in 1791.

In determining the scope of the rights at stake as well as the remedies available for their violation, the Supreme Court has taken explicit account of governmental needs and has sought to strike a workable balance between those needs and informational privacy. Whether it has struck the appropriate balance and even used the right methodology for doing so are matters of controversy. The Court's work has been respectably criticized for both giving too much and too little weight to the interest of protecting informational privacy. In the limited space here, only the most basic features of legal doctrine can be summarized. It is important to recognize that the Fourth Amendment and the privilege against self-incrimination apply to actions by governmental officials. They offer no protection whatever against invasions of privacy perpetrated by private persons acting at their own behest.

The Fourth Amendment applies only to "searches and seizures." In deciding what this phrase comprehends, the Supreme Court generally has asked whether the governmental action frustrates an expectation of privacy that society regards as reasonable. Of course, persons have a justifiable expectation of privacy in the home, so that, absent consent, entry into it and the area close by constitutes a search. Persons also have a justifiable expectation of freedom of movement, so that an arrest constitutes a seizure.

One interesting set of issues concerns the use of technology to discern activities in the home. In *United States v. Kyllo*, 533 U.S. 27 (2001), the Supreme Court held that thermal imaging of a home constitutes a search. The Court declared that the

use of technology to access information that could not otherwise be obtained without entry into the home constitutes a search, at least when the technology is not in widespread use. It also constitutes a search to eavesdrop electronically on phone conversations originating in the home or even from a public phone booth unless one party to the conversation has consented.

In contrast, the Supreme Court has held that it does not constitute a search for law enforcement personnel to obtain a person's bank records, rummage through trash, use a **pen register** that records the phone numbers called, or electronically track the location of an **automobile** driven on public streets. The reasoning in these cases is that because the person has made this information accessible to third parties, the person has no protectible expectation of privacy.

Searches and seizures require justification. The Fourth Amendment's text provides that searches and seizures must be reasonable, and that warrants may not issue without probable cause. As some scholars have argued, this may be read to impose a general requirement of reasonableness and then to specify that reasonableness necessitates probable cause when a warrant is obtained. So read, the amendment generally requires neither a warrant nor probable cause for warrantless searches and seizures. The Supreme Court nonetheless has interpreted probable cause and issuance of a warrant as the general benchmark of reasonableness across the board, not just for warrant searches and seizures. The amendment thus embodies a preference for a warrant, which must issue from a neutral magistrate or judge and contain a particularized description of its scope. A warrantless search or seizure may be constitutional only if it fits into one of the exceptions that Court has recognized. Measured in terms of the real-world conduct they encompass, the exceptions are broad. For instance, warrants are often not required for searches and seizures involving automobiles, brief investigatory stops, or "exigent circumstances" involving a risk of flight or destruction of evidence.

For both warrant-based and warrantless searches, the Fourth Amendment generally requires probable cause. As with the warrant requirement, the Supreme Court has created exceptions. Some searches and seizures, such as administrative searches of closely regulated businesses and investigatory stops require only reasonable suspicion. Lesser justification is permissible, the Supreme Court has concluded, by virtue of the more minimal intrusion into privacy or the atypical governmental interests at stake. In a few areas, the Court has dispensed with a requirement of individualized suspicion altogether. For instance, it has upheld random stops near the border to check for aliens who have entered illegally, roadside **sobriety checkpoints** to prevent drunk driving, and **drug testing** unrelated to law enforcement in certain school and employment contexts.

A victim of Fourth Amendment violations has available two principal remedies. First, if the person has been charged with a crime, evidence obtained as a result of the violation may be excluded. This exclusionary rule has precipitated much criticism because of its effect of withholding relevant evidence of guilt and possibly letting the guilty go free. Historically, the Supreme Court has defended the rule as necessary to deter violations or, to put the point somewhat differently, to eliminate an incentive to violate that would otherwise exist (although more recently the Court found, in *Hudson v. Michigan*, that evidence seized even when this rule is violated may be admissible in court). In its core application, the rule precludes the prosecution from introducing illegally obtained evidence as part of its case-in-chief.



Outside of this application, the Supreme Court has established a number of exceptions to the rule premised on a judgment that the rule would impose costs in excess of any deterrent benefits in those applications. The exclusionary rule does not apply: when evidence has been obtained through good faith reliance on a warrant; when the prosecution seeks to impeach the accused's own trial testimony; or, in grand jury and deportation proceedings.

Second, a victim may sue governmental officials responsible for a Fourth Amendment violation for money damages. Litigants seeking such damages must surmount significant hurdles. As a practical matter, a person who in fact has committed criminal wrongdoing has great difficulty winning jury sympathy. In addition, individual governmental officials are legally immune from damage liability unless it can be shown that the law concerning the legality of their conduct was so specific and clearly established that no reasonable person could view their conduct as legitimate.

The Fifth Amendment privilege against self-incrimination prohibits civil and criminal courts from requiring a witness to answer questions that might incriminate her or him. It also prohibits law enforcement authorities from using coercion to induce a suspect to confess involuntarily. In *Miranda v. Arizona*, 384 U.S. 436 (1966), the Supreme Court concluded that interrogation while in police custody is inherently coercive. To dispel the inherent coercion, the suspect must be informed of the right not to answer questions and the right to have an attorney if the suspect so desires.

The degree to which the privilege protects privacy is limited by the rule that it does not generally allow documents to be withheld. The contents of documents, the Supreme Court has reasoned, are not testimonial in nature, and the privilege does not preclude government from requiring the disclosure of documents, presumably including even private diaries. The privilege permits documents to be withheld only when the government does not know of their existence, so that the very act of production, in effect, would constitute an incriminating admission that they exist.

Remedies for violations of the privilege against self-incrimination and against *Miranda* are similar to those available for Fourth Amendment violations. Money damages may be recovered from the responsible officials subject to the same practical and legal obstacles present in the Fourth Amendment context. Evidence obtained as a result of a confession coerced in violation of the privilege against self-incrimination is subject to exclusion. Statements of the accused in violation of *Miranda* are excluded but, in contrast with the Fourth Amendment context, evidence derived from such statements—the so-called fruits of the violation—are not subject to automatic exclusion. If police illegally seize a map revealing the location of the murder weapon, which the police then retrieve, the weapon would be subject to exclusion. But the weapon would not be excluded if a suspect reveals the weapon's location in statements obtained in violation of *Miranda*.

The ongoing War on Terror and technological developments raise new issues that the law regarding informational privacy inevitably will come to address. The War on Terror implicates the relationship between informational privacy and national security. The Supreme Court has sought to accommodate the needs of law enforcement through the definition of searches and seizures and through the creation of exceptions to the warrant and probable cause requirements and the exclusionary rule. It is certainly possible that the Supreme Court will relax normal Fourth Amendment requirements in the name of national security. As this

volume goes to press, for instance, it is known that the Bush administration has engaged in electronic surveillance of communications between persons in the United States, including citizens, and persons abroad suspected of involvement with Al Qaeda. Based on the threat of terror from foreign terror groups, the administration has argued that the Fourth Amendment does not require a warrant and requires only reasonable suspicion rather than probable cause for such surveillance. *United States v. United States District Court*, 407 U.S. 297 (1972), rejected a national security exception to the warrant requirement in the context of threats from wholly domestic groups. However, the Supreme Court studiously left open whether such an exception exists respecting foreign-based threats.

Technology threatens to shrink privacy in two sometimes overlapping ways. First, technologies such as electronic tracking, thermal imaging, face recognition, high resolution satellite photography, and information storage and retrieval greatly enhance government's ability to collect information. Second, **Internet**-based communication such as **electronic mail**, list serves, chat rooms, discussion boards, and **credit card** transactions multiply the circumstances in which individuals reveal information about themselves to third parties in ways that may be stored and later accessed by government. In other contexts, the Supreme Court has reasoned that by voluntarily disclosing information to a third party for one purpose, individuals relinquish any legitimate expectation of privacy respecting disclosure of the information to other third parties for other purposes. A mechanical application of this logic would imply that very little **computer**-based communication is subject to Fourth Amendment protection. The lower court case law and the scholarly commentary have just begun to grapple with how to strike a constitutionally appropriate balance between privacy and governmental needs in the computer age.

II. Individual Autonomy

In addition to limiting the government's access to information, the Constitution gives individuals a right to make certain choices about their lives. The First Amendment's protection of freedom of speech grants individuals a right to form and express their own beliefs and, according to the Supreme Court, implies a "freedom to associate and privacy in one's associations" (*NAACP v. Alabama*, 357 U.S. 44, 1958). The First Amendment's religion clause makes religious belief principally a matter for individuals, not government, and gives them freedom to exercise their religion as well as the freedom from governmental religious establishments. This entry will not focus on these First Amendment rights but will instead address the rights of autonomy the Supreme Court has recognized in the areas of sexuality and family life. It is these rights, which are not enumerated in the Constitution's text, that have come to dominate discussions of and controversies over constitutional privacy.

Like informational privacy, constitutionally protected areas of individual autonomy rely upon a principle of governmental noninterference. Autonomy, however, requires noninterference of significantly greater scope. Constitutional protections of informational privacy inhibit the government's access to certain sources of information, yet they do not by themselves preclude the government from regulating any activity: other sources of information remain available. Government may not enforce a criminal prohibition against abortion, for example, by coercing



an individual to incriminate herself or by searching her home without a warrant for medical bills establishing that a suspect has had one. Insofar as the Constitution's protections of informational privacy are concerned, however, the government may enforce an abortion prohibition by securing the testimony of the physician who performed the abortion. In contrast, rights of autonomy preclude the government from prohibiting the decisions and actions within those rights. The Supreme Court's abortion decisions do not permit government to completely prohibit women from choosing to have early abortions.

In addition to denying government the authority to regulate certain activities, autonomy implies a right of informational privacy as a corollary. Constitutional rights of informational privacy inhibit access only to certain sources of information. In contrast, rights of autonomy tend to render certain subjects of information off limits. Of course, government may not use sources of information shielded by the Fourth Amendment and the Fifth Amendment privilege against self-incrimination to pry into activity protected by a right of autonomy. But a right of autonomy also tends to foreclose inquiry through other sources of information as well. Because women have a constitutional right to abortion, government may neither obtain a Fourth Amendment warrant nor question witnesses about such a choice unless it is relevant to some other subject that is a permissible object of government regulation. By tending to shield certain subjects from official inquiry, rights of autonomy create an umbrella of privacy that is larger than that established by the Fourth and Fifth Amendments.

In press accounts and popular discussion, one often hears that the constitutional right of privacy is a matter of some controversy. It is important to recognize that there is no controversy over the existence of constitutional protections of informational privacy that derive almost entirely from the rights specified in the Constitution's text. The scope of these protections is a matter of interpretation and argument, to be sure, but no one challenges their very existence. Similarly, rights of autonomy are not in question insofar as they involve textually specified rights such as the First Amendment's protections of freedom of speech and of religion.

In contrast, there is serious controversy over the existence of rights of autonomy that do not derive from any specific right found in the Constitution's text. In its decisions pertaining to contraception, abortion, and homosexuality, the Supreme Court has affirmed rights of individual autonomy that go considerably beyond textually specified rights. In his majority opinion in *Griswold v. Connecticut*, 381 U.S. 479 (1965), Justice Douglas declared that a constitutional **zone of privacy** derives indirectly from textually specified guarantees found in the First, Third, Fourth, and Fifth Amendments. These specific guarantees, Justice Douglas opined, "have penumbras, formed by [their] emanations."

In more recent decisions, the Court has not relied upon Justice Douglas's concept of a penumbral right. Instead, it has located rights of autonomy in the Due Process Clause of the Fourteenth Amendment. These rights cannot be derived even indirectly from the text of that clause, which provides that "no State shall deprive any person of life, liberty, or property without due process of law." The text evinces a concern for the process alone. It permits the government to deprive individuals of what is important to them, including life itself, as long as government provides the

process that is due. The Court nonetheless has looked beyond the purely procedural orientation of the Due Process Clause's text to incorporate a concept of "ordered liberty" encompassing an individual's right to control certain areas of life.

In doing so, the Court has unleashed a vigorous and interesting debate over the existence of unenumerated constitutional rights generally. The Court's critics maintain the Constitution's text and history provide no warrant for such rights. In their view, the justices who recognize such rights necessarily rely upon their own subjective political and philosophical predilections and engage in illegitimate judicial legislation.

Those who defend the existence of unenumerated rights can point to the text and history of the Ninth Amendment and the Privileges and Immunities Clause of the Fourteenth Amendment. The Ninth Amendment provides that "the enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." Its drafting and ratification history suggest that it affirms the existence of unspecified rights. In the debates over ratification of the original Constitution, the Anti-Federalists had argued that the original Constitution should not be ratified because, unlike state constitutions, it did not contain a listing of protected individual rights. In response, the Federalists maintained that any such listing would be dangerous. A list, they argued, inevitably would be incomplete and give rise to an inference that unlisted rights are unprotected. The most natural reading of the Ninth Amendment is that it guards against this objectionable inference.

The Privileges and Immunities Clause of the Fourteenth Amendment also can be seen to recognize the existence of constitutional rights going beyond those specifically enumerated in the text. That clause prohibits states from abridging "the privileges or immunities of citizens of the United States" but does not specify those privileges. Senator Jacob Howard, who served as the Fourteenth Amendment's floor manager in the Senate, evidently understood the clause to protect rights not specifically described in the Constitution's text. He declared that the protected privileges encompass "fundamental rights lying at the basis of society" whose content would be "discussed and adjudicated when they should happen practically to arise." Representative John A. Bingham, the principal author of that part of the Fourteenth Amendment containing the Privileges and Immunities Clause, shared this understanding. He held that the "privileges and immunities of citizens of the United States are chiefly defined in the first eight amendments to the Constitution." In other words, the protected privileges include but are not limited to the rights the text enumerates. These views were rooted in natural law philosophy. There were undoubtedly physical laws regulating the universe that scientists had not yet specified but, with scientific progress, would so specify in future. So, too, the moral laws regulating the universe were incompletely understood. It was important to leave room for progress in the understanding of these moral laws and not to forever freeze the list of fundamental rights.

Those who oppose the existence of unenumerated rights offer alternative explanations of these provisions. The Ninth Amendment, they argue, means only that states remain free to establish rights beyond those protected in the federal Constitution as a matter of their own law. As for the Privileges and Immunities Clause of the Fourteenth Amendment, they contend that Senator Howard's and Representative Bingham's natural law view was not widely enough shared to give it the force of law.



Although it has chosen the Due Process Clause rather than the Privileges and Immunities Clause of the Ninth Amendment as the source, the Supreme Court has affirmed the existence of unenumerated constitutional rights in general and the rights of personal autonomy in particular. In so doing, the Court has opened the door to a controversy over the determination of their scope. Once the existence of unenumerated rights or a right of autonomy is conceded, how does or should the Supreme Court determine what it encompasses? The Court obviously cannot determine the scope of an unenumerated right simply by consulting the Constitution's text. Nor would many modern thinkers contend that fundamental rights are awaiting discovery in a natural moral order accessible through reason or intuition.

In fixing the scope of the unenumerated right of autonomy, the Supreme Court has used different approaches. Some cases purport to rely on societal tradition. In *Washington et al. v. Glucksberg et al.*, 521 U.S. 702 (1997), for instance, the Court insisted that "fundamental rights and liberties [be] . . . 'deeply rooted in this Nation's history and tradition.'" The Court declined to recognize a fundamental right to physician assisted suicide, finding no established tradition in support of this practice. The emphasis on tradition often is linked to unease with unenumerated rights and reflects a strategy for limiting their import. Opponents of unenumerated rights, such as Justice Scalia, point to the danger that the unelected Supreme Court justices will give their own subjective notions the force of constitutional law. Opponents seek to limit judicial subjectivity by requiring that any claimed right find overwhelming support in the enactments of legislatures and judicial decisions over the course of time. Using this strategy, Justice Scalia consistently has rejected appeals to unenumerated rights.

The Supreme Court has not always relied upon tradition, particularly when it has expanded the scope of enumerated rights of autonomy. In *Roe v. Wade*, 410 U.S. 113 (1973), for instance, the Court held that constitutional privacy gives women a right to choose an abortion despite acknowledging that its decision conflicted with laws then in force in a majority of the states. In striking down a Texas law prohibiting consensual adult homosexual **sodomy**, the Court spoke of an "emerging awareness" that such laws impermissibly invade the control of adults over their private sex lives. It did not, however, purport to derive its holding from tradition. In fact, *Lawrence v. Texas*, 539 U.S. 558 (2003), expressly overrules *Bowers v. Hardwick*, 478 U.S. 186 (1986), an earlier decision that had rejected a claimed constitutional right to consensual homosexual intimacy because of the lack of a supporting societal tradition.

When it does not place exclusive reliance upon tradition, the Supreme Court has referred to its past decisions and the principles it has identified as standing behind them. The Court has not fashioned any precise rules or principles. Its explanations variously invoke the life-shaping character of the choice at stake, its quasi-religious nature, and the absence of demonstrable harm to others. The Court even has relied upon decisions of foreign courts as support. The phrase "reasoned judgment," which some Justices have used, captures the imprecision of the method at work.

The uncertain scope of and rationale for its decisions in establishing new rights have fueled charges that the Court has engaged in law creation rather than interpretation. It is no doubt true that the Court's cases are susceptible of multiple readings and give the justices fairly wide berth. However, a method based upon societal tradition

likewise gives the Court great latitude. The justices often select from competing traditions. For example, longstanding proscriptions against sodomy may exist alongside an established practice of nonenforcement and a more general tradition of governmental noninvolvement in the sex lives of consenting adults. The justices' choice of which tradition to emphasize is not guided by tradition. It instead can be seen to reflect an undisclosed view of the desirability of the particular right in question or the doctrine of unenumerated rights. In short, the choice whether to recognize any particular autonomy right or unenumerated right generally is not dictated by the Constitution's text or history. It inevitably engages the justices' philosophical beliefs concerning the powers of government relative to the individual, the role of the judicial branch relative to the legislature and executive branches, and the degree to which government regulation may be based upon religion.

While the Supreme Court's use of an unenumerated right of autonomy traces back to the nineteenth century, the focus of the right has shifted from economic to personal matters. In a series of cases in the late nineteenth and early twentieth century, the Court read a kind of economic libertarianism into the Fourteenth Amendment's Due Process Clause. That clause, the Court held, affords strong, although not absolute, protection to an individual's liberty to contract freely with others. It invoked this right of freedom of contract largely against economic regulation, using it to invalidate numerous measures to protect workers, women, and children. In *Lochner v. New York*, 198 U.S. 45 (1905), for instance, the Court struck down a New York statute limiting the number of hours bakers could work on the grounds that it violated the liberty of bakers and bakery owners to contract freely.

In the mid-1930s, the Court retreated from the *Lochner*-era doctrine that due process implies protection for property rights. But the Supreme Court did not forever abandon the idea of an unenumerated right of autonomy. Beginning in the 1960s, it infused this idea with new content, focusing on rights pertaining to personhood and family life rather than to business and property.

This evolution from rights of property to personhood is illustrated by the contrast between the fate of two *Lochner*-era decisions and that of *Lochner* itself. In *Meyer v. Nebraska*, 262 U.S. 390 (1923), the Supreme Court overturned a Nebraska law that prohibited the teaching of German in schools. The other decision, *Pierce v. Society of Sisters*, 268 U.S. 510 (1925), struck down an Oregon statute prohibiting parents from sending their children to private schools. Consistent with the general tenor of the *Lochner* era, in *Pierce* the Court stressed the property right of private schools to deal freely with customers. The Supreme Court continues to cite *Meyer* and *Pierce* with approval. Their underlying rationale, however, has been subtly recast in accordance with modern jurisprudential sensibilities. Instead of focusing on the rights of teachers and schools to sell their wares in a free market, the modern Court has focused on language in those decisions that speak of parents' liberty to direct their children's upbringing. In contrast, the result in *Lochner* could not be explained on the basis of an individual's right to make decisions of a deeply personal nature pertaining to family or self. The result in *Lochner* consequently is no longer regarded as good law, and government now may regulate wages and working conditions without violating a constitutional right of autonomy.

According to Supreme Court case law, the Constitution creates a zone of autonomy that is not limited to and does not derive from the rights specified in



the text. In that zone, government may not dictate the outcome of certain key decisions pertaining to personhood and family life. These broad-brush statements conceal considerable diversity in cases over which rights are found in this zone, their basis and scope, and the degree to which government may impose restrictions.

The Supreme Court long has recognized a fundamental right on the part of parents to direct the upbringing of their children. During the *Lochner* era, it relied upon this right to strike down laws prohibiting parents from sending their children to private schools and from authorizing them to be taught foreign languages. More recently, it overturned a state court decision that, without giving any deference to parental objections, had granted grandparents a right to visit children.

Under Supreme Court precedent, individuals also have a right to decide whether to become parents in the first instance. The Court first recognized a right on the part of married couples to obtain contraceptives and later extended the right to unmarried persons. A much more dramatic extension of the right came with the landmark decision in *Roe v. Wade*, which holds that women have a constitutional right to choose an abortion. Under *Roe*'s trimester framework, government may not regulate abortion as such in the first trimester, may impose only those restrictions that are strictly necessary to promote maternal health in the second trimester, and may generally prohibit abortion altogether after the fetus becomes viable. In *Planned Parenthood v. Casey*, 505 U.S. 833 (1992), the justices, by a narrow 5-to-4 majority, reaffirmed *Roe*'s central holding that government may not prohibit abortion altogether before fetal viability. The crucial plurality opinion jointly authored by three justices modified *Roe*'s framework in a way that gives government greater regulatory leeway. So long as it does not unduly burden the right to an abortion, government may regulate throughout the pregnancy to promote maternal health and to provide pregnant women with truthful information designed to persuade them to choose childbirth over abortion.

Another aspect of what might be described as the right to define one's family is the choice of partner. *Loving v. Virginia*, 388 U.S. 1 (1967), invalidated a Virginia miscegenation statute forbidding persons of different races from marrying. In addition to holding the explicit racial classification a violation of equal protection, the Supreme Court concluded that it violated an unenumerated due process right to marry. This "fundamental freedom," the Court reasoned, may not be denied on "so unsupportable a basis as" race. More recently, the Court has recognized a right on the part of homosexuals to choose intimate partners and engage in sexual intimacy. *Lawrence v. Texas* overturned a criminal prohibition against consensual homosexual sodomy in the home. Overruling a prior case that had refused to locate such conduct within a fundamental right, the Supreme Court spoke of the liberty of all individuals to choose their personal bonds and accompanying sexual intimacies. Government may not use the criminal law to demean homosexuals for making such choices.

Finally, the Supreme Court has begun to address whether constitutionally protected autonomy includes a **right to die**. Its cases suggest that while there is some right to voluntary passive euthanasia (the withdrawal or withholding of medical treatment), there is essentially no right to physician-assisted suicide (the provision of the means to end life to the patient by the physician).

The Supreme Court's case law is not a model of clarity or consistency. Whereas the right to die cases view constitutional autonomy as defined by societal tradition,

the cases pertaining to abortion and sexuality do not. In affirming the existence of autonomy rights not based upon tradition, the Court has appealed to a variety of rationales. The cases also vary widely concerning the degree of protection that unenumerated rights receive. Constitutional analysis typically distinguishes between fundamental and nonfundamental rights. Restrictions on nonfundamental rights receive “strict scrutiny.” Under this demanding standard of judicial review, regulation survives only if the justices make their own independent determination that regulation is strictly necessary to further a compelling interest. Although *Roe v. Wade* used strict scrutiny, the Court now uses an “undue burden” standard in its abortion cases. This test deliberately gives government more regulatory freedom than does strict scrutiny. In addressing regulation of voluntary passive euthanasia and parental rights, the Court has been vague about the standard of review. The Court’s opinion in *Lawrence v. Texas* even uses the language of the highly deferential rational basis test applicable to nonfundamental rights.

The existence and scope of an unenumerated right of autonomy has been a source of political controversy, in significant measure because of its connection with abortion. It has received attention during presidential elections and has provided a conspicuous backdrop for presidential appointments and Senate confirmation hearings. It seems quite unlikely that a majority of the justices will repudiate the existence of such a right altogether and overrule established precedents such as *Griswold v. Connecticut* and *Meyer v. Nebraska*. The question for the future is whether a majority of justices will conceive of the right so narrowly that it lacks contemporary significance.

Two issues appropriately have received attention as relevant in the near term. One concerns the fate of the right to an abortion. As of this writing, five current justices have reaffirmed and two have repudiated *Roe v. Wade*’s central holding that a woman has a constitutional right of access to abortion before fetal viability. Together with Justice Alito and Chief Justice Roberts, who have not expressed any view, new appointments to the Court could call into question the bare majority that evidently now exists in support of this holding.

The other prominent issue, which lower courts have begun to address with conflicting results, is whether same-sex couples may claim a constitutional right to marry. One issue is whether laws prohibiting such marriages violate the Equal Protection Clause of the Fourteenth Amendment by unjustifiably discriminating on the basis of homosexuality. The other issue, which is relevant here, concerns whether such laws violate an unenumerated right of autonomy. *Lawrence v. Texas* and *Loving v. Virginia* furnish considerable support for holding that all adults have a constitutional right to choose their marital partners. A number of the attributes that have prompted the Court to include a choice within a constitutionally protected zone of autonomy are present: the choice involves family; it has a strong bearing on the direction of one’s long-term future; a choice to marry a person of the same sex does not inflict any direct or immediate harm on others; and, the reasons for denying such a choice are largely religious at bottom. On the other hand, a tradition-based approach easily could lead the justices to conclude that same-sex marriage is not within a constitutionally protected zone of autonomy. A significant number of recent state enactments explicitly outlaw same-sex marriage, and the federal Defense of Marriage Act authorizes states not to recognize the validity of same-sex marriages rendered in other States.



See also: **Privacy, Definition of; Privacy, Philosophical Foundations of**

Suggested Reading: Bennett, Colin, and R. Grant (eds.). *Visions of Privacy*. Toronto: University of Toronto Press, 1999; Bork, Robert. *The Tempting of America*. Boston: Free Press, 1989; Brinn, David. *The Transparent Society*. New York: Perseus, 1999; Goldberg, Carole. *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security*. New York: W. W. Norton, 2002; Kerr, Orin S. "Searches and Seizures in a Digital World," *Harvard Law Review* 119 (2005): 531–579; Levy, Leonard W. *Origins of the Fifth Amendment: The Privilege against Self-Incrimination*. New York: Macmillan, 1968; Rappaport, Aaron J. "Beyond Personhood and Autonomy: Moral Theory and the Premises of Privacy," *Utah Law Review* (2002): 441–507; Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House, 2000; Rubinfeld, Jed. "The Right of Privacy," *Harvard Law Review* 102 (1989): 737–752; Solove, Daniel. *The Digital Person*. New York: New York University Press, 2004; Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy," *Harvard Law Review* 4 (1890): 193.

Thomas G. Stacy

Cookies. *See* **Computers; Internet**

Counter Intelligence Program (COINTELPRO)

Convinced that American Communists were agents of the Soviet Union and thus threatened the nation's security, **Federal Bureau of Investigation (FBI)** officials, in initiatives dating from the Bolshevik Revolution in 1917, closely monitored the U.S. Communist Party, including **wiretapping** the Soviet embassy, Communist Party headquarters, and prominent American Communists. FBI surveillance of Communist activists intensified during the Cold War era. For example, FBI officials pressured the Justice Department to prosecute Communist activists for violating the Smith Act of 1940 for conspiring to overthrow the U.S. government by force, and also for failing to register with the Subversive Activities Review Board as required under the McCarran Act of 1950. These efforts succeeded at first when the Supreme Court upheld the constitutionality of the Smith Act and the conviction of the top leaders of the Communist Party in *Dennis v. United States*, 341 U.S. 494 (1951).

The shift in the Supreme Court's interpretation of federal **surveillance** powers with the onset of the Warren Court subverted this prosecutive strategy. In *Yates v. United States*, 354 U.S. 298 (1957), the Court reaffirmed the constitutionality of the Smith Act, but held that the act proscribed only advocacy to commit a violent act and not mere advocacy. One year earlier, in *Communist Party v. Subversive Activities Control Board*, 351 U.S. 115 (1956), the Court upheld the constitutionality of the McCarran Act, but held that the **privilege** of the Fifth Amendment allowed the Communist Party leadership to refuse to identify the Party's membership and its publications. These rulings caused FBI officials to question the value of prosecuting Communists under these acts, further heightening their concerns about having to expose FBI informers in the Communist Party during trials. In August 1956, seeking alternative means to combat the Communist threat, FBI officials authorized a formal program, COINTELPRO–Communist Party, to

“harass, disrupt, and discredit” the Communist Party by either promoting factionalism within party ranks or leaking derogatory information about party officials to the public. COINTELPRO–Communist Party was a highly secret program, initiated solely on the authority of FBI Director **J. Edgar Hoover**.

During the tumultuous 1960s, FBI officials extended the COINTELPRO system to other targeted radical organizations and their leadership: in 1961 to the Socialist Workers Party, in 1964 to white hate/nationalist organizations (notably the Ku Klux Klan), in 1965 to black hate/nationalist organizations (notably the Black Panther Party), and in 1968 to the New Left (notably Students for a Democratic Society). FBI agents were pressured to devise innovative and aggressive tactics to disrupt the targeted organizations. The proposed and adopted methods varied from the banal to the sinister, including provoking violence among black nationalist organizations, sending anonymous letters to parents of radical students reporting on their son’s or daughter’s illicit sexual activities or use of illegal drugs, and sending anonymous letters to the wives of Klan members reporting on their husbands’ extramarital activities.

COINTELPRO was a carefully guarded program. Nonetheless, FBI officials’ creation of centralized files that recorded recommended courses of action and headquarters review and approval of documents ironically made the program vulnerable to a March 1971 break-in at the FBI’s Media, Pennsylvania, resident agency. After seizing and then photocopying FBI files, radical activists sent copies to members of Congress, journalists, and the identified targets of FBI surveillance. In response, in August 1971 Hoover ordered the termination of the COINTELPRO program and advised FBI agents that future proposed “counterintelligence action” should be submitted to FBI headquarters “under the individual case caption” and should be conducted on “an individual basis,” rather than under a centralized caption program.

The FBI director’s attempt to foreclose further publicity about FBI activities was negated, however, by the action of NBC correspondent Carl Stern. A recipient of one of the photocopied Media documents, which was captioned COINTELPRO, and not knowing the meaning of the document’s caption, Stern filed a **Freedom of Information Act** request for the FBI’s COINTELPRO files. Attorney General John Mitchell rebuffed Stern’s request. The NBC correspondent filed suit in federal court, and in September 1973 the court ruled in his favor. At first deliberating whether to appeal, Justice Department officials, chastened by the changed political setting created by the recent Watergate hearings, decided not to contest the order. The released COINTELPRO files later became one focus of an intensive congressional review conducted in 1975 by the **Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities** (also known as the Church Committee), which commanded widespread public attention and documented the scope and nature of FBI abuses of privacy rights.

See also: **Internal Security Act of 1950; McCarthyism**

Suggested Reading: Cunningham, David, and Barb Browning. “The Emergence of Worthy Targets: Official Frames and Deviance Narratives within the FBI,” *Sociological Forum* 19 (2004): 347–369; Goldstein, Robert Justin. “The FBI and American Politics Textbooks,” *Political Science* 18 (1985): 237–246; PBS Now. *Going Undercover/Criminalizing Dissent?* <http://www.pbs.org/now/politics/cointelpro.html>.



Online, March 2006; Theoharis, Athan. *The FBI and American Democracy: A Brief Critical History*. Lawrence: University Press of Kansas, 2004; Wolf, Paul. *COINTEL-PRO*. <http://www.icdc.com/~paulwolf/cointelpro/cointel.htm>. Online, March 2006.

Athan Theoharis

Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975)

In 1971 Martin Cohn's 17-year-old daughter was the victim of an assault and rape, which she did not survive. Six youths were soon indicted for her rape and murder. Although there was substantial press coverage of the incident and the trial, the victim's name was never disclosed, pursuant to a Georgia statute making it a misdemeanor to publish or broadcast the identity of a rape victim. Some eight months later, during the trial, a reporter covering the incident learned the name of the victim from an examination of the indictments. These indictments were **public records**, to which the reporter had access. Later that day, the reporter broadcast a report concerning the trial over through a television station owned by Cox Broadcasting Corporation's network. In the report, he revealed the victim's name. The report was repeated the following day.

Martin Cohn brought an action against Cox, relying on the statute and claiming that the **disclosure** invaded his right to privacy. Cox admitted that it made the broadcasts but claimed that the First Amendment protected the disclosure. The trial court rejected the constitutional claims and granted summary judgment, holding that the statute provided for a civil action, and that Cox was liable under the statute as a matter of law because it had broadcast the victim's identity. On appeal, the Georgia Supreme Court, in its initial opinion, held that the trial court erred in finding that the statute created a civil cause of action for invasion of privacy. It therefore reversed the lower court and did not reach the constitutional argument. It did hold, however, that a jury must resolve the invasion of privacy claim, which could stand on its own, without the statute. Upon a motion for rehearing, the Georgia Supreme Court did reach the constitutionality of the statute: it sustained the statute as a legitimate limitation of free speech, holding that there was no public interest or general concern about the identity of a rape victim that would make the right to disclose the identity rise to the level of First Amendment protection. The Cox Broadcasting Corporation appealed.

The Supreme Court of the United States delivered an opinion authored by Justice Byron White. After a lengthy discussion of jurisdiction, White concluded that the Court was authorized to consider the merits of the case and reversed the judgment of the Georgia Supreme Court. The Court recognized that there is a **zone of privacy** surrounding every individual that the state may protect from invasion by an abusive press. It also recognized that the twentieth century had seen "a strong tide running in favor of the so-called right of privacy." The Court noted, however, that this case did not involve the appropriation of a name or a photograph, a physical intrusion into a private area, or a publication of false, defamatory, or otherwise private information.

Cox Broadcasting's argument was that the press may not be held civilly or criminally liable for publishing information that is neither false nor misleading but is absolutely accurate, however damaging it may be to reputation or individual sensibilities. The Court recognized that truth is a defense in defamation actions by public

figures, but the question as to whether the truthfulness of the disclosure is protected for private individuals involved in matters unrelated to public affairs was undecided.

The issue pitted two deeply rooted rights against one another: the right to privacy versus the freedom of speech and of the press. The Court narrowed the issue to the question of whether the State may impose sanctions upon the accurate publication of the name of a rape victim obtained from judicial records that were maintained in connection with a prosecution and open to public inspection. The Court held that the State may not; the statute was unconstitutional. The Court stated that the developing law concerning the tort of invasion of privacy recognized a **privilege** in the press to report the events of judicial proceedings. In particular, publishing information contained in public records is not within the reach of the sort of privacy action Cohn sought here. The Court recognized that the public has a right to a vigorous press, and that truthful information available in public records is protected speech. Here, the reporter based his broadcast upon notes taken during proceedings in open court, and upon the public records provided to him at his request. In the Court's view, a statute sanctioning this disclosure violated the constitutional guarantees of the First Amendment. Consequently, in this case, the Court determined that freedom of the press took precedence over claims to the right of privacy.

See also: **Constitutional protections; Journalism; Sexual violence**

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Hall, Kermit L. *Conscience, Expression and Privacy: The Supreme Court in American Society*. New York: Garland, 2000; Smith, Robert Ellis. *Compilation of State and Federal Privacy Laws*. Providence, RI: Privacy Journal, 1992; Sullivan, Kathleen M., and Gerald Gunther. *First Amendment Law*. St. Paul, MN: West, 1998.

Larkin R. Evans

Credit cards

Two of every three American citizens possess one or more credit cards. Every card operates in a credit card system: a form of retail transaction where a card issuer (i.e., banks and other financial institutions) lends the cardholder money for purchases. A unique credit card number identifies each individual account and the magnetic strip stores personal and account information. Scanners at retail outlets verify a card's authenticity and check accounts for sufficient credit. At the end of the twentieth century, American consumers possessed over 1.5 billion credit cards. Collectively, all of the account and **personal identifiable information** linked to each card is stored in large networked databases. The opportunities for financial gain and the risks of loss present in this system engender a number of problems with respect to individual privacy, ranging from receipt of junk mail to **identity fraud**.

The first form of credit cards, which arrived early in the twentieth century, was the "retail card" issued by merchants to boost sales of their own products. The modern "universal card," which is accepted by multiple merchants, appeared after



World War II with the Diner's Club. A second universal card followed from American Express in 1958. Both Diner's Club and American Express were "travel and entertainment" cards, requiring customers to settle all charges at the end of the month. Bank cards, a different form of universal card, offered revolving credit, where debts carried over from month to month and accrued interest. In 1959, Bank of America offered the first bank card, which was called the BankAmericard and was renamed Visa in the 1970s. A group of Chicago banks introduced Master Charge in 1968, which later became MasterCard. At present, four major credit card brands control the majority of the market: Visa, MasterCard, American Express, and Discover. Visa and MasterCard, now joint ventures that consist of thousands of financial institutions, have consistently dominated the industry to such a degree that a U.S. district court found both guilty of antitrust violations in 2001.

The modern credit card represents an emblem of contemporary consumer culture. As consumption increasingly defines private life, consumer spending now represents about two-thirds of the \$11 trillion U.S. economy. Debt finances an expanding proportion of this spending. Consumer credit dramatically accelerated in the late twentieth and into the twenty-first century. Between 1989 and 1999, consumer credit rose over 80 percent. In the early years of the twenty-first century, American households used approximately 18 percent of their disposable income to service debt. According to the U.S. Federal Reserve, total consumer debt exceeded \$2 trillion dollars in 2005. A sharp fall in household savings has accompanied the birth of this debt-dependent society. Saving rates in the United States plunged to all-time lows in 2005, dropping from 8 percent in the early 1980s to the present .2 percent. But the consumer debt avalanche indicates more than lifestyle changes concerning buying and saving; it reveals a broad social tendency toward the individualization of risk that also began in the 1980s with the rollback of the welfare state. In the twenty-first century, consumer credit substitutes for the social safety net.

Critical observers of the "Credit Card Nation" stress the social cost of credit dependency. One such social cost involves the radical invasions of privacy made possible by the credit card industry. Since the 1980s, consumer culture and social policy have privileged private consumption over civic participation and public investment. Ironically, the business infrastructure financing this transformation opened private life to new legal and illegal intrusions. The source of these privacy threats emanates, in part, from the information-intensive quality of the credit card industry.

The consumer credit industry depends upon the storage and rapid flow of personal data. In a general sense, credit involves inter-temporal exchange: a buyer obtains a good or service for a deferred payment. Because a promise to pay completes the transaction, trust forms the foundation of credit. Creditors, then, manage trust to reduce uncertainty by assessing a borrower's willingness and ability to repay. Thus, credit cards impel the collection of personal information for risk analysis. These data are an invaluable and strategic asset for card issuers, so the credit industry continuously creates, maintains, and upgrades customer databases. Major sources of consumer information for card issuers include applications, billings, and **transaction-generated data** from individual purchases, third-party processors, major credit bureaus, and **data brokers**. Businesses in the credit industry use personal information for multiple purposes: (1) identification of possible

customers; (2) evaluation of the 100 million-plus applications every year; (3) account management (i.e., setting interest rates and credit limits); (4) fraud detection; and (5) packaging and assessment of portfolios. Overall, the credit industry subjects consumers to a perpetual gaze in order to optimize revenues from established accounts and locate new customers.

The organizational structure of the credit card system intensifies the flow of personal information. Thousands of financial institutions and some non-financial institutions, like General Motors and Marriot, enter joint ventures to issue cards. To cut business costs, card issuers frequently outsource transaction processing to third-party processors, consequently sending personal information to more firms. Issuers also furnish payment records to credit bureaus. Issuers also purchase personal data from bureaus in the form of credit reports and lists of “prescreened” prospects. In the case of the largest issuers, personal information flows throughout the organizational units of corporate conglomerates in a practice known as “affiliate sharing.” Customer purchase records present another revenue source to card issuers. Companies may exploit transaction-generated data for internal marketing by developing consumer profiles; alternatively, they may sell these data on the information market to direct marketers and data brokers.

Although the 1970 **Fair Credit Reporting Act** curtailed the use of credit reports—and granted consumers access to view their reports and correct errors—prescreening, affiliate sharing, and the sale of transaction-generated data escaped regulation until the late 1990s. In this loose regulatory climate, the widespread exchange of personal information directly encouraged extensive use of junk mail and **telemarketing**, which many Americans regard as intrusive invasions of privacy. In any year, over 5 billion credit card solicitations target U.S. consumers. The sale of transaction-generated data (and the complex forms of data analysis and **data mining**) fuels a larger advertising industry that saturates Americans with a broader array of commercial propaganda. However, some recent federal legislation—including the 1996 amendments to the Fair Credit Reporting Act, the 1999 Gramm-Leach-Bliley Act, and the 2003 Fair and Accurate Credit Transaction Act—have given consumers more control over the use of their personal information. For example, “opt-out provisions” allow consumers to restrict the sale of personal information by credit bureaus and card issuers.

Aside from these commercial threats to privacy, the credit industry creates opportune conditions for identity fraud. On occasion, illegitimate agents simply purchase personal information from banks, credit bureaus, and other information brokers. For example, Charters Pacific Bank in Los Angeles sold over 4 million credit card numbers that were illegally billed. In other instances, security breaches of consumer databases leave consumers vulnerable. Following the scandal of a major data broker named ChoicePoint in February 2005 that jeopardized the privacy of 145,000 consumers, the Privacy Rights Clearing House calculated that 114 subsequent major breaches occurred in the industry during the remainder of the year. The credit industry presents simpler means of fraud as well. Its heavy reliance on junk mail makes any mailbox a criminal opportunity. Furthermore, innovative forms of retail intended to speed commerce (e.g., e-commerce, telephone transactions, and pay-at-the-pump) sidestep face-to-face practices of verification, making the use of stolen cards less risky. Industry defenders assert that fraud and identity



theft add sizable cost to business. Privacy advocates counter that cost-cutting pressures lead to an overreliance on automation and insufficient investment in security, and, on top of that, information handlers fail to notify exposed consumers.

Novel challenges to privacy emerge in this debt-dependent society. For every citizen, information becomes indispensable in a riskier environment stripped of social protections. And in the United States, personal information is proprietary but not owned by private persons, who are left to their own devices to negotiate mounting privacy hazards.

See also: **Credit rating; Digital cash; Financial Services Modernization Act of 1999; Opt-in vs. opt-out**

Suggested Reading: Cate, Fred H. "Privacy, Consumer Credit, and the Regulation of Personal Information." In Thomas A. Durkin and Michael E. Staten (eds.), *The Impact of Public Policy on Consumer Credit*, pp. 229–276. Boston: Kluwer Academic Publishers, 2002; Cate, Fred H., Robert E. Liton, Michael Staten, and Peter J. Wallison. *Financial Privacy, Consumer Prosperity, and the Public Good*. Washington, DC: Brookings Institute, 2003; Electronic Privacy Information Center. *Right to Financial Privacy Act*. www.epic.org/privacy/rfpa/. Online, March 2006; Evans, David S., and Richard Schmalensee. *Playing with Plastic: The Digital Revolution in Buying and Borrowing*. Cambridge, MA: MIT Press, 1999; Fischer, Richard L. *The Law of Financial Privacy*. Washington, DC: A.S. Pratt & Sons, 2002; Manning, Robert D. *Credit Card Nation: The Consequences of America's Addiction to Credit*. New York: Basic Books, 2000; Scousen, Mark. *The Complete Guide to Financial Privacy*, 4th ed. New York: Simon & Schuster, 1983.

Brian Azcona

Credit rating

The ability of consumers to obtain credit, housing, insurance, utility service, employment, and other services is determined in part by centralized records of credit histories maintained by credit bureaus. A credit rating, or credit score, is a "grade" of creditworthiness that credit bureaus compile as a summary of the consumer's credit history and then issue to businesses upon request. The rating is a shorthand version of a consumer's credit history in numerical form. A business can then use the rating in making a decision whether or not to engage in the transaction with the consumer, and if so, under what terms. The precise algorithm credit bureaus use to compile credit ratings is not publicly known, but factors generally affecting the rating include the amount of money owed to creditors, the consumer's payment history, whether the consumer is seeking several new extensions of credit, and the types of credit lines the consumer holds.

Credit histories in one form or another have long been an important factor in decisions to extend or deny credit to consumers. Before the development of computerized credit scoring, such decisions required a skilled evaluation of the information in a consumer's background and credit history to determine the likelihood of payment in a timely manner. **Computer** models now perform such evaluations and reduce the calculation to a number. In the system most often used by credit bureaus, the numbers range from zero to over eight hundred, with a higher score indicating a stronger credit history.

During the 1990s, mortgage underwriters increasingly used credit ratings to evaluate credit risks of mortgage applicants. By the end of the century, approximately 70 percent of all mortgages were underwritten using an automated credit rating, and the percentage was rising. As the scoring system became regarded as a reasonably accurate predictor of consumer risk, greater numbers of **credit card** issuers, insurers, and other businesses began using credit scores as part of their decisionmaking processes.

Today, credit ratings are not only used to decide whether or not to extend credit but are also increasingly being used to set prices and terms for mortgages and other forms of consumer credit. In certain cases, even very small differences in scores can result in higher interest rates and less favorable loan terms. Credit ratings are also used to determine the cost of private mortgage insurance, which protects the lender from loss and is usually required on mortgages with down payments of less than 20 percent. Lenders also review credit ratings to evaluate existing credit accounts and use the information when deciding whether to change a customer's credit limits, interest rates, or other terms on credit accounts.

In addition to lenders, landlords and employers may review credit scores. Landlords may do so to determine if potential tenants are likely to pay their rent on time. Employers may review this information during the hiring process, especially for positions in which employees are responsible for handling large sums of money. Utility, **home telephone**, and **cellular telephone** service providers also may request a credit score to decide whether or not to offer service to consumer applicants.

Less traditional uses for credit reports and credit ratings are becoming increasingly common. Probate judges review credit scores before determining whether an individual should be named as executor of a deceased's estate, and airlines use credit histories as part of passenger screening for potential terrorist risks. Insurance companies use credit ratings when underwriting consumer applications for new insurance and renewals of existing policies. Credit information has been used as a basis to raise premiums, deny coverage for new customers, and deny renewals of existing customers.

The expanded use of automated credit scoring has brought changes to the marketplace that have benefited consumers. The growth in the use of credit scores has dramatically increased the speed at which credit decisions can be made. Especially for consumers with relatively good credit, approvals for loans can be given in a fraction of the time previously required, without manual review of the information.

Credit scores also increase the potential for customized pricing of credit based on the risk an individual poses. Charging more to consumers considered higher risk can remove some of the cost of risk carried by the general consumer population, and can allow for price reductions among consumers who pose less risk. Some have also argued that reliance on automated credit ratings can reduce discrimination because the automation of decisionmaking removes or reduces the influence of subjective bias that can occur when consumer applications are reviewed by an individual with decisionmaking authority.

Critics of credit scoring maintain that savings often are not passed on to consumers who pose less risk, and scoring systems simply allow lenders to earn greater profits from consumers who do not have high credit scores. In addition, the increased speed at which underwriting decisions can be made has created pressure



to approve credit applications more quickly. Some contend that the combination of this increased pace and the increased ability to customize the price charged based on credit ratings allows lenders to approve a larger share of consumers for loans, but not necessarily at the best rates for which some consumers would qualify if a more personalized approach were taken. Moreover, consumers who do not have a solid understanding of credit scores are more likely to be charged unnecessarily high rates if the scores are based on erroneous or incomplete data, and the consumer is not familiar enough with the system to correct the problem.

Critics have also argued that the factors used to determine a credit score may only mask, and not remove, bias from approval and pricing decisions. Lenders are still free to offer different levels of assistance in dealing with errors in credit records or with other issues related to credit scores, such as providing rescoring services to selected customers in an effort to offer better terms. Such discretionary assistance remains a potential source of bias in the approval process, no matter whether a consumer is evaluated using an automated credit rating or a manual system.

There is ample evidence that credit scores have statistical validity and are predictive of credit risk and repayment behavior for large populations. This does not mean that credit ratings are error free in individual cases, or that credit scoring models are always predictors of individual creditworthiness; it only means that they work reasonably well on average. Thus, while the use of credit ratings can yield predictable results in the aggregate for a large insurer or issuer of credit, it can impose hardship on an individual consumer who might be a good risk but happens to have a low score.

While debate surrounding the implications of credit scoring continues, its use is strongly established in the American financial services industry. Concern over the statistical validity of credit scoring focuses on two dimensions: the fairness of the models that interpret the data and the accuracy of the underlying credit data held in the databases of the major credit bureaus. Because the rating formulas that transform the vast amount of data in an individual's credit history into a precise number are not publicly available, evaluating the fairness and accuracy of the models continues to be problematic.

Credit scores of individuals depend on the information found in their credit histories. The system for creating consumer credit histories involves a large number of participants who fall generally into one of four categories: consumers, data repositories or credit bureaus, data users, and data furnishers. Approximately 200 million consumers have credit reports maintained by the three major credit bureaus (Equifax, Experian, and TransUnion), which are privately run businesses that collect, organize, and sell consumer information. The three major credit bureaus all contain similar sets of data about consumers, but the information in each bureau's report on an individual is not identical. Data users request credit reports from the credit bureaus. Data users include lenders, insurers, landlords, utility companies, employers, and other entities that are interested in assessing the risk of entering into a transaction with a consumer. Users review the credit information in credit reports to make decisions about extending credit, offering and pricing insurance policies, providing utility services, renting apartments and houses, offering employment, and for other purposes allowed by law. Some data users are also data furnishers, who regularly report information about consumers' accounts to the

credit bureaus, who then add the information to consumers' credit histories and organize it in a form that businesses can use. Furnishers of information may send data (e.g., account payment activity) to some or all three of the major credit bureaus.

There is no requirement that any business report information to any credit bureau, but most businesses that regularly use reports also feed information to at least one of the major credit bureaus. In a typical transaction in which a consumer applies for credit, such as a credit card, unsecured line of credit, or installment loan (e.g., for an automobile or furniture), the potential creditor can request a credit report from one, two, or all three of the credit bureaus. A credit bureau that receives such a request will send the credit report to the potential creditor and record an entry on the consumer's credit report that the report was sent. The creditor can use the information in the credit report (including the credit score) to help decide whether to extend or deny credit to the consumer, and what the interest rate and other fees will be for the extension of credit. If the creditor accepts the application, the creditor may then act as a data provider and report information on the consumer's payment history to one, two, or all three of the credit bureaus for as long as the account remains active. Payments made on time will be reported as such, as will payments that are 30, 60, or 90 days late.

Information in a consumer's credit report usually includes identifying data such as the consumer's name, **Social Security number**, date of birth, former names or aliases, current and former addresses, employment history, income, and the consumer's employment address. Reports also include **public record** information (e.g., judgments, tax liens, and bankruptcies), collections and payment history on credit accounts, balances outstanding on consumer debts, creditor and bank names along with account numbers, highest amounts owed, size and frequency of payments, any amounts past due, date of delinquencies, dollar amount of maximum delinquencies, and a list of companies that have requested the consumer's credit report in recent months. In addition, the **Fair Credit Reporting Act** requires credit bureaus to include any consumer statement or explanation of a dispute concerning the accuracy or completeness of information contained in the credit history. State and local governments may also report directly to credit bureaus if consumers fail to pay child support, have unpaid parking tickets, or have been overpaid for unemployment benefits.

Credit ratings are compiled from the totality of information contained in the credit report. Private firms provide analytic services to the major credit bureaus through the development of complex formulae that help interpret the information in the bureaus' files. These companies, the most popular of which is the Fair Isaac Corporation, produce the tools that use the information in a consumer's file to generate credit scores based on various risk factors. The rating compiled by Fair Isaac is known as a FICO score. Some large lenders and mortgage insurance companies have created their own tools that help them create scores and interpret credit information for applications involving large extensions of credit.

Generally speaking, account information can have either a positive or negative effect on a consumer's credit rating. On-time payments have a positive influence while late payments have a negative influence. However, the amount of positive influence a consumer receives from a timely payment may vary based on the type



of creditor being paid. For example, timely payments to a prime credit card lender may have a greater positive influence on a score than timely payments to a lender considered less favorable, such as a furniture or consumer electronics store. Other factors that can affect a score include the length of time credit has been established, the amount of credit used compared to the amount of credit available, and the length of time a consumer has resided at the current address.

Information obtained from public records and government entities, such as bankruptcy filings, delinquent child or family support payments, unpaid parking tickets, or overpayments of unemployment benefits, is often derogatory information that has a negative influence on credit scores, but public records may also include positive information such as the satisfaction of a bankruptcy or the payment of a judgment lien.

Any type of activity involving bad debts referred to a collection agency will have a negative impact on a credit history, regardless of how the debt was created. Collections will continue to have a negative impact after they have been paid or otherwise satisfied, although they will have a less negative impact once they are satisfied and some time passes. Under federal law, credit scoring cannot consider a consumer's race, color, religion, national origin, sex, marital status, receipt of public assistance, or the consumer's exercise of rights under consumer credit laws.

Until recently, a credit bureau did not have to disclose consumer credit scores upon a consumer's request. Congress amended the Fair Credit Reporting Act to require credit bureaus to disclose the current credit score or the most recent score that the bureau had calculated, a statement indicating that the number and scoring model may be different than the number or model used by other bureaus or any particular lender, the range of credit scores for the model used, the most important factors that adversely affected the score of the consumer who inquired, and the name of the analytical service company that the bureau used to compile the credit score. Although a consumer is entitled to one free credit report from each of the three major credit bureaus each year, the bureaus can charge a separate fee for releasing the consumer's credit score that was derived from information in the report.

In addition to requesting a credit score from one of the major credit bureaus, consumers can directly contact the Fair Isaac Corporation, the analytical service company that the credit bureaus most often use to create the score. For a fee, the company will release the score that it derives from data in each of the three major credit bureaus and a combined score using information from all three of the files.

If consumers want to raise their credit scores, credit scoring companies suggest several basic strategies. Consumers should pay bills on time, get current on any overdue accounts, keep balances low on credit cards, pay down debt rather than move it from one credit account to another, and not open a lot of new accounts in a short period of time. Various businesses and authors have studied the credit scoring system and recommend additional strategies to increase scores. However, because the formulae for creating credit scores is not publicly known, it is not always clear that any particular action (such as closing a seldom-used credit card account) will raise or lower a consumer's credit rating.

See also: **Bank Secrecy Act; Banking and financial records; Landlord and tenant; Personally identifiable information**

Suggested Reading: Cate, Fred H. “Privacy, Consumer Credit, and the Regulation of Personal Information.” In Thomas A. Durkin and Michael E. Staten (eds.), *The Impact of Public Policy on Consumer Credit*, pp. 229–276. Boston: Kluwer Academic Publishers, 2002; Cate, Fred H., Robert E. Liton, Michael Staten, and Peter J. Wallison. *Financial Privacy, Consumer Prosperity, and the Public Good*. Washington, DC: Brookings Institute, 2003; Electronic Privacy Information Center. *Right to Financial Privacy Act*. <http://www.epic.org/privacy/rfpa/>. Online, March 2006; Evans, David S., and Richard Schmalensee. *Playing with Plastic: The Digital Revolution in Buying and Borrowing*. Cambridge, MA: MIT Press, 1999; Fair Isaac Corporation. *FICO Credit Scores, Online Credit Reports, and Identity Theft Protection*. www.myfico.com. Online, March 2006; Fischer, Richard L. *The Law of Financial Privacy*. Washington, DC: A.S. Pratt & Sons, 2002; Hendricks, Evan. *Credit Score and Credit Risk*, 2nd ed. Washington, DC: Privacy Times, 2005; Manning, Robert D. *Credit Card Nation: The Consequences of America’s Addiction to Credit*. New York: Basic Books, 2000; Rodriguez, Anthony, Carolyn L. Carter, Willard P. Ogburn, and Joanne S. Faulkner. *Fair Credit Reporting*, 5th ed. Boston: National Consumer Law Center, 2002 (2005 Supp.); Scousen, Mark. *The Complete Guide to Financial Privacy*, 4th ed. New York: Simon & Schuster, 1983; Weston, Liz Pulliam. *Your Credit Score: How to Fix, Improve, and Protect the 3-Digit Number that Shapes Your Financial Future*. Englewood Cliffs, NJ: Prentice Hall, 2004.

James P. Nehf

Criminal suspects and arrestees

Privacy rights of individuals arrested for crime or suspected of it are established and protected by constitutional provisions, statutes, and judicial decisions at both the federal and state levels. At least two distinct privacy interests are identifiable in these protections. The first is an interest in limiting access by the government to the **homes**, belongings, and conversations of criminal suspects and arrestees, as well as information about their activities and other personal matters. This interest is protected by laws that limit the government’s ability to obtain information about people generally. The second is an interest in limiting **disclosure** by the government of information about arrestees and suspects that is in its possession—specifically, the very information that a given individual has been arrested for or suspected of crime. This interest is protected by laws that limit the government’s ability to release such information to the public.

Government access to information about individuals is limited according to several rationales. One is that people should be able to conduct their lawful affairs in private from the government—speaking their minds to **family** and friends, reading whatever books and magazines they wish to read, enjoying their hobbies, engaging in intimate behavior—and that the government should be allowed to invade that privacy only when, and only to the extent that, sufficient justification exists. Underlying this rationale is the commitment to robust democracy; the concern is that ideas and voices that might differ with those of the government would be discouraged or silenced if the government had unfettered access to information about people’s daily activities, reading materials, personal relationships and gatherings, group memberships, and the like. Another rationale is that personal information might be embarrassing or simply too revealing to allow unfettered government access to it—for instance, information



about one's habits, health, or finances. A third rationale is that certain means of obtaining information about individuals, such as inspecting a person's bodily cavities or drawing blood for chemical analysis, intrude sufficiently on personal dignity and bodily integrity to require strict regulation.

The primary source of laws that limit government access to personal information on these grounds is the Fourth Amendment to the U.S. Constitution. That amendment protects individuals, their homes, their papers, and their possessions against "unreasonable searches and seizures" by the government, and requires that warrants for arrest or search be supported by "probable cause" and particularly describe who or what is to be searched or seized. The U.S. Supreme Court has interpreted the amendment to mean that government actors ordinarily must obtain judicial warrants before conducting searches or seizures.

The Court has declared that the "search" language of the amendment specifically protects personal privacy. Indeed, the Court has defined a search, for purposes of determining whether the amendment applies, as any government action that implicates an individual's "**reasonable expectation of privacy**." And the Court has defined the standard the amendment sets out for issuing warrants: probable cause as a "fair probability" of crime, or facts and circumstances that create a "reasonable belief" in criminal activity. Thus, every government search of a person, a home, or personal belongings by a police officer or other government agent—every government action that implicates an individual's reasonable expectation of privacy—ordinarily requires a **search warrant**, issued by a judge or magistrate and based on a finding by that judicial officer that there is a fair probability that the targeted individual is guilty of a crime or the area to be searched contains evidence of a crime. But the Court has created many exceptions to that requirement, several of which see more practice than the presumptive warrant requirement.

The Court has deemed a wide variety of government investigative activity to be searches under the "reasonable expectation of privacy" definition and thus subject to Fourth Amendment scrutiny. **Wiretapping** or other **surveillance** of a person's conversations or correspondence, for instance, is a search that requires a warrant. Physically searching a person for evidence of crime also ordinarily requires a warrant—but there are two major exceptions. The first is when a person is arrested upon a police officer's own determination of probable cause, in which case the officer may thoroughly search the person and the area immediately around the person—the "grab area"—for weapons and evidence of crime. Such a search, called a search incident to arrest, can include all containers within the arrestee's grab area. The second exception to the requirement of a warrant for physical searches is when a police officer does not arrest but only detains a person for brief questioning, which is allowed upon a lower degree of suspicion of criminal activity called "reasonable suspicion." As long as the officer also has reasonable suspicion that the person may have a weapon, a less intrusive search, called a protective search or "pat down," is permitted to ensure the officer's safety.

Searches of cars and other movable vehicles are governed by similar rules. A police officer's own determination of probable cause allows an immediate and thorough search of all areas of a car in which evidence of the suspected crime might be, including the trunk and all containers within the car. When arresting a driver or passenger of an **automobile**, an officer is permitted to search the interior

of the car, including the glove compartment, for weapons or evidence of crime. Short of an arrest, the interior of a car can also be searched just for weapons—for instance, when a police officer detains a person for a traffic stop or brief questioning—upon the lower degree of suspicion called reasonable suspicion, as long as the officer has that degree of suspicion that the person may have a weapon in the car.

Homes are protected more strictly by the Fourth Amendment; the Supreme Court has stated repeatedly that the home is at the core of the amendment's protection. With only one exception, police officers may not search or even enter a private home without a warrant, even to arrest someone for whom they have determined probable cause of criminal activity. The exception is the case of "exigent circumstances," which means not only probable cause of crime but also the additional reasonable belief that immediate entry is necessary for one or more of three purposes: to protect others from harm, to prevent the destruction of evidence, or to catch a fleeing suspect. And even with a warrant permitting them to enter a home to search or arrest, police officers are generally expected, and in many states required by state law, not to enter until they have announced their presence and given the occupant at least a brief opportunity to open the door. However, in the recent case of *Hudson v. Michigan*, the Court found that evidence seized even when this rule is violated may be admissible in court.

Police officers are also forbidden to acquire information about activities within a home by means other than physically entering it if they do not have a warrant. In the Supreme Court's most recent statement on the matter, the case of *United States v. Kyllo*, 533 U.S. 27 (2001), the Court forbade the warrantless use of a "thermal sensor" or imaging device used from outside a home to detect excessive heat emanating from the home caused by high-intensity lamps used for growing marijuana. Use of the device constituted a search of the home for purposes of the Fourth Amendment, the Court said, because it revealed information about the interior of the home that would not otherwise be available without physically entering it. Because thermal-imaging devices were not yet "in general public use," the Court said, using them in that manner implicated an individual's reasonable expectation of privacy and therefore required a warrant.

After a person is arrested and taken into custody, privacy protection under the Fourth Amendment continues, most pertinently with respect to searches that involve bodily inspections and intrusions. Taking a blood sample from an arrestee to test it for alcohol content, for instance, ordinarily requires a warrant or court order. But in the 1966 case that remains the leading precedent on the matter, *Schmerber v. California*, 384 U.S. 166 (1966), the Supreme Court approved of the warrantless extraction of blood from a hospitalized arrestee when the police had probable cause that incriminating evidence would be found—namely, evidence that the arrestee had been driving while intoxicated, which caused the accident that put him in the hospital—and the additional reasonable belief that the evidence would otherwise be lost. In other words, there were "exigent circumstances." And although the Supreme Court has not ruled on these specific issues, opinions of lower courts indicate that the same rules govern other very invasive searches, such as performing surgery to retrieve a bullet or conducting body cavity searches for drugs or other items, while lesser physical intrusions, such as taking an arrestee's fingerprints, a sample for urine analysis, dental impressions, or a chemical swab



of part of an arrestee's body, are permissible upon no more than a police officer's determination of probable cause that incriminating evidence will be found.

For any search to be lawful under the Fourth Amendment, it must also be undertaken reasonably. This means that the search may not extend beyond the area reasonably likely to contain the evidence sought, nor may it be conducted with excessive force or otherwise executed in a manner that is not reasonably justified by the circumstances of the search and the purpose of it. For instance, while lawfully searching a home for a stolen television set, officers ordinarily may not open bedroom drawers; if given consent by a person—another exception to the warrant requirement—to search certain belongings, officers may not search beyond those belongings.

The constitutions of all 50 U.S. states contain provisions that are analogous to the Fourth Amendment. In some instances, these provisions are interpreted to offer greater privacy protection than that offered by the Fourth Amendment. New Jersey's highest court, for instance, has interpreted the corresponding provision in its state constitution to require exigent circumstances in addition to probable cause before an automobile may be searched without a warrant. And, while the boundaries of privacy protection under the Fourth Amendment and its state counterparts are ultimately determined by court decisions, many of the protections are also codified in federal and state statutes.

These boundaries are constantly being tested and redrawn. In recent years, some states have enacted laws that require law enforcement officers to obtain **DNA** samples of all individuals arrested for certain offenses (typically violent ones) whether or not the officers have probable cause that incriminating evidence will be found. Whether taking these samples—typically of saliva or skin—pursuant to these laws is lawful under the Fourth Amendment, indeed whether it is even a “search” for Fourth Amendment purposes, will likely be for the courts to determine.

Laws that limit the government's disclosure of information about arrestees and suspects—in particular, the very information that an individual was ever arrested for crime or suspected of it—take a variety of forms and address several means by which that information might reach the public. In each case, protecting the privacy of arrestees and suspects, especially those who were never formally charged with or convicted of an offense, is the primary rationale. The privacy interest these laws protect is defined in many ways—for instance, an individual's right to “control” personal information, deriving from a basic “**right to be let alone**” by others, and allowing one to “define oneself.” Its rationale with respect to arrestees and suspects is the significant harm that can befall one who is publicly identified as an accused or suspected criminal: social status can be damaged, family members shunned, employment lost, or future job prospects threatened.

This interest is not one that is seen as protected by the U.S. Constitution. In the 1976 case of *Paul v. Davis*, the Supreme Court rejected the claim that the public identification of an arrestee by a government actor before trial violates the arrestee's constitutional right to due process. (In that case, local police had included an arrestee's name on a list of “active shoplifters” they had distributed to area merchants. The individual had been arrested for shoplifting but not yet convicted of the charge; the charge was eventually dismissed.) In fact, the First Amendment to the Constitution stands in opposition to such a privacy right. According to a series of Supreme Court decisions, the free-speech guarantee of that

amendment creates a general right of public access to criminal proceedings, so that citizens can be informed enough about government affairs to exercise their speech rights intelligently; and both the free-speech and the free-press guarantees of the amendment allow the media and other private parties to publicize truthful information—such as the fact of an individual’s arrest or status as a criminal suspect—at least when that information has been acquired lawfully. Nevertheless, legislatures and courts have allowed or required government actors to withhold information about arrestees and suspects on privacy grounds in certain contexts, and the Supreme Court has considered and approved of a number of these restrictions.

Regarding suspects, government disclosure of the fact that an individual is or has been suspected of a crime is forbidden on privacy grounds in several ways. Grand jury proceedings, for instance, in which citizens hear evidence to decide whether or not to indict a given individual (i.e., whether or not there is probable cause of guilt), have long been closed to the public by statute or court rule in the federal system and the states. One rationale for this **secrecy** is to protect individuals whom the grand jury ultimately does not indict from public knowledge of the fact that they were under suspicion. The Supreme Court has repeatedly approved of both grand jury secrecy and the privacy rationale for it.

Indictments themselves are typically public documents; however, they might contain the names of individuals other than the charged defendant who are suspected of participating in the crime even though the indictment does not formally charge them. Accordingly, courts often order the redaction of these names in order to protect the reputations of these individuals, and the American Bar Association has formally adopted a principle forbidding naming such “unindicted co-conspirators” in indictments. Courts have extended similar protections to other documents in criminal cases that might be accessed by the public—pre-indictment search warrants, transcripts of wiretapped conversations, bills of particulars (detailed statements by prosecutors that give defendants additional information about the charges against them), pre-sentence reports—and in each case they have done so expressly to protect the privacy of individuals who are identified in the documents as criminal suspects but who have not been convicted or formally charged.

Information that identifies suspects in other government documents is also protected from disclosure on privacy grounds under statutes that otherwise confer broad rights of public access to government information. The federal **Freedom of Information Act** (FOIA), for instance, which requires government agencies to disclose agency information to the public upon request, exempts several categories of information from that requirement; one category is information the disclosure of which would or could constitute “an unwarranted invasion of personal privacy.” Several federal court decisions have interpreted this language to allow government agencies to redact information that identifies past or present criminal suspects before releasing documents that are subject to disclosure. Some state courts have interpreted analogous language in their state disclosure statutes similarly.

Information that identifies actual arrestees can also be withheld. At least one federal court has recently ruled that the personal privacy exemption of the federal FOIA applies to that information. The U.S. Department of Justice (DOJ) also argued that the exemption supported its decision to withhold the names of hundreds of individuals its agents had arrested and charged with immigration violations after the attacks



of September 11, 2001. A federal appeals court upheld the DOJ's withholding of the names on other grounds, issuing no ruling on the privacy argument. More broadly, while information about arrests that have taken place on a given day, including the names of the arrestees, is generally publicly available in every state (typically at the pertinent police station), the compilation of this information with respect to a particular individual—in other words, a person's arrest record or “rap sheet”—is not. According to the laws of most states, government actors are forbidden to disclose an individual's full arrest record to any person or entity other than another government agency except in strictly limited circumstances, such as for statistical research. Instead, states typically draw a distinction between records of arrests that have resulted in convictions and records of those that have not, permitting public disclosure of the former but not the latter. Nonconviction arrest records can also be sealed or expunged by law in a number of states. The U.S. Supreme Court approved of withholding arrest records on privacy grounds in the 1989 case of *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, in which the Court upheld a **Federal Bureau of Investigation (FBI)** refusal to disclose a person's rap sheet under the personal privacy exemption. Notably, the Court did not distinguish between arrests that resulted in convictions and those that did not.

Information that identifies juveniles who are suspected, accused, or even convicted of crime is also confidential in most states, and the Supreme Court has repeatedly endorsed this practice. Although the interest in juvenile **confidentiality** is not always or solely characterized as a privacy interest, its primary rationale—to protect juvenile offenders from negative attention that would stigmatize them, hindering their rehabilitation and their reintegration with society—is a quintessential privacy interest.

See also: **Constitutional protections**

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Dressler, Joshua, and Alan C. Michaels. *Understanding Criminal Procedure: Volume One, Investigation*, 4th ed. New York: Matthew Bender, 2006; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 4th ed., 6 vols. Egan, MN: Thomson/West, 2004; LaFave, Wayne R., Jerold H. Israel, and Nancy J. King. *Criminal Procedure*, 4th ed. St. Paul, MN: Thomson/West, 2004; Reza, Sadiq. “Privacy and the Criminal Arrestee or Suspect: In Search of a Right, in Need of a Rule,” *Maryland Law Review* 64 (2005): 755–874.

Sadiq Reza

Cruzan v. Director, Missouri Dep't of Health, 497 U.S. 261 (1990)

Nancy Cruzan established the federal constitutional right of every American to refuse unwanted medical treatment in the landmark 1990 U.S. Supreme Court case, *Cruzan v. Director, Missouri Dep't of Health*. Cruzan was in a single-car accident on a deserted country road in the early-morning hours of January 11, 1983. Her car crossed the centerline, went down a ditch, flattened several saplings and a rural

mailbox, and flipped onto its top. She was thrown from the car and landed 35 feet beyond where the car stopped. The car traveled nearly the length of two football fields from the point where it left the road until it stopped. It took some time for neighbors down the road to wake up, come outside, and rush back in to call for help, and still longer for emergency vehicles to make their way to the remote rural site. A review of police, ambulance, and fire reports suggests that Cruzan may have gone as long as 30 minutes without oxygen before emergency workers revived her that night.

For the week after the accident she remained in a full, closed-eye coma. Then, on day seven, her eyes opened, a point of brief (but false) hope for her **family**, and she moved into a kind of open-eyed unconsciousness. Extensive efforts at rehabilitation did nothing. Eventually—and quite predictably in hindsight, given the long period of time without oxygen—Nancy Cruzan lapsed into the kind of eyes-open unconsciousness that doctors described to the family as a persistent vegetative state. Some portion of her brainstem—that part of the human brain that controls basic, primitive human reflexes—had survived the accident. The brainstem can go significantly longer periods of time without oxygen and survive than the upper, thinking part of the brain, which is much more fragile. The persistent vegetative state was so named in 1972 by Drs. Fred Plum and Bryan Jennett in the prestigious medical journal *Lancet*. This condition came about as a result of increasingly sophisticated life-saving techniques at accident sites and better-equipped emergency rooms. As a result, patients who previously would have died were able to be brought back from the brink of death, but not all of the way back. In the early 1970s, doctors were seeing more and more patients in this condition, necessitating a diagnosis and a name. Nancy Cruzan slept and woke; she breathed on her own; she could slightly move her badly paralyzed limbs; her eyes moved around the room and at times would appear to fix on a person or object; she would startle in reaction to loud noises; and she would sometimes appear to grimace or smile. But in the four years after the accident, her family never saw any reaction that they considered conscious thought—that they thought was Nancy. Her doctors agreed. They told the Cruzans that Nancy was permanently unconscious, without hope of ever regaining consciousness, and that she could live another 30 years in that condition with attentive nursing care and continued use of the main medical technologies keeping her alive, which were artificial nutrition and hydration, or a feeding tube.

The family came to the conclusion that if Nancy could speak to them, given her condition, she would ask to have the feeding tube removed. The director of the state hospital told the family that the hospital would not remove the feeding tube without a court order. A judge told them that they could be charged with murder if they moved Nancy home to remove the feeding tube without a court order. So they decided to go to court. In March 1988, the Cruzans found themselves on trial in southern Missouri against the attorney general of Missouri and the state Department of Health. At the end of that trial, the trial judge ruled in the family's favor. On appeal, the Missouri Supreme Court overturned this decision, setting up a showdown in the nation's highest court.

In the summer of 1989, the U.S. Supreme Court agreed to hear the *Cruzan* case and set the argument date for December 6, 1989, for its first **right-to-die** case. Throughout that fall, on television and radio, in barbershops, on golf courses, in



churches, and at medical schools, the public was talking about the case. What was this new “persistent vegetative state” condition that television commentators were calling by its acronym, PVS? What exactly was a feeding tube? Who should decide? Many commentators suggested that the raising of public awareness about these complex questions was in many ways more important than the legal battle itself. On June 25, 1990, the Supreme Court issued its decision. The final vote of the justices split 5-4, and five of the nine justices wrote their own separate opinions on what they thought the law was: the end result was the majority opinion, two concurring opinions, and two dissents. As sometimes happens with complicated Supreme Court opinions, the interest groups on both sides found something to claim as victory within those five opinions.

Chief Justice William Rehnquist, who wrote the majority opinion, reasoned that competent people have a federal constitutional right, a liberty right, to refuse medical treatment. The Court had never before directly recognized such a right. A majority of the justices also recognized that tube feeding was medical treatment, like a respirator or dialysis or any other device that takes the place of a natural function that has been lost. On the other hand, the majority opinion ruled that the federal Constitution did not require Missouri to defer to the parents of an adult like Nancy Cruzan (she was 25 years old at the time of the accident) to make the decision to remove medical treatment. If Missouri chose to rely solely on evidence of Nancy Cruzan’s own wishes, the Court noted that the state could impose such a standard without running afoul of Nancy’s constitutional rights. The Court also stated that leaving the life support in place in one way simply preserved the status quo, with advances in medicine, or possibly “the discovery of new evidence regarding the patient’s intent” creating at least “the potential that a wrong decision will eventually be corrected or its impact mitigated.”

The Cruzans took this language and went back to court in Missouri for a new trial in November of 1990. Three friends of Nancy Cruzan had telephoned her parents when they saw the story in the news over the previous year. These friends told the Cruzans about conversations they’d had with Nancy about living on life support. This time the attorney general and the Department of Health chose not to oppose the family, or even to participate in the trial. On December 14, 1990, just shy of eight years after her accident, the trial court again ruled in favor of Nancy Cruzan’s parents. Doctors at the state hospital removed her feeding tube immediately, and the hospital transferred Nancy to their hospice wing that afternoon.

Over the course of the next 11 and a half days, the nation watched the final chapter of the Cruzan saga unfold in the remote, hilly southern Missouri town of Mt. Vernon. Protesters from around the country arrived and satellite television trucks were not far behind. Various groups filed emergency appeals in the state and federal courts over those 11 days, seven appeals in all; signs popped up on the lawn like “Missouri Euthanasia Center” and “Atrosity [sic] Torture Murder.” On the day before Christmas, a big new sign appeared that read “Nancy’s Gift at Christmas from her Parents and Doctor—DEATH!” Inside the hospital, the family huddled together, day after day, talking softly, holding Nancy’s hands, and praying. At 2:47 a.m. on December 26, 1990, Nancy Cruzan’s breathing stopped, and she died.

In the wake of the *Cruzan* case, many states passed laws seeking to address the issues raised by the case. Congress passed a law called the Patient Self-Determination

Act, which provides that all patients entering hospitals in the United States must be counseled about living wills and other types of health care planning. The *New York Times* wrote that Nancy's case had helped "free countless Americans of some of the fears attending death."

See also: **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**; *Washington et al. v. Glucksberg et al.*, 521 U.S. 702 (1997)

Suggested Reading: Caring Connections. <http://www.caringinfo.org>. Online, December 2005; Colby, William. *Long Goodbye: The Deaths of Nancy Cruzan*. Carlsbad, CA: Hay House, 2002; Colby, William. *Unplugged: Reclaiming Our Right to Die in America*. New York: AMACOM Books, 2006; Webb, Marilyn. *The Good Death: The American Search to Reshape the End of Life*. New York: Bantam Books, 1997.

William H. Colby

Cryptography

Whether it be cuneiform inscribed on clay tablets, histories on papyrus, agricultural transactions on quipu, or philosophical tomes on paper, writing is fundamental to human civilization. Writing is about communication, but sometimes the communication needs to be secret. That is the role played by cryptography, the science of secret (*crypto*) writing (*graphy*). In almost every civilization, cryptography appeared shortly after writing. Only the Chinese empire, where written language was confined to a small elite and ideographic writing made the process of encryption difficult, seems to have made scant effort to develop encryption methods.

Until the modern era, if two people wanted to communicate privately, they moved to a private space, a field, or a room where they could not be overheard. The invention of electronic communications—first the telegraph, then the telephone, and more recently the **Internet**—changed the pace and extent of communications, as well as the need for **confidentiality**. And so cryptography, once the domain of the military, diplomats, lovers, and young children, is now a tool of the public. Every time an individual purchases an item online via a secure website, every time an employee logs onto the company's internet via a virtual private network, every time an individual downloads a song to an iPod, someone is using cryptography. Modern digital communications systems operate on strings of numbers: 0s and 1s. The first step in encryption is to convert the alphabetic system into bits. Like much in cryptography, this idea is not new. In the second century B.C., the Greek historian Polybius proposed a method for encoding letters as numbers. Applying his method to the Roman alphabet, the letters could be written in a 5×5 grid (with *i* and *j* combined in a single element) and each letter then labeled by its grid entry; for example, *d* is (1,4) while *f* is (2,1). Once the message has been transformed into bits, the unencrypted string, or plaintext, is encrypted into the ciphertext by the cryptosystem.

Fundamentally there are two types of cryptographic transformations: substitution and transposition. In 1500 B.C., a Mesopotamian scribe employed substitution. Using cuneiform symbols with multiple syllabic interpretations in their least common mode, the scribe hid a formula for ceramic glaze. Transposition ciphers take the letters of a message and shift them around within the message according to a predetermined technique. For example, a transposition cipher might take the grid



proposed by Polybius and write the text into a square by rows in one order and read it off by columns in a different order.

There are two aspects to an encryption system: the method for the encryption system, called the algorithm, and a secret, called the key. The key is specific to the pair—or group—of people who want to communicate privately. This methodology was codified by the nineteenth-century cryptographer Auguste Kerchoffs, who observed that any cryptosystem used by a large group of people will leak information about how the system works. The system must be secure even if the algorithm is public, so the **secrecy** of the system must lie entirely in the key (which is shared with a much smaller group of people). Opening the algorithm to public scrutiny helps establish confidence in the algorithm's security and thus enables the algorithm's acceptance.

As is well known to printers (and Scrabble players), in any language, letters have a particular frequency distribution. For example, in English text, the letter *e* appears about 13 percent of the time, and the letter *t* appears about 9 percent of the time. There is also a frequency distribution of pairs of letters, triples of letters, and so forth. In English, for example, the pair *th* is the most common pair, or digraph, while *er* is the second most common. Frequency distributions are a well-known tool for attacking substitution and transposition ciphers; the first description of frequency distribution appears in the Arabic encyclopedia, the *Subh al-a sha*, completed in 1412 A.D. Frequency analysis can also be used against polyalphabetic ciphers, cryptosystems that use more than one alphabet for a single encryption.

In cryptosystems the whole may be greater than the sum of its parts. The proper combination of substitution and transposition with a key can make for a very strong cryptosystem. That was the basis for the development of the U.S. Data Encryption Standard (DES), an algorithm with a 56-bit key that served as a U.S. cryptography standard from 1977 to 2005 and was widely used inside and outside the government. In a strong algorithm, each additional bit of key length increases the algorithm's security by a factor of 2. The increasing speed and dropping price of processors spelled the end of DES's security, and in recent years the algorithm was replaced by triple-DES, a cipher with apparent 112-bit security. The cryptosystems described thus far have all been symmetric-key systems, in which both the sender and the receiver use the same key for encryption and decryption. The difficulty of transmitting the key, especially between two parties who have not previously communicated (such as the initial time a consumer makes a purchase at an online store), led to the 1975 invention of asymmetric-key, or public-key, cryptography by Whitfield Diffie and Martin Hellman.

Public-key cryptography makes public both the algorithm and the public, or encryption, key; the decryption key, often referred to as the private key, is not published. The system's impenetrability is based on the apparent difficulty of certain mathematical functions, ones that are easy to compute and hard to invert. Multiplication and factoring appear to be one such pair. These provide the underpinnings for the RSA public-key cryptosystem, which provides the key exchange mechanism of the **Secure Socket Layer (SSL)** protocol. Because public-key computations are slower than symmetric-key systems, a public key is often

used for exchange of a symmetric key, after which the data are encrypted using a symmetric-key algorithm. A second generation of public-key cryptosystems based on the more complex arithmetic of elliptic curves is coming into use. These systems, employing a smaller key size for the same security level as RSA, are being implemented in low-power and small-memory devices.

Public-key cryptography makes possible **digital signatures**, which provide a guarantee of the authenticity of the sender. Cryptography actually serves four functions: confidentiality, the functionality that no one but the intended recipient can understand the communication; integrity, a guarantee that the message has not been modified or corrupted; **authentication** (of the sender); and nonrepudiation, evidence that prevents the sender from later denying the communication.

Communication has two aspects, the content and the transactional information: for example, the writing on the envelope and the enclosed letter indicate who the sender and receiver are, when the message was sent, how long it is, and the content of the message. Traffic analysis, the study of the transactional (i.e., envelope) information, has long been of great value to intelligence agencies. Even if the message itself cannot be decrypted, the transactional data reveal much about the target's organizational structure and intentions. Traffic analysis was used heavily during World War II, but until recently there has not been much effort or interest in the civilian world in developing ways to hide transactional information. Because the Internet enables real-time tracking of what information individuals are accessing, there is now a strong interest in developing systems to make transactional information anonymous, including what sites an Internet user is browsing. The various systems for anonymous re-mailing and anonymous browsing, including Anonymizer and Onion routing, are all based on public-key cryptography.

In 1975, when the U.S. government put forth a call for the public cryptosystem that became DES, the public cryptography community numbered just a handful of researchers, and most cryptography research was done by military agencies. A quarter of a century later, when it came time to replace DES, the community had gone public. DES's replacement, the Advanced Encryption Standard, adopted in 2002, was developed by Belgian researchers and was vetted by cryptographers around the world. This is one small measure of how cryptography has moved from the secretive military and government realm into the public world.

See also: **Anonymity; Authentication**

Suggested Reading: Dam, Kenneth, and Herbert Lin. *Cryptography's Role in Securing the Information Society*. Washington, DC: National Academy Press, 1996; Diffie, Whitfield, and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press, 1998; Kahn, David. *The Codebreakers: The Story of Secret Writing*. New York: Macmillan, 1967; Schneier, Bruce. *Applied Cryptography*. New York: John Wiley & Sons, 1996.

Susan Landau

Curtilage

Simply put, the curtilage is the area immediately outside one's **home**. Traditionally, the Fourth Amendment was interpreted to protect not only the interior of a home, the area inside the four walls, but to also protect the area immediately outside the home: the curtilage. The term has included garages, driveways, cottages,



and backyards for Fourth Amendment protections from unreasonable searches and seizures. The Supreme Court instructed in *California v. Ciraolo*, 476 U.S. 207 (1986), that “[t]he protection afforded the curtilage is essentially a protection of families and personal privacy in an area intimately linked to the home, both physically and psychologically, where privacy expectations are most heightened.”

The curtilage concept originated in common law to afford the area immediately surrounding a dwelling house the same protection from burglars as was afforded the house itself. The curtilage is the area to which the intimate activity associated with the “sanctity of a man’s home and the privacies of life” extends (*Boyd v. United States*, 116 U.S. 616 (1886)). Courts have extended Fourth Amendment protections to the curtilage. Further, they have defined the curtilage, as did common law, by reference to the factors that determine whether an individual reasonably may expect that the curtilage will remain private. The difficulty for the courts in addressing issues of privacy and protection from unreasonable searches has been in determining where the curtilage ends.

In *Hester v. United States*, 265 U.S. 57, 59 (1924), the Supreme Court ruled that that the Fourth Amendment’s protection did not extend to “open fields.” The Supreme Court reaffirmed that holding in *Oliver v. United States*, 466 U.S. 170 (1984), and ruled that the extent of the curtilage should be determined by factors that bear upon whether an individual reasonably could expect that the area in question should be treated as the home itself. The court instructed that the central component of any inquiry to determine if an area constituted curtilage should be an inquiry as whether the area harbors the “intimate activity associated with the ‘sanctity of a man’s home and the privacies of life.’”

In *United States v. Dunn*, 480 U.S. 294 (1987), the Supreme Court drew upon the history of its own cases, as well as the experience of the lower courts, to hold that curtilage questions should be resolved by considering four factors: (1) the proximity of the area claimed to be curtilage to the home; (2) whether the area was included within an enclosure surrounding the home; (3) the nature of the uses to which the area was put; and (4) the steps taken by the resident to protect the area from observation by people passing by. The court, however, warned “that combining these factors [does not produce] a finely tuned formula that, when mechanically applied, yields a ‘correct’ answer to all extent-of-curtilage questions. Rather, these factors are useful analytical tools only to the degree that, in any given case, they bear upon the centrally relevant consideration—whether the area in question is so intimately tied to the home itself that it should be placed under the home’s ‘umbrella’ of Fourth Amendment protection.” The difficulty in protecting privacy rights in areas traditionally viewed as curtilage is seen in a review of cases addressing the question.

The call was easy for the *Hester* Court to make. In that case, revenue agents witnessed what they believed was a moonshine sale and pursued suspects through a field where they found discarded whiskey bottles. Acknowledging that while there might have been a **trespass**, the Court held there was no illegal search or seizure. It relied upon British common law for the holding that the right to be secure in one’s home from unreasonable searches and seizures did not extend to open fields. But in the nearly 60 years between *Hester* and *Oliver*, the issue had become so muddled that the Supreme Court felt compelled to re-address the issue to resolve “the confusion the open fields doctrine has generated among the state and federal courts.”

The court in *Oliver* had no difficulty upholding the actions of state investigators who ignored no trespassing signs and entered into a field to seize a marijuana crop. In that case, two Kentucky state police officers drove onto a private farm to investigate a claim that the farm owner was growing the marijuana. They drove past the farmer's home and got out at a gate with that displayed a no-trespassing sign. They followed a path around the gate and walked for several hundred yards past a barn and a camper. Despite shouts from an unidentified person advising the officers to leave the property, the investigators continued on to find marijuana growing more than a mile from the landowner's home.

In ruling that *Oliver* had no expectation of privacy, and therefore, no Fourth Amendment protections from the warrantless search in his fields, the court held the rule of *Hester v. United States* may be understood as providing that an individual may not legitimately demand privacy for activities conducted out of doors in fields, except in the area immediately surrounding the home. This rule is true to the conception of the right to privacy embodied in the Fourth Amendment. The Amendment reflects the recognition of the Framers that certain enclaves should be free from arbitrary government interference. For example, the Court, since the enactment of the Fourth Amendment, has stressed the overriding respect for the sanctity of the home that has been embedded in our traditions since the origins of the Republic.

In contrast, open fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance. There is no societal interest in protecting the privacy of those activities, such as the cultivation of crops, that occur in open fields. Moreover, as a practical matter, these lands usually are accessible to the public and the police in ways that a home, an office, or commercial structure would not be. It is not generally true that fences or "No Trespassing" signs effectively bar the public from viewing open fields in rural areas.

The court likewise demolished any expectation of privacy for a homeowner with a 10-foot-high privacy fence in *California v. Ciraolo*. In that case, the yard immediately behind a home was within the curtilage, and a tall fence prohibited passersby from seeing what was growing in the yard. The Court even acknowledged the resident had "a subjective expectation of privacy." Nevertheless, the Court held that a search by an airplane flying over the yard was not a search entitled to Fourth Amendment protection. Since the inspection by air did not involve a physical invasion into the curtilage, there was no legitimate privacy right. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection," the Court ruled.

The idea that what can be seen from the air by anyone is not subject to Fourth Amendment protections was again upheld in *Florida v. Riley*, 488 U.S. 445 (1989). In that case, police used a helicopter to fly over a greenhouse to view through slats in the roof. Despite obvious efforts by the greenhouse owner to obscure the public's view, the Supreme Court approved the aerial search. In short, the Court held that even though the greenhouse was within the curtilage of Riley's home, Riley had no reasonable expectation of privacy since the interior of the greenhouse was visible from the air.

Garbage left in closed opaque plastic bags on the curb had been considered private under California law until the Supreme Court ruling in *California v. Greenwood*,



486 U.S. 35 (1988). In that case, police investigators searched through trash bags left for collection by the Greenwoods. Based on evidence of drug use found in the garbage, police obtained a **search warrant** for the Greenwood residence. Inside the home, police found various drugs, and the Greenwoods were prosecuted. The defendants claimed the search of their garbage constituted an illegal search and seizure under California law and the Fourth Amendment.

The *Greenwood* Court agreed that the couple may well have expected their privacy in the garbage to be protected and that the nature of their garbage bags would not become public. Nevertheless, the court held the expectation unreasonable. “It is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public. Moreover, respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents’ trash or permitted others, such as the police, to do so.” The court also dismissed the Greenwoods’ reliance on state law.

This review of cases shows that while the concept of privacy within curtilage technically survives, the courts have generally been unwilling to protect it.

See also: **Constitutional protections**

Suggested Reading: Black, Henry C. *Black’s Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Dash, Samuel. *The Intruders: Unreasonable Searches and Seizures from King John to John Ashcroft*. New Brunswick, NJ: Rutgers University Press, 2004; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000; Turkington, Richard C., and Anita L. Allen. *Privacy Law: Cases and Materials*. St. Paul, MN: West, 2002; Stephens, Otis H. (ed.). *Unreasonable Searches and Seizures: Rights and Liberties Under the Law*. Santa Barbara, CA: ABC–CLIO, 2005.

David J. Brown

D



Data brokers

Given the value of data about individuals, it is inevitable that someone will gather, organize, and sell such data. Data brokers' services vary to suit the needs of their clients. Marketers may want data that will help them reach their target audiences more efficiently. Employers, lenders, insurance vendors, and others may want a variety of information about a specific individual. A business may want detailed information about people in a specific area for use in making a location decision.

Data brokers may provide direct access to the data they collect by selling extracts from their data, or they may provide a more restricted service, such as selling profiles of one individual at a time. Their services may also include computing a score from a statistical model, such as a score indicating the likelihood of fraud in a credit application.

Data brokers collect their data from a variety of sources, including

- Credit-granting consortiums (banks, department stores, **credit card** issuers, etc.)
- Insurance or insurance applications
- Real estate transactions
- Tax records and property appraisals
- Product registrations
- Rebate forms
- Sweepstakes forms
- Store discount cards
- Telephone directories
- Billable telephone addresses
- Legal or criminal justice records
- Licensing (driver's and other)
- Vehicle registrations
- News organizations
- Post office deliverable address counts



Some types of information may voluntarily be made public by the individual; these might include personal websites and web logs (blogs). Other information may also be given voluntarily but without the realization that the information might be put to more generally use than the provider intended. Product registrations or a registry of disaster victims fall in this category. A great deal of information is gathered in the course of business transactions, some of which may be subject to legal privacy restrictions and some not. Credit transactions, credit card balances, credit limits, insurance applications, and purchases made with store discount cards are examples.

New data may be computed from existing data. Credit scores are computed from a variety of statistics on an individual. Some data brokers even use statistical modeling to calculate estimated data. A broker may, for example, calculate an average household income for block groups based on **United States Census** data along with data from magazine subscriptions, vehicle registrations, property appraisals, post office deliverable address counts, and estimates by local governments. That information could then be associated with an individual in connection with the individual's address.

Data brokers serve a variety of clients. These include law enforcement, landlords, employers, political parties, and stalkers. Data brokers exert varying degrees of control over the use of their data, sometimes as restricted by law. Some take subscriptions only from established businesses or government agencies, although such a policy has not proven to be a foolproof method of preventing misuse. Data collected by data brokers have potentially annoying applications, such as **spam**, and may be devoted to potentially illegal purposes, including **identity fraud** or denial of credit.

Another potential problem with data brokers is the accuracy of their data. Data may be entered incorrectly or data from the wrong person may be entered into a database. For some types of data, such as credit data, legal requirements give individuals the opportunity to suggest corrections to the data collected about them. Individuals generally have no say in how their personal facts are aggregated to generate a composite such as a credit score. Web search engines in a sense are data brokers. Employers may search web pages using an applicant's name and find matches to the wrong person. In addition, statistical models can produce false positives, an example of which is an account flagged as likely to be fraudulent but that is actually not.

Although there are laws that restrict the exchange of certain types of information, such as health insurance information, credit information, or student records, a great deal of information about individuals can be gathered and exchanged freely. Given the easy availability of personal data, credit approvals can be made quickly, appropriate medical treatment can be given, and consumers can hear about products they may want. All of these uses give the collection of personal data great value. Unfortunately, the profitability associated with many misuses makes the data an attractive target for theft when legal restrictions bar access.

The concern over security of collections of personal data extends to collections not made by commercial entities. The security of individual and business census data, law enforcement records, and national security data collections is a major privacy issue. For the latter collections the accuracy of the data is also a

major concern. If inaccurate information in the national security database prevents you from flying, or if an inaccurate entry in a law enforcement database makes you vulnerable to false arrest, how easily can you get that information corrected?

See also: **Credit rating; Public records**

Suggested Reading: Annual Credit Report. <http://www.annualcreditreport.com>. Online, September 2005; Electronic Privacy Information Center. <http://www.epic.org>. Online, September 2005; Leahy, Patrick. *Specter, Leahy Introduce Personal Data Privacy and Security Act of 2005*. <http://leahy.senate.gov/press/200506/062905a.html>. Online, September 2005; *Privacy.org: The Source for News, Information, and Action*. <http://www.privacy.org>. Online, September 2005.

Larry Hoyle

Data mining

Data mining can be defined as the use of statistical techniques to unearth previously undiscovered relationships from large volumes of data. The goal of data mining may be classification, such as trying to identify whether an individual belongs to a particular group, or it may be prediction, such as trying to identify those who will spend the most at a website.

A wide range of commercial, governmental, charitable, educational, and medical organizations make use of data mining applications. Objectives of data mining include

- *Security.* Based on the information known about an individual, is she likely to associate with terrorists? Should she be placed on the “no fly” list? Should she be targeted for additional investigation and surveillance?
- *Customer relations management.* How can the information in a firm’s database be used to identify products and services in order to increase a firm’s bottom line? Say someone just bought the new Harry Potter book online. How can that customer’s information be used to determine what other products he might be interested in?
- *Political and charitable fundraising.* What characteristics make it likely that someone will send a contribution in response to a fundraiser’s mailing?
- *Credit scoring.* Based on the individual’s credit history, would it be a good risk to give an applicant a 30-year mortgage?
- *Fraud detection.* What characteristics of an insurance claim make it likely to be a fraudulent one? Was it really the cardholder who bought concert tickets on his credit card, or was his card stolen?
- *Medical.* What group of patients is most likely to benefit from a new treatment? What cities are most at risk of a flu epidemic?

Data mining has exploded over the last decade due to several factors: First, the amount of information available about individuals and events has expanded rapidly. For example, many grocery stores use frequent-shopper cards to collect information on purchases by individual customers. Digital images collected by **surveillance** cameras, satellites, and other sources add to the diversity of data available to be mined. Additionally, **public records** such as property tax assessments that previously were on paper only are now commonly found online. Second, the organization of raw data

in databases and data warehouses makes the exploration of large data collections feasible. Third, the exponential growth that has occurred in computing power allows firms and governments to run complex algorithms on extremely large databases.

Data mining employs statistical algorithms to detect and explore patterns and relationships. In other words, given the data, data mining creates one or models. This differs from traditional statistical analysis, in which models or hypotheses come first and the researcher asks, “Do the data support my model?” Some of the statistical techniques used in data mining are regression, decision trees, and neural networks. With any of these techniques, one measure is chosen as a target variable. The target variable may have discrete outcomes, such as “made purchase” versus “did not make purchase” or “tax fraud” versus “no tax fraud.” Or it may have continuous outcomes, such as “amount of money spent.” Other measures or variables are chosen as predictors, such as income, past spending, or education. Data mining techniques then attempt to make the most accurate prediction of the target variable.

Regressions try to fit an equation to the available data. The equation has inputs and produces a predicted value. In traditional statistical analysis, the researcher pre-specifies which subset of possible inputs should be included in the equation. In a data mining approach, the researcher puts in all of the information at her disposal and lets the algorithm choose what information actually is important.

Decision tree analysis takes a different approach. This technique divides the data into successively smaller groups, using rules to determine which divisions are best. For example, a tree analysis might find that the most effective rule for predicting the amount spent on books is to divide customers into those who earn over \$100,000 and those who do not. The second split might be to divide the “under \$100,000” group into those who have a college degree versus those who do not.

A neural network is a mathematical model that in some sense simulates a collection of nerve cells (neurons). Each neuron has a set of inputs and one output. The outputs of neurons can connect to the inputs of other neurons. Each neuron “learns” by changing the way it combines input values in proportion to the difference between the actual and predicted values of the target variable.

Data miners usually divide their large datasets into several parts or “samples.” Possible relationships are “discovered” using multiple techniques on one sample of data. Another subset of the data is used to establish how well each technique predicts the target variable. Data miners compare alternative techniques to see which one works best on the new data subset. In some cases a regression model might predict best, and in other cases the neural network might be best. These models may also be applied to new samples of data. A financial institution might, for example, develop a model to classify pending **credit card** purchases as either fraudulent or valid. The model can be applied to new purchases as they happen and be used to authorize the purchase.

Data mining offers a number of social benefits. The techniques have been used to reveal and then rectify fraudulent Medicare claims. Several states now use data mining techniques to direct tax audits at those returns that are predicted to contain fraud or error. Pharmaceutical companies have begun to incorporate data mining in the drug discovery process in an effort to predict if a compound will have toxic effects. Hospitals use data mining results to design emergency room protocols to deliver

more effective patient care. On the commercial front, businesses have employed data mining to target advertising campaigns and to improve customer service.

Data mining also raises serious privacy concerns in a number of areas. For example, people may be *misclassified*. Even a good model predicts only that people with a certain set of attributes are statistically likely to possess the target attribute. Some people might be denied a mortgage based on a creditworthiness model even though they actually would make all their payments on time. A larger concern is the *misapplication* of data mining techniques. A model that excluded whole neighborhoods from mortgages, for example, would be effectively redlining. Data may also be used for *unauthorized* purposes. Information from a consumer's warranty form may be used in data mining applications unrelated to the provider's intent.

Some data are legally protected. Data collected from patients by a health care provider are protected from **disclosure** by law. Although it might not be illegal, data mining that uses other, unprotected data to proxy the protected data certainly violates the spirit of the law.

Because data mining may be effective in the aggregate, however, the very existence of these techniques creates some threat to privacy by creating a demand for data to input to the model. The desire to identify potential terrorists leads to pressure to supply more personal data to mine for suspects. What can get lost in the face of this pressure is the careful consideration of whether it is good for society in the long run to have public access to personal information such as a person's **library records** or genotype. It is conceivable, for example, that accurate predictions of the likelihood of developing certain diseases can be made based on an individual's genotype. What are the social implications of making these individuals ineligible for health insurance as a result of their genotype not being kept private?

See also: **Banking and financial records; Credit rating**

Suggested Reading: American Civil Liberties Union. *Privacy & Security*. <http://www.aclu.org/Privacy/PrivacyMain.cfm>. Online, November 2005; Berry, Michael J., and Gordon S. Linoff. *Data Mining Techniques: For Marketing, Sales, and Customer Relationship Management*, 2nd ed. Indianapolis: Wiley, 2004; Center for Media & Democracy. *SourceWatch: Data Mining*. http://www.sourcewatch.org/index.php?title=Data_mining. Online, November 2005; Thearling, Kurt. *Data Mining and Analytic Technologies*. <http://www.thearling.com/index.htm>. Online, November 2005.

Patricia Oslund
Larry Hoyle

***Davis v. Mississippi*, 394 U.S. 721 (1969)**

In *Davis v. Mississippi*, 394 U.S. 721 (1969), the United States Supreme Court held that the taking of fingerprints is covered by the Fourth Amendment prohibition against unreasonable searches and seizures. Fourteen-year-old John Davis was fingerprinted during a rape investigation in Meridian, Mississippi. The victim could give no description of her assailant other than that he was a "Negro youth." The police executed a "dragnet" investigation, interrogating suspects and taking fingerprints. Davis's fingerprints, which were recorded on two occasions, matched latent finger and palm prints taken from the scene of the crime. He was convicted and sentenced to life in prison. The Mississippi Supreme Court upheld the conviction.

On appeal, the state conceded that they did not have probable cause to arrest Davis at the time they took his fingerprints. The majority opinion, written by Justice William Brennan, held that Davis's fingerprint was the fruit of an illegal search, and the evidence must therefore be excluded from trial. Davis's conviction was reversed. The court made clear, however, that Fourth Amendment protection applied not to the fingerprints themselves, the taking of which was not overly intrusive, but to the arrest for the purpose of taking fingerprints. Moreover, the apprehension without probable cause had involved an interrogation and a redundant second request for fingerprints. The Court left open the possibility that the police could request or demand fingerprints from citizens with something less than probable cause, using "narrowly circumscribed procedures." Some states subsequently passed statutes authorizing detention for recording physical characteristics based on a standard less than probable cause.

Justice Hugo Black dissented, viewing the decision as an excessive expansion of the scope of the Fourth Amendment. Justice Potter Stewart also dissented, calling the reversal a "useless gesture." Stewart argued that fingerprints were not "evidence" in the conventional sense because, even if they were "wrongfully seized," they could be "identically reproduced and lawfully used at any subsequent trial."

Today, the primary importance of *Davis* is in the context of DNA evidence. The legality of "DNA dragnets" has been much discussed, and *Davis* is one of the key precedents in that debate. While some scholars argue that *Davis* makes DNA dragnets unconstitutional, others claim that the decision's apparent allowance of limited detentions to record fingerprints would apply to DNA recording as well, especially if the DNA were limited to nondiagnostic identifying characteristics, as opposed to the entire genome.

Suggested Reading: Cole, Simon A. *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Cambridge, MA: Harvard University Press, 2001; Dilworth, Donald C. (ed.). *Identification Wanted: Development of the American Criminal Identification System, 1893–1943*. Gaithersburg, MD: International Association of Chiefs of Police, 1977; German, Ed. *Latent Print Examination*. onin.com/fp. Online, November 2005; Imwinkelried, Edward J., and David H. Kaye. "DNA Typing: Emerging or Neglected Issues," *Washington Law Review* 76 (2001): 413–474.

Simon A. Cole

Decisional privacy. *See* Privacy, definition of

Declaration of Independence

No document better distilled American Revolutionary thought regarding liberal equality than the Declaration of Independence. It adapted philosopher John Locke's notion of inalienable human rights and the government's duty to its citizens. On the motion of Virginian Richard Henry Lee, which John Adams of Massachusetts seconded, the Continental Congress established a committee to draft the document. The committee was composed of Adams, Benjamin Franklin, Roger Sherman, Thomas Jefferson, and Robert R. Livingston. They assigned the actual writing to 33-year-old Thomas Jefferson. He understood that his task was "[n]ot to

find out new principles, or new arguments, never before thought of” but to express widely held convictions of “the American mind.” His success lay in the document’s concise natural rights formulation of Revolutionary argument. Members of the Continental Congress signed the Declaration on July 4, 1776, but they had voted for the actual act of independence on July 2.

The Declaration explained the reason for breaking away from England within the context of ethical theory. The manifesto took for granted the self-evidence of natural human equality. It prohibited despotic rule without the people’s consent. The people had no obligation to remain the subjects of a government that infringed on their co-equally inalienable rights of life, liberty, and the pursuit of happiness. A litany of accusations against George III followed. They were meant to show that the king’s despotic rule had forced the colonists’ hand, leaving them no choice but to declare their independence. The Declaration asserted that a divine natural order granted all people equal and inalienable rights. The power of government was derived from the will of the people who could overthrow any authority that failed to safeguard their happiness and could subsequently form a new nation.

Despite the Declaration’s bold assertion of rights, it lacked an explicit censure of slavery or slave importation. This was no accident. Jefferson’s original draft had accused King George of acting “against human nature itself” by keeping open an international slave trade that violated the “rights of life and liberty in the persons of a distant people.” But when South Carolina objected to that clause, the Continental Congress excised it from the final draft.

This wavering of principles did not efface the Declaration’s vision for creating a nation dedicated to preserving civil rights, which later generations understood to include the right to privacy. Its doctrine, as Samuel Adams said nearly 30 years after the states ratified it, became part of “the political creed of the United States.” This creed prohibited tyranny and committed the national government to achieving the common good rather than pandering to the interests of any individual, family, or class. To many groups, the Revolution brought no relief for their political impotence, but the implications of the Declaration were profound for all future generations willing to put the creed into sincere legal operation. The ethical perspective of the manifesto demanded unabated national self-criticism to address shortcomings related to the demands of America’s statement of purpose. A hurdle of constitutional doctrine that faced the advocates of civil rights, such as revolutionary abolitionists and feminists, was the Declaration’s lack of an enforcement mechanism. The principles it espoused said something about the American people, but it little benefited those under the immediate yoke of subordination.

For the Revolutionary generation, the Declaration was intrinsic to American civil culture. In the decades that followed, Fourth of July commemoration was celebrated throughout the country. At one of those events in the 1790s, John Quincy Adams, who would become the sixth president of the United States, asserted, “The Declaration of Independence and the Constitution of the United States are parts of one consistent whole, founded upon one and the same theory of government.” Although in legal terms the Declaration did not dictate the passage of any particular law, instigate any police action, or mandate the interpretation of any case, it provided all three branches of government with a sense of normative purpose. The Declaration of Independence also served as a measuring stick against which the



people could evaluate governmental conduct. But because it was only a general statement, liberty and equality were often cast aside for personal gain or exploitation, with little or no federal response. The country that asserted its affinity to universal equality found excuses for the misappropriation of slave labor and the exclusion of women from many privileges of citizenship.

Fortunately, the story of the Declaration did not end with the Revolutionaries but became a legacy to shape the conscience of future generations. Abolitionists considered it the cornerstone of a government committed to protecting individual rights for the entire populace, regardless of race. They grounded demands for the immediate liberation of slaves in the Declaration's self-evident truth of equal freedom. To them slavery was inimical to the immutable law of nature, designed to keep African Americans subjugated to the whims of their oppressors.

Abraham Lincoln, even before he became president, explicitly accepted much of the abolitionist view against slavery, which he called a "great moral wrong" that offended the Declaration's "fundamental principles of civil liberty." In the Declaration, he found an egalitarian ethic that served as "the great fundamental principle upon which our free institutions rest." Dealing with secession and Civil War, Lincoln seemed to elevate the Declaration above the Constitution, finding in it principles of "liberty to all" and the proposition of equality that would enable the nation to achieve a "new birth of freedom."

After the Civil War, the majority in Congress were filled with a fervor stemming from the Declaration's self-evident truths about the inalienability of fundamental rights. Congressmen like Representative Thaddeus Stevens and Senator Charles Sumner understood that racial inequality was incompatible with the country's commitment to the freedom and happiness of the whole. Most factions of the Reconstruction Congress, during the 1860s and 1870s, were united in their desire to further the values of the Declaration.

Legislators formulated constitutional amendments to provide Congress with the power to enforce the Declaration's ideals. Those changes to the Constitution in effect made the federal government the guarantor of the rights promised in the Declaration of Independence. As Speaker of the House Schuyler Colfax explained, "The Declaration of Independence must be recognized as the law of the land, and every man, alien and native, white and black, protected in the inalienable and God-given rights of life, liberty, and the pursuit of happiness." The Reconstruction amendments imported principles of governance from the Declaration into the Constitution. By tying the conception of the Declaration with the Constitution, they intrinsically connected guarantees of fundamental rights, such as those of the Bill of Rights, with national citizenship. This meant that states could not trump nationally recognized rights, shifting authority to the national government in matters of group discrimination.

The Thirteenth Amendment's abolition of slavery was predicated on the enlightened notion of universal human liberty. Indiana Representative Godlove S. Orth, for instance, expected the Thirteenth Amendment to "be a practical application of that self-evident truth" of the Declaration "that [all men] are endowed by their creator with certain unalienable rights; that among these, are life, liberty, and the pursuit of happiness." Private actors were henceforth prohibited from any badges and

incidents of involuntary servitude that kept people from enjoying the scope of freedom that should have been secured at the nation's founding.

When questions were raised about the effectiveness of the Thirteenth Amendment, work began on the Fourteenth Amendment to realize the ends implicit in the Declaration's statement on governmental purpose. The Equal Protection Clause of the Fourteenth Amendment was most clearly tied to the ideals that the Revolutionaries had espoused. It placed authority in the federal government to protect fundamental rights against any contrary state laws or state-sponsored actions. The Due Process Clause likewise protected the inalienable right to liberty against arbitrary state intrusions. Substantive due process brings privacy within the purview federal liberty interests.

The Fourteenth Amendment's arguably implicit importation of equality principles from the Declaration into the Constitution provided the impetus for numerous Supreme Court privacy decisions. The Court has relied on these underlying notions of liberty and equality in such key privacy cases as *Griswold v. Connecticut*, 381 U.S. 479 (1965) (concerning intimacy and the use of contraceptives); *Roe v. Wade*, 410 U.S. 113 (1973) (on abortion rights); and *Lawrence v. Texas*, 539 U.S. 558 (2003) (dealing with homosexual intimacy).

See also: **Constitutional protections; Privacy, philosophical foundations of; Privacy and inequality**

Suggested Reading: Becker, Carl. *The Declaration of Independence: A Study in the History of Political Ideas*. New York: Harcourt, Brace, 1922; Detweiler, Philip F. "Changing Reputation of the Declaration of Independence: The First Fifty Years," *William and Mary Quarterly* 19 (3rd ser., 1962): 557–574; Maier, Pauline. *American Scripture: Making the Declaration of Independence*. New York: Alfred A. Knopf, 1997; Wills, Garry. *Inventing America: Jefferson's Declaration of Independence*. Boston: Houghton Mifflin, 2002 (1978).

Alexander Tsesis

Digital cash

The 1996 Olympic Games in Atlanta caught the attention of a number of privacy advocates when the Olympic facilities refused to accept cash. To some observers, this development foreshadowed the coming of a cashless society where digital forms of payment would completely replace paper money.

In the twenty-first century, a growing proportion of economic transactions rely on electronic forms of payment, such as **credit cards**, debit cards, prepaid cards, and electronic fund transfers (EFTs). Electronic forms of payment offer consumers a number of benefits. Electronic funds transfers, such as automatic billing, allow consumers to avoid the hassles of the checkbook. They ensure timely payment, eliminating the problem of late fees. Prepaid cards enable consumers to obtain specific services, such as mass transit, with greater ease. Debit and credit cards eliminate the inconvenience of cash shortages. They also provide a sense of security as they incorporate some protections against lost or stolen cards. Furthermore, some forms of retail, such as e-commerce, depend on electronically completed transactions. While the digital direction of modern commerce does offer consumers new conveniences, it also raises privacy questions.

Although the replacement of lost or stolen cash depends entirely on the good grace of others, cash does offer an important advantage with respect to privacy: consumer **anonymity**. The paper money used to pay for a good or service leaves no record of the purchaser. Conversely, every commercial exchange that is electronically mediated generates an electronic “paper trail”: data that may be compiled, stored, and merged for the purpose of generating consumer profiles. Banks, credit bureaus, and other financial institutions can sell such **transaction-generated data** on the information market to **data brokers** and direct marketers. The compilation and exchange of personal information recorded from electronic payments thus sustains an assortment of intrusive marketing techniques such as **telemarketing**, **spam**, and junk mail. Aside from its use for marketing purposes, the electronic “paper trail” is available to law enforcement personnel who can assess such information. Purchasing records enable investigators to identify items bought and sold, as well as the whereabouts of any citizen.

Electronic forms of payment also make consumers vulnerable to criminal invasions of privacy, including **identity fraud** or theft. One’s exposure to cash loss is limited to the quantity of money that the individual carries on his or her person, but the potential financial loss from credit or debit cards is far greater. Debit cards present the highest risk. Unlike credit cards, where the law limits the cardholder’s liability to \$50, the consumer’s legal liability is unlimited with debit cards. Additionally, since payment occurs immediately, the consumer has no time to contest a charge and no leverage to withhold payment.

In summary, while the acceptance of a variety of new forms of electronic payment indicates that both consumers and marketers appreciate the associated conveniences, these innovations also have the potential to inflict financial damage far beyond what is possible with the use of cash.

See also: **Banking and financial records; Credit rating; Personally identifiable information**

Suggested Reading: Cate, Fred H., Robert E. Liton, Michael Staten, and Peter J. Wallison. *Financial Privacy, Consumer Prosperity and the Public Good*. Washington, DC: Brookings Institute, 2003; Evans, David S., and Richard Schmalensee. *Playing with Plastic: The Digital Revolution in Buying and Borrowing*. Cambridge MA: MIT Press, 1999; Fischer, Richard L. *The Law of Financial Privacy*. Washington, DC: A.S. Pratt & Sons, 2002; Manning, Robert D. *Credit Card Nation: The Consequences of America’s Addiction to Credit*. New York: Basic Books, 2000.

Brian Azcona

Digital signatures

“On the Internet no one knows you’re a dog,” reads the caption of the iconic *New Yorker* cartoon. That lack of identifiability is great for maintaining one’s **anonymity** but creates difficulty in using the **Internet** to conduct online transactions. There needs to be a way to bind an entity to the information that is being provided. Digital signatures do exactly that.

Digital signatures were invented by Whitfield Diffie and Martin Hellman in 1975. The signatures rely on public-key **cryptography**, whose security is based on what appear to be difficult mathematical problems. Public-key algorithms work by the publication of a “public key” with which messages are encrypted by the sender,

while the receiver has secret information, the “private key,” with which to decrypt the message. The system succeeds because a particular mathematical function is computed quickly whereas the inverse computation is slow.

In digital signatures, the roles of the public and private keys are reversed. The sender—in order to prove that he or she is indeed the sender of the electronic packet—wraps the information (or a shortened version of it, called a hash) in cryptography keyed by the sender’s private key. Because the sender’s public key is public information, anyone receiving the message can unwrap it, but that is not the issue.

In digital signatures the concern is linking the message to the sender. The computational complexity of the signature function makes it highly unlikely that anyone other than the sender could sign the message, and this enables **authentication** of the communication. The computations involved are too complex for a human to perform; it is actually the sender’s machine that computes the digital signature. If the sender’s machine has been corrupted, or if the sender contracts with a third party to do the signing, this could lead to counterfeiting—the transmission of other data signed using the sender’s private key. Of course, this is no different from the off-line world, where counterfeit signatures are also a possibility.

All data exchange between **computers** must occur according to a fixed protocol so that the machine correctly interprets the received bits; this is the purpose of standards. In 1992 the National Institute of Standards and Technology (NIST), the arm of the U.S. government responsible for setting standards for information security for its civilian agencies, sought a digital signature standard.

The RSA algorithm was the first practical public-key method for digital signatures, and the RSA signature scheme had been in use since the early 1980s (when the algorithm’s main application was machine-to-machine authentication of software configurations). The NIST now proposed that a different algorithm be used: DSA. The DSA choice was problematic: the algorithm been designed by the National Security Agency (whose process was not transparent), appeared to be subject to possible patent infringement problems, and was deemed too short—and thus easier to break and counterfeit—to be fully secure. Public objections resulted in changes to the proposed standard, the most important of which was a variable key size, enabling appropriate security.

Digital signatures simplify technical data exchange, allowing machines to “sign” information about their software, as well as online contractual arrangements. The latter, of course, require laws recognizing the validity of digital signatures, and many nations now have such laws.

Often technologies developed for one purpose are subsequently used for another. Internet websites operate more efficiently if they can identify repeat “customers,” and many sites attempt to do so, sometimes using digital signatures for authentication. Because digital signatures precisely identify the sender (or the sender’s machine), there is the capability of aggregating user information. Such problems can be avoided through the use of digital signatures with technology to ensure anonymity.

Suggested Reading: American Bar Association, Section of Science and Technology, Information Security Committee. *Digital Signature Guidelines Tutorial*. <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>. Online, November 2005;



Menezes, Alfred, Paul van Orschot, and Scott Vanstone. *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 2001; Mitchell, C. J., F. Piper, and P. Wild. "Digital Signatures." In *Contemporary Cryptology: The Science of Information Integrity*. New York: IEEE Press, 1991; United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards. *Digital Signature Standard (DSS)*, Publication 186 (May 19, 1994).

Susan Landau

***Dirkes v. Borough of Runnimeade*, 936 F. Supp. 235 (1996)**

In *Dirkes v. Borough of Runnimeade*, the United States District Court, District of New Jersey, decided that the dissemination of the video rental history of a former police officer and his wife violated the **Video Privacy Protection Act of 1988**. Accordingly, the court allowed the case to proceed against numerous defendants, including the Borough of Runnimeade, the Borough of Runnimeade Police Department, and several Borough of Runnimeade police officers who secured the former officer's rental information in the course of a disciplinary investigation. Although it was heard by a relatively low-level court, the case represents one of the strongest defenses of privacy protection ever made in a court case; indeed, it recalls and quotes numerous historical texts promoting the heightened importance of maintaining individual privacy protections in the modern era.

The case centered on an investigation of and disciplinary action against the plaintiff, Chester Dirkes, who was formerly a police officer in the Borough of Runnimeade Police Department. The department alleged that during the course of an investigation, Dirkes had removed pornographic magazines and videotapes from a citizen's **home**. The department then issued a disciplinary notice and suspended Dirkes without pay or benefits. Although he was acquitted of the charges in a formal trial held a few weeks later, the Borough hired special counsel and resumed its internal affairs investigation against Dirkes.

To aid in this continued investigation, one of the police officers working on the case obtained the names and rental dates of several pornographic videotapes rented by Dirkes and his wife. The officer gathered this information from an employee of Videos to Go, an establishment that Dirkes apparently visited regularly to rent videotapes. In obtaining this information, the police officer did not obtain a **search warrant**, a subpoena, or any sort of formal court order. Instead, he simply asked for and received the information from the employee at the store. As a result of this investigation, this private information was circulated and disclosed to numerous people at various proceedings, including one before the Superior Court of New Jersey, Camden County.

Dirkes and his wife then filed suit against numerous defendants, alleging the violation of two provisions of the Video Privacy Protection Act of 1988 (18 U.S.C. §2710), as well as common law privacy rights. The court found that these claims were valid and enforceable against all the defendants given the broad construction of the act.

The court began its analysis by quoting several famous articles and discussions emphasizing the importance of an individual's privacy. The court noted that the

Privacy Act of 1974, the Fair Credit Reporting Act, the Tax Reform Act of 1976, the Right to Financial Privacy Act of 1978, and the **Cable Communications Policy Act of 1984** all confirm that Congress reserves extensive protections against **disclosures** of citizens' personal information, particularly in the modern era of increasing technological advancement, in which the risk of disclosure is much greater. The court quoted numerous Supreme Court opinions stressing this point, including *Olmstead v. United States*, 277 U.S. 438 (1928), in which **Louis Brandeis**, in a famous dissent, argued that the "**right to be let alone**" is "the most comprehensive of rights and the right most valued by civilized man." Thus, the court concluded, "Consistent with this principle, in construing the scope of the [Video Privacy Protection] Act, this Court must strive to protect this aspect of an individual's right to privacy in the face of technological innovations that threaten this fundamental right."

The court found it undisputable that the defendants violated the Video Privacy Protection Act; the violation simply was not an issue. Instead, the court focused its analysis on which defendants were properly charged as violators. The court ultimately rejected the argument that only the video outlet that revealed the private rental information of Dirkes and his wife could be properly sued by them. On the contrary, the court found "that those parties who are in possession of **personally identifiable information** as a direct result of an improper release of such information are subject to suit under the Act. Because it is undisputed that [one of the police officers], the Department, and the Borough all possess the information as a direct result of a violation of the Act, each is a proper defendant." Thus, by broadly interpreting the reach of the statute based on its high regard for individual privacy, the court maximized the protection of individual privacy in this case.

Suggested Reading: Barteo, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

Ryan C. Hudson

Disclosures

Disclosures can take many forms and come from a variety of sources. These forms and sources of disclosure determine the nature of any associated threat to privacy and the character of privacy protections.

Disclosures by government may be the most damaging to privacy. They can arise from the application of laws that address interests other than privacy. Three important areas demonstrate how disclosures permitted or required by law may affect privacy. In one of these areas, public financial disclosure, the government requires high-ranking government employees to provide private information, which is then disseminated by the government. This tolerance of disclosure is grounded in the need to protect government programs from conflicts of interest or corruption and to reassure the public of the integrity of the public sector.

In the second area, litigation, the government, through the courts, requires the disclosure of private information by parties seeking redress or defending themselves in civil litigation. Although such disclosure may often be voluntary, the courts possess the authority to require the parties, as well as third persons, to provide information that may threaten privacy. Increasingly critics have challenged the ways in which the courts reconcile the need for information in litigation with limitations on disclosure.

In the third of these areas, protection of whistleblowers, the government encourages the disclosure of information in order to defend a variety of public interests. These disclosures may include private information. The degree of risk to privacy from these disclosures depends on the definition of permitted versus prohibited disclosures, the standards for disclosure, and the identity of those to whom disclosures may be made.

An examination of these three areas shows how privacy protection permeates government activities that rely on disclosures of information. It also demonstrates that the definition of privacy and the means of its protection are affected by the context of these disclosures.

Disclosures can also protect privacy. For example, the access to and correction of records permitted by the **Privacy Act of 1974** reduce the likelihood of the government maintaining inaccurate or false information. Disclosures likewise expose and thereby deter government invasions of privacy. In this regard, the disclosures required by **public records** law and volunteered by whistleblowers support rather than threaten privacy.

Public financial disclosure laws provide public access to information regarding the private financial affairs of public employees. Employees subject to these laws must submit required information or face criminal and civil penalties, including administrative sanctions. Such laws seek to increase public confidence in government, to alter the perceptions about and conduct of public employees, and to encourage debate regarding conflict-of-interest provisions. The majority of states had adopted some form of public financial disclosure laws prior to the enactment of the federal Ethics in Government Act of 1978.

The Ethics in Government Act illustrates the scope of disclosures under these laws and their effect on privacy. The Act also demonstrates ways in which these disclosure laws address concerns about privacy. The Ethics in Government Act applies to high-level government officials and civil servants. The act requires these employees to file disclosure forms that are then made available to the public. The forms direct the reporting of a variety of financial interests, including earned and unearned income, financial transactions, compensation received, and positions held in businesses and nonprofit organizations. The disclosure forms call for considerable detail regarding the reporting of gifts and income.

Critics attack financial disclosure laws as invasions of the right of privacy of affected government officials. Legal challenges to the provisions on this ground, however, have proved to be unsuccessful. Despite the failure of most judicial challenges, criticisms based on the infringement of privacy have had an influence on these laws. In the act, Congress sought to limit the information reported to the types of financial interests likely to involve conflicts of interest. Congress also sought to reduce administrative burdens and intrusions on financial privacy.

The Ethics in Government Act limits the reporting of assets and liabilities to broad bands of value and places minimum value on the compensation and gifts that must be disclosed. The act incorporates other protections for reporting employees, including the review of reports prior to disclosure, destruction of reports after six years, and penalties if the reports are used for unlawful purposes or for commercial interests such as solicitation.

Public financial disclosure not only may affect the privacy of employees but also may infringe on the privacy of others. Many financial disclosure laws include the financial interests of spouses and other close relatives among those that must be reported by employees. Infringement of the privacy of third persons seems less justified, and some state courts have struck down the requirement to report the assets of a spouse.

Although the privacy interests of third persons demand special consideration, the exclusion of the financial interests of close relatives invites evasion. The Ethics in Government Act includes the financial interests of spouses of employees but seeks to accommodate the privacy interests of third persons by allowing exemptions that limit the circumstances in which their financial interests must be reported. These exemptions emphasize factors such as a spouse's independent receipt of gifts or independent property holdings.

Persons who bring or defend civil litigation are subject to rules designed to provide other parties with information regarding claims and defenses. These rules allow discovery of documents, the questioning of witnesses under oath, physical and mental examinations, and interrogatories to other parties. These discovery devices enable the parties to address fairly and efficiently the merits of claims and defenses. However, they also give parties extensive information about others, including much information that is private—personal finances, membership and donor lists of private associations, physical and psychological data, private associations and affiliations, and personal attributes and items of conduct.

The disclosure of this information, acquired under the authority of the courts, by parties to the litigation threatens personal privacy, invites abuse, encourages intimidation, and discourages individuals from seeking redress in the courts. As a result, judges have the authority to order parties not to disclose or promulgate this information except in the context of the litigation itself. These “protective orders” are common and important safeguards of the judicial process and of privacy.

Critics of the authority of judges to issue these protective orders assert that these orders have been used to deny the public and government agencies information about public health and safety. In response, several states have enacted provisions that restrict the ability of judges to limit the disclosure of health and safety information acquired by the parties in litigation. One of the broadest of these provisions, the Florida Sunshine in Litigation Act, prohibits protective orders to prevent the



disclosure of information regarding a public hazard. The definition of public hazard encompasses information about any person who has caused or is likely to cause injury—a definition that may place some private information about individuals beyond the scope of protective orders.

Private information may be disclosed in other ways during litigation. Many litigation documents, such as pleadings, motions, and judicial rulings, are public records. In addition, the common law and the Constitution provide access to court proceedings and to rulings that terminate or conclude the litigation. Some courts have extended this right to documents filed by the parties in regard to such rulings. Although courts have the authority to close proceedings and to seal records, these actions are unusual.

Access to litigation materials illustrates how the electronic revolution has altered the character of disclosures accompanying public documents. Electronic dissemination makes the disclosure of information contained in litigation widely available throughout the world. For example, persons who file for bankruptcy may face the disclosure of much private information. Parties in a variety of types of litigation face the disclosure of medical files, tax and employment records, and personal identifiers.

Scholars disagree as to whether the medium of disclosure should affect the determination of what constitutes a public record. Some argue that access to judicial records should remain the same regardless of the medium of disclosure because a person has no expectation of privacy in public records. Others argue that electronic disclosure alters the expectation of practical obscurity that litigants appropriately held when documents were available only in paper form at a specific physical location.

The practices of the federal courts illustrate both the importance of public access through the **Internet** and the risks to privacy posed by such access. The software Public Access to Court Electronic Records, which enables users to access documents over the Internet, permits a person, at a small cost per page, to view case file documents, listings of case parties, reports on case-related information, chronologies of such information, claims registers, judgments, and case status information, as well as a nationwide party and case index.

On the other hand, courts retain the right to deny access to court files by weighing the interest in privacy against the presumption of public access. The courts may also consider other interests arguing against disclosure, including the likelihood of pretrial publicity, impairment of law enforcement, and judicial efficiency. Model rules developed by the Judicial Conference of the United States permit courts to require the redaction of certain private information in court filings for bankruptcy and criminal cases. For example, in criminal cases certain personal information and identifiers may be withheld, including **Social Security numbers** exclusive of the last four digits; financial account numbers, except for the last four digits; names of minor children other than their initials, the month and day of birth, and home addresses other than the city and state.

Because the system of electronic access requires registration, it can track the accessing of particular documents by each user. This tracking is justified as a deterrent to possible abuse.

The federal government and most states protect from reprisals both public- and private-sector employees who disclose information regarding certain types of

misconduct by their employers or by others. In addition, the federal government and many states have false claims laws that encourage disclosures of fraudulent claims against the government by providing that whistleblowers receive a portion of any amounts recovered on behalf of the government. Whistleblower laws support the rule of law, the prevention of corruption, the discovery and deterrence of misconduct, and protection of the public from health and safety risks and from financial losses. Protected disclosures, however, may contain private information, including financial and medical data.

These statutes address the protection of privacy in a number of ways. First, they prohibit certain disclosures. The prohibitions can be broad, such as one that denies protection for any disclosure barred by law, or more narrow, such as ones incorporating only specific prohibitions. Broad prohibitions encompass any privacy law that prohibits the disclosure of certain information. More narrow ones must specifically incorporate any privacy protections.

Second, the standard for disclosure influences the number of disclosures that can be made and perhaps the risk to privacy. Most statutes require that the whistleblower have a reasonable belief that the disclosed information evidences violation of the types of misconduct addressed by the law. Some statutes require that the misconduct in fact exist for the whistleblower to receive protection, and a few protect a disclosure made solely on the basis of a good faith belief of wrongdoing. More disclosures are likely under the good faith standard than under the standard of wrongdoing in fact.

Third, these statutes address to whom disclosures may be made. Some statutes permit disclosures to the public at large; other statutes limit them to certain public bodies or law enforcement agencies. A few permit otherwise prohibited disclosures to be made to special officials with the authority to address the issues raised by such disclosures.

Usually, the same standard for disclosures applies regardless of the party to whom the disclosures may be directed. In other cases, the standard for disclosure can vary depending upon the person or entity to whom the disclosure is made. For example, disclosures within a company or agency may be subject to the most lenient standard, disclosures to regulatory or law enforcement agencies marked by a more demanding standard, and disclosures to the public associated with the most demanding standard for disclosure.

Whistleblower laws place the responsibility for disclosures on the individual. Protected disclosures may be made even though an employee's agency or company might have decided not to release the information. Whistleblower protection vindicates this responsibility and uses it to advance important public interests. Individual responsibility, however, allows employees to resolve information disclosure issues differently than the institutions for which they work. This difference between individual choice and institutional policy has implications for the protection of privacy.

Of course, leaks and anonymous disclosures pose even greater threats to privacy. These types of disclosures are not bounded by the judgments contained in whistleblower laws. Effective laws may reduce the likelihood of leaks by encouraging disclosures under legal standards. The possibility of unauthorized disclosures threatening privacy justifies the information management requirements of some privacy laws and their emphasis on security.



It is perhaps easier to see how disclosures can threaten privacy than to understand how they protect it. The access provisions of the Privacy Act illustrate the protective character of disclosures. By permitting individual to examine records pertaining to them, the Privacy Act gives individuals the ability to evaluate the information contained in these records and to judge the compliance of the government or employer with the information management requirements of the law. Disclosures in these circumstances serve to protect rather than to threaten privacy.

Likewise, disclosures by whistleblowers can help to secure rights to privacy. Disclosures exposing the illegal collection, management, and use of information by the government or by private parties deter such abuses. These disclosures also allow a response to abuses at a time when the damage to affected individuals may be limited. These disclosures encourage legal and political actions to guarantee effective privacy protection.

In the context of the regulation of information held by the government, disclosures can reflect opposing government views of privacy. Privacy scholar Alan Westin emphasizes the relationship between access and privacy in democratic governments. He defines democracy and authoritarianism in terms of information policy. Authoritarian governments are identified by ready government access to information about the activities of citizens and by extensive limitations on the ability of citizens to obtain information about the government. In contrast, democratic governments are marked by significant restrictions on the ability of government to acquire information about its citizens and by ready access by citizens to the information about the activities of government. Rather than being inexorably in conflict, disclosure and privacy are both intertwined with democratic accountability.

See also: **Civil service laws; Open meetings laws; Public health and safety; Public records; Workplace privacy**

Suggested Reading: Devine, Thomas. "The Whistleblower Protection Act of 1989: Foundation for the Modern Law of Employment Dissent," *Administrative Law Review* 51 (1999): 531–579; Judicial Conference. *Report of the Judicial Conference Committee on Court Administration and Case Management on Privacy and Public Access to Electronic Case Files* (2001). <http://www.privacy.uscourts.gov>. Online, March 2006; U.S. Office of Government Ethics. *Public Financial Disclosure: A Reviewer's Reference*, 2nd ed. Washington, DC: Office of Government Ethics, 2004; Westin, Alan. *Privacy and Freedom*. New York: Atheneum, 1967.

Robert G. Vaughn

DNA and DNA Banking

DNA is the abbreviation for deoxyribonucleic acid, a molecule encoding genetic information that is found in the nucleus of all human cells, except mature red blood cells. It controls the structure, function, and behavior of cells and determines individual hereditary characteristics. DNA banking involves the collection and storage of bodily specimens that contain DNA, the storage of strands of DNA extracted from such specimens, and the maintenance of databases of sequenced DNA. According to an inventory commissioned by the National Bioethics Advisory Committee in 1999, specimens of human material that contain DNA are collected from approximately 20 million individuals per year and stored in collections ranging in size from less than 200 specimens to more than 92 million.

Given this proliferation of DNA banking, a significant portion of the general public has or soon will have their DNA stored in a DNA repository. These repositories, sometimes referred to as DNA banks, tissue banks, gene banks or biobanks, can differ in many respects. A DNA bank may be organized as a public, private, non-profit, or commercial entity that exists for a discrete period of time or indefinitely, depending on its purposes. Some repositories store DNA as an unintended consequence of possessing bodily material that has been collected for other uses. Other repositories store bodily specimens (e.g., blood, saliva, urine, sperm) specifically because the specimens contain human DNA. Of the dedicated DNA repositories only a few engage in DNA banking as an end in itself; most DNA banking is undertaken to support activities such as biomedical research, law enforcement, or genealogical research. The purpose, size, storage technology, longevity, and corporate status of the entity can influence the kind and degree of privacy risks presented by its DNA banking and the extent to which its activities are regulated to reduce those risks.

Since DNA is present in most human cells, it would be impossible to conduct routine medical care and related laboratory services without collecting and banking DNA. For example, blood banks and clinical, diagnostic, and pathology laboratories routinely collect and process tissue samples for a variety of diagnostic and therapeutic purposes with no intention of deriving genetic information from the samples. This incidental DNA banking does not in itself raise privacy issues beyond those associated with creating and maintaining personal medical information. Although federal and state privacy laws that govern medical record keeping and **disclosures** of health information undoubtedly apply to their activities, no additional legal restraints are placed on these entities merely because they are in possession of DNA samples. Most notably, institutions such as these are not required by federal or state law to destroy specimens after a particular time, and therefore they may retain specimens (and any information linked to them) based on their specific storage capacity and internal policies. Consequently, the possibility, if not the probability, of unauthorized access and misuse of samples is presented by incidental DNA banking. Until the samples are either destroyed or stripped of individual identifiers, this possibility entails some risk to personal privacy.

Some companies bank DNA as a consumer service that is available to anyone who is able to pay the requisite fees. This service has been marketed to parents as a means of preserving their DNA or their children's DNA to make it available if needed for identifying missing persons or bodily remains. In this kind of DNA banking, samples must be maintained in an identifiable form, but there is no need for them to be linked to any personal information beyond identifiers and contact information. Assuming that storage facilities fulfill their contractual obligations to safeguard the samples against unauthorized access, any personal genetic information should remain encoded in the DNA, and banking under these conditions would appear to present minimal risk to personal privacy. Nevertheless, commercial DNA banking of this type is a new industry that is relatively unregulated in the United States. It presents unresolved legal issues, including the degree of privacy protection available to those who purchase the banking services. For example, some banks offer to store samples for 20 years or longer. What happens to the contractual promises made to "depositors" in the event that a bank goes out of business, files



for bankruptcy protection, or merges with another entity is not clear. What such banks are legally obligated or are permitted to do with samples that are unclaimed when the term of storage expires or when storage fees are not paid has yet to be addressed by any state or federal statute or court ruling.

The concerns related to storing or banking DNA are compounded when banking is done for purposes related to **genetic information and testing**. An individual's entire genome is encoded in each DNA sample collected from that individual. Since DNA is relatively stable, there is no need to go back to an individual to collect additional samples every time a new procedure for deriving information from DNA becomes available. Therefore, possession and storage of a DNA sample presents the opportunity to access a wealth of information about that individual, including information that could not be anticipated at the point in time the sample was collected. Consequently, once steps are taken to preserve an individually identifiable sample for analysis, the risks to that individual's privacy can be significant. Given that an individual shares DNA to varying degrees with his or her genetic relatives, those privacy implications may extend to family members as well. The primary risk is that unauthorized testing of DNA might result in strangers knowing more about an individual's genetic makeup than that person knows herself or wants others to know. In response to these concerns, many states have enacted laws that regulate the circumstances surrounding genetic testing. However, few of these laws even mention the collection or storage of DNA samples and instead focus on what constitutes adequate consent or authorization to conduct testing and to use or disclose test results. Moreover, these laws tend to be directed toward the behaviors of insurers or employers and do not usually include a general prohibition against secret or surreptitious collection and testing of DNA that is applicable to everyone.

In 1998 the Icelandic Parliament enacted the Act on a Health Sector Database, a law authorizing the collection and storage of the entire nation's health information and genetic material by a private biotechnology corporation and granting that company, deCODE Genetics, an exclusive license to exploit the data. This model of a national biobank ignited an ethical and legal debate about how biobanks of such magnitude should be regulated. Specific questions were raised about whether the planned methods for collection and storage of DNA samples and personal information will adequately protect the privacy of the hundreds of thousands of Icelanders involved. Much of the criticism of the Icelandic model focused on its use of presumably open-ended consent for inclusion of Icelanders' personal information in the databank as opposed to a voluntary, informed-consent process. Doubts were also raised as to whether measures for protecting data, such as the use of encryption techniques, were sufficient to guard against breaches or **disclosures** of data.

In the wake of the controversies over Iceland's model for biobanking, planners of other large-scale gene banks (e.g., in Estonia, the UK, Japan, and Quebec) are experimenting with different approaches with regard to the structure, protocols, and oversight of their banks to protect the interests of individuals who contribute samples and information. Notable differences include the consent procedures that the banks will employ, the extent of personal information that will be passed on to researchers, and the measures that will be taken to prevent researchers from being able to determine whose DNA and information they receive.

The United States has not yet set up a national DNA bank to support genetic variation research that is comparable to the Icelandic project or the UK biobank. Nevertheless, DNA banking is being pursued by a significant number of nonprofit as well as for-profit entities in the United States. Several of the for-profit banks function as brokers and intermediaries that facilitate research and don't actually conduct in-house research. This is significant because established laws and regulations for the protection of human subjects in research do not apply to a broker model of DNA banking. However, research laws, particularly the federal regulations known as the Common Rule (codified at 45 CFR 46) will generally apply to researchers that purchase samples and data from these broker-style banks. Therefore, to satisfy concerns of their clients over compliance issues and to protect their own options to directly engage in research at a later time, some banks have chosen to design their protocols for collecting samples and information and for protecting the privacy of their donors to be consistent with the federal research regulations. Nevertheless, such compliance is voluntary, and in the absence of a federal law imposing such rules on DNA banking or uniform state laws regulating these activities, the banks' policies would not be enforceable.

See also: **Fair information practices; Human subjects protections; Personally identifiable information**

Suggested Reading: Annas, George J. "Privacy Rules for DNA Databanks," *Journal of the American Medical Association* 270 (1993): 2346–2350; Clayton, Ellen Wright. "Informed Consent and Biobanks," *Journal of Law, Medicine and Ethics* 33 (2005): 15–20; Eiseman, Elisa, Gabrielle Blom, Jennifer Brower, Noreen Clancy, and Stuart Olmsted. *Case Studies of Existing Human Tissue Repositories*. Santa Monica, CA: Rand, 2003; National Bioethics Advisory Commission. *Research Involving Human Biological Materials: Ethical Issues and Policy Guidance*, vol. I. Rockville, MD: National Bioethics Advisory Commission 1999; Oosterhuis, J. Wolter, Jan Willem Coebergh, and Evert-Ben van Veen. "Tumour Banks: Well Guarded Treasures in the Interests of Patients," *Nature Reviews Cancer* 3 (2003): 73–77; Rothstein, Mark. "Expanding the Ethical Analysis of Biobanks," *Journal of Law, Medicine and Ethics* 33 (2005): 89–99.

Patricia A. Roche

Do-not-call registry

On June 27, 2003, the U.S. Federal Trade Commission opened the National Do-Not-Call Registry (DNCR) in compliance with the Do-Not-Call Implementation Act. The DNCR is a registry of telephone numbers in the United States that **telemarketing** firms are prohibited from calling. The act, which took effect March 31, 2003, also requires telemarketers to display their phone numbers on caller ID devices and mandates that a live operator be on the line within two seconds of the time the customer answers the phone.

The DNCR was a joint establishment of the Federal Trade Commission and the Federal Communications Commission in response to growing consumer frustration over telemarketing calls. Telemarketing had been widely regarded as an intrusion on personal privacy, violating consumers' "**right to be let alone**" and their **anonymity**. Industry estimates in 2002 indicated that telemarketers could initiate as many as 104 million calls per day to homes and business. Increases in the



use of auto-dialers, which are used to deliver prerecorded messages to thousands and to initiate phone calls while telemarketers are still pitching to other consumers, exacerbated consumer aggravation.

The Telephone Consumer Protection Act of 1991 (TCPA) was the primary law in place governing the conduct of telephone solicitation, but it was rendered ineffective because consumers had to separately request that each telemarketer be put on the company-specific do-not-call lists, which were often ignored by telemarketing companies. As a result, 30 states had set up their own do-not-call lists to regulate intrastate telemarketing by 2003.

The federal rule required the National Do-Not-Call Registry to merge with similar but less restrictive state lists. Beginning October 1, 2003, telemarketers would be required to synchronize their databases every three months with the DNCR and would face a maximum penalty of \$11,000 for each call in violation. Tax-exempt nonprofit organizations and calls of a political or religious nature would not be subject to the do-not-call requirements since they are not considered telephone solicitations under the TCPA. Telemarketing companies with an established business relationship with a particular individual may also call up to 18 months after the last business transaction unless the individual specifically asks the company not to call again.

Before its implementation on October 1, 2003, the DNCR was challenged in federal district courts in Oklahoma and Colorado. The telemarketing industry argued that the DNCR infringed on commercial speech by introducing unconstitutional content-based restriction and that the FTC lacked adequate authority. Congress reacted on October 2 by granting the FTC specific jurisdiction over the enforcement the DNCR. The U.S. Court of Appeals, Tenth Circuit, on February 17, 2004, upheld the constitutionality of the DNCR, stating that the FTC had a legitimate and substantial interest in protecting citizens’ privacy in terms of the right to be left alone in their own homes. The court also justified the FTC’s decision targeting commercial telemarketing by citing complaint statistics presented in the legislative history of the TCPA, which indicated that commercial telemarketing intruded on personal privacy more than noncommercial solicitations.

On October 23, 2004, the U.S. Supreme Court turned away an appeal by the American Teleservices Association and refused to question the legitimacy of the NDCCP, which already had more than 63 million phone number registered.

Suggested Reading: Ayers, Ian, and Matthew Funk. “Marketing Privacy,” *Yale Journal on Regulation* 20 (2003): 77–137; Cain, Rita Marie. “Federal Do Not Call Registry Is Here to Stay: What’s Next for Direct Marketing Regulation?” *Journal of Interactive Marketing* 19 (2005): 54–62; Galloway, Chester S., and Steven P. Brown. “Annoying, Intrusive, and Constitutional: Telemarketing and the National Do-Not-Call Registry,” *Journal of Consumer Marketing* 21 (2004): 27–38; Petty, Ross D. “Marketing without Consent: Consumer Choice and Costs, Privacy and Public Policy,” *Journal of Public Policy & Marketing* 19 (2000): 42–53.

KuoRay Mao

“Don’t ask, don’t tell”

A person’s sexual orientation, and whether or not he or she discloses it to others, is generally understood to be a private matter. The decision of the Supreme Court

in *Lawrence v. Texas*, 539 U.S. 558 (2003), recognized that the constitutional right of privacy encompasses adult consensual relationships and that homosexuals’ “right to liberty under the Due Process Clause gives them the full right to engage in their conduct without intervention of the government.” One major exception exists with respect to employment in the United States military.

Federal law in the United States prohibits openly gay and lesbian people from serving in the armed forces. The asserted rationale by military leaders for this policy of legalized discrimination focusing on status and not conduct is that the presence of openly gay and lesbian personnel would interfere with the military’s ability to accomplish its mission. As with most things military, Congress defers to military leaders to determine what is best for the military, including an institutionalized policy of employment discrimination. Although the late conservative senator Barry Goldwater (R-AZ) observed that “[e]veryone knows that gays have served honorably in the military since at least the time of Julius Caesar,” it is argued that because heterosexuals have such antipathy for gay people, they would be unable and unwilling to serve with them. A similar argument was made with respect to racial integration of the armed forces. Although racial segregation has ended and the practice of racial intolerance is banned, the military asserts that it is unable to control or punish intolerance toward gay people. The United States is virtually alone among Western military powers in banning openly gay personnel.

“Don’t Ask, Don’t Tell” is the common name for the federal law, enacted in 1993, and attendant regulations banning openly gay and lesbian service members. While the previous policy prohibited service outright, the “Don’t Ask, Don’t Tell” standard allows gays and lesbians to serve in the military, but under drastic restrictions. Under the “Don’t Ask, Don’t Tell” framework, the military is forbidden to ask about the sexual orientation of a service member or recruit, and the service member or recruit is not to reveal (in words or conduct) his or her sexual orientation. Engaging in sexual conduct with a member of the same sex, however, remains grounds for discharge. The military is not to pursue suspected homosexuals without credible evidence. The law is an attempted compromise between an outright ban on gay service members and an end to discrimination.

It has long been the position of the U.S. military that homosexuality is incompatible with military service. In keeping with that official edict, in the 1980s, nearly 17,000 men and women were discharged on the grounds of homosexuality. By the end of the 1980s, two decades after the start of the gay liberation movement, civil rights groups had begun to push for an end to the military ban. Numerous social scientists and military experts came forward to refute the premise that the presence of gays and lesbians in the military had an adverse effect on the mission of the military. Legal challenges were also mounted, albeit unsuccessfully. Public opposition to discrimination against gays grew with news reports of brutal, unprovoked attacks by service members against suspected gay comrades.

In 1992 then-candidate Bill Clinton, declaring the unfairness of the discriminatory treatment of gays and lesbians, pledged to end the ban. After Clinton’s inauguration in 1993, it appeared that the military’s ban on gay personnel might be overturned. But Clinton’s proposal to end the ban faced strong opposition from the Joint Chiefs of Staff and members of Congress, who were spurred on by the political opposition. President Clinton withdrew his campaign promise to lift the ban on



homosexuals in the armed forces and agreed to the compromise of “Don’t Ask, Don’t Tell,” which was later amended to include “Don’t Pursue.”

As the civil rights group Servicemembers Legal Defense Network (SLDN) has observed, “Don’t Ask, Don’t Tell, Don’t Pursue” signifies new limits to military investigations and the intent to respect service members’ privacy:

[The military] agreed to take steps to prevent anti-gay harassment. They agreed to treat lesbian, gay and bisexual service members even-handedly in the criminal justice system, instead of criminally prosecuting them in circumstances where they would not prosecute heterosexual service members. They agreed to implement the law with due regard for the privacy and associations of service members.

However, SLDN also has concluded, “Intrusive questioning continues. Harassment continues in epidemic proportions. Little regard for service member privacy has been shown during the life of this law. Simply put, asking, pursuing, and harassing have continued.”

A 1998 legal case illustrates the military’s refusal to comply with the letter and spirit of “Don’t Ask, Don’t Tell,” as well as the implications of the policy for electronic privacy. In *McVeigh v. Cohen*, brought in federal court in Washington, D.C., the Navy was found to have engaged in a “witch hunt” to oust an 18-year veteran and decorated sailor. The Navy was ultimately found to be in violation of “Don’t Ask, Don’t Tell” and to have impermissibly invaded the sailor’s privacy in violation of the federal **Electronic Communication Privacy Act of 1986**. The sailor, a master chief petty officer, had used his AOL **electronic mail** account to collect toys at holiday time for the children of his shipmates. A recipient felt that the username associated with the e-mail account suggested the sailor was gay, and reported him. The Navy commenced an investigation and, under false pretenses, convinced AOL to reveal information about its subscriber, which the Navy used to confirm that the sailor was gay. On that basis, the Navy sought to oust CPO McVeigh. United States District Judge Stanley Sporkin enjoined the Navy from discharging McVeigh. He found that the Navy, in addition to engaging in the prohibited witch hunt, had violated federal electronic privacy law in a way that suggested an era of snooping by “**Big Brother**” government. AOL, whose terms of service promised privacy to its subscribers, quickly settled with McVeigh.

In the same year *McVeigh* was decided (1998), the Defense Department released a review of “Don’t Ask, Don’t Tell.” It acknowledged many improper investigations and recommended better training for those responsible. Improper investigations have declined since then but have yet to be completely eliminated. For example, the Defense Language Institute has discharged highly trained linguists in recent years, many with much-needed expertise in Arabic, because of alleged homosexual conduct using criteria advocates believe were unwarranted. Since “Don’t Ask, Don’t Tell” became law, thousands of gay and lesbian service members have been ejected from the military, at a projected cost of hundreds of millions of dollars. The rate of discharge for homosexual conduct has declined in recent years, which is historically consistent with discharge patterns in previous times of war. The military is thought to be more lenient in its enforcement efforts in wartime due to recruitment difficulties.

The *McVeigh* case represents one of the few successful legal challenges under “Don’t Ask, Don’t Tell.” Challenges to the constitutionality of the policy so far

have been unsuccessful, but a 2004 lawsuit, filed in the wake of the Supreme Court decision in *Lawrence v. Texas* and its broad language on the privacy rights of gays and lesbians, is pending. In addition, in late 2005 more than 100 members of Congress co-sponsored legislation to end the “Don’t Ask, Don’t Tell” policy

Suggested Reading: Belkin, Aaron, and Geoffrey Bateman. *Don’t Ask, Don’t Tell: Debating the Gay Ban in the Military*. Servicemembers’ Legal Defense Network, <http://www.sldn.org>. Online, December 2005; Butler, Judith. *Excitable Speech: A Politics of the Performative*. New York: Routledge, 1997; Johansson, Warren, and William A Percy. *Outing: Shattering the Conspiracy of Silence*. New York: Harrington Park Press, 1994; McGowan, Jeffrey. *Major Conflict: One Gay Man’s Life in the Don’t-Ask-Don’t-Tell Military*. New York: Broadway Books, 2005; Shilts, Randy. *Conduct Unbecoming: Gays and Lesbians in the US Military*. New York: Penguin Putnam, 1994.

Christopher Wolf

Douglas, William O. (1898–1980)

William O. Douglas was born on October 16, 1898, in Maine, Minnesota, but he spent much of his childhood in the state of Washington. In his youth Douglas enjoyed hiking and fishing in the Cascade Mountains. His wilderness experiences left a lasting impression on him, and he even published a semi-autobiographical account about his rapturous love for the outdoors. After serving as the valedictorian of his high school class, Douglas attended Whitman College on a full-tuition scholarship and graduated in 1920. After teaching for two years, he attended Columbia Law School, graduating from there in 1925. After a brief stint in a major law firm, Douglas taught at Columbia Law School and then at Yale Law School.

His career was marked by a further spike when he became chairman of the Securities and Exchange Commission (1937–1939). He did not stay there long, as President Franklin D. Roosevelt nominated him to the Supreme Court of the United States, and the Senate quickly confirmed his appointment. He served on the Court from April 17, 1939, when he was just 40 years old, to November 12, 1975—a period longer than any of the Court’s other justices served. During that time, Douglas wrote a record number of 1164 opinions and over 450 dissents. He worked with almost one-third of all the other justices who had been appointed to the highest court before his retirement.

For a time, Douglas contemplated resigning from the Court to occupy an eminent office in the executive branch of government. In 1944, when the Democratic Party nominated Roosevelt for a fourth presidential term, Douglas nearly became the vice-presidential candidate on the ticket. Roosevelt’s top two choices for running mate were Douglas and Harry Truman. The president scribbled both names on a piece of paper. Although there was some indication that Roosevelt preferred Douglas, by happenstance Truman’s name appeared first on Roosevelt’s list. Robert Hannegan, party chairman of the Democratic National Committee, understood the order in which Roosevelt wrote the names to be indicative of his preferences. Truman therefore became Roosevelt’s vice president, succeeding him as president after his death. Just four years later, in 1948, Truman asked Douglas to join the ticket as his vice-presidential running mate, but Douglas turned down the offer.



Douglas chose to remain a member of the Court. At the heart of his landmark privacy jurisprudence is an unorthodox belief in the Constitution's plasticity. In cases dealing with individual rights, Douglas often relied on a broad interpretation that places more emphasis on pre-constitutional liberties than on *stare decisis*. "The Constitution is a compendium," he declared, "not a code, a declaration of articles of faith, not a compilation of laws." Douglas also believed that the Bill of Rights is a sampling of rights rather than an exhaustive list, that there are also unenumerated rights that the Bill of Rights implies in the First, Third, Fourth, Fifth, and Ninth Amendments. In his view, the people are sovereign; the Constitution is an instrument for their common good. The right of privacy protects people's ability to make choices without government interference in their personal concerns and relationships. Douglas framed privacy opinions in broad humanitarian terms that continue to guide decisionmaking.

When Justice Douglas wrote his seminal decision in *Griswold v. Connecticut*, **381 U.S. 479 (1965)**, the Supreme Court had already decided several cases on privacy that addressed such spheres as people's right to live free of unreasonable searches and seizures, to refuse to provide self-incriminating testimony, and to preserve "the sanctity of" their "**home** and the privacies of life." The Court had also placed informational privacy within the realm of the First Amendment. Indeed, Justice Douglas had written a majority opinion in *Skinner v. Oklahoma* (1942) that found unconstitutional, on equal protection grounds, a state law calling for the **sterilization** of certain convicts; however, in it he never mentioned privacy, despite the "basic liberty" of procreation that was involved. He then connected the constitutional protection of liberties to "more than freedom from unlawful government restraint," to "privacy" and the "**right to be let alone**," in *Public Utilities Commission v. Pollack* (1952).

Douglas's majority opinion in *Griswold* analyzed whether the Constitution protected marital privacy. The case involved a constitutional challenge brought against a Connecticut law against using or counseling about the use of contraceptives. Douglas located the rights of married people to make reproductive decisions and associate without unnecessary governmental intrusion in the "penumbras" of privacy "formed by emanations from those guarantees that help give them life and substance." In his 1958 book *The Right of the People*, he explained that the "penumbra of the Bill of Rights" protected natural rights that "have a broad base in morality and religion to protect man, his individuality, and his conscience against direct and indirect interference by government." His reliance on constitutional penumbras was met with some resistance both within the Court and among academics. Justice Hugo Black rejected the decision because he could "find in the Constitution no language which either specifically or implicitly grants to all individuals a constitutional 'right to privacy.'" Similarly, several constitutional scholars, John Hart Ely and Herbert Wechsler being among the most prominent, have disparaged those constitutional decisions that rely on substantive principles to protect individual rights. Douglas, to the contrary, regarded certain vital rights to be derived "from the totality of the constitutional scheme under which we live" and determined that it was the Court's obligation to protect them against government interference.

Despite the criticism of privacy rights, most justices have found privacy intrinsic to the Constitution. Indeed, the more Douglas was able to pull the Court in the

direction of his thinking, the more willing he became to take controversial stands. In *Roe v. Wade*, 410 U.S. 113 (1973), which upheld a woman's right to terminate a pregnancy, Chief Justice Burger decided to assign the majority opinion to Justice Blackmun, who recognized the right to privacy "whether founded on the Fourteenth Amendment's concept of personal liberty and resting upon state action, or . . . on the Ninth Amendment reservation of rights to the people." Douglas's concurrence, agreeing with the Court's decision but assuming a different rationale for it, was one step ahead. To him, the Ninth Amendment was linked to the "'Blessings of Liberty' mentioned in the preamble to the Constitution." His concurrence set out spheres of privacy: The First Amendment protects the absolute right to "the autonomous control over the development and expression of one's intellect, interests, tastes, and personality." The state may exercise more control over the sphere of liberty pertaining to "freedom of choice in the basic decisions of one's life respecting marriage, divorce, procreation, contraception, and the education and upbringing of children."

In another sphere of privacy, the government must demonstrate a compelling state interest to limit the "freedom to care for one's health and person, freedom from bodily restraint or compulsion, freedom to walk, stroll, or loaf." Douglas's descriptions of freedoms related to individual rights intrinsic to living meaningful lives, not merely being left undisturbed by government interference. The Court has continued to rely on Justice Douglas's privacy formulation, most recently in finding that the right to privacy extends to homosexual couples in the landmark case *Lawrence v. Texas*, 539 U.S. 558 (2003).

Suggested Reading: Ashmore, Harry S. (ed.). *The William O. Douglas Inquiry into the State of Individual Freedom*. Boulder, CO: Westview Press, 1979; Douglas, William O. *Of Men and Mountains*. New York: Harper, 1950; Murphy, Bruce A. *Wild Bill: The Legend & Life of William O. Douglas*. New York: Random House, 2003; O'Fallon, James (ed.). *Nature's Justice: Writings of William O. Douglas*. Corvallis: Oregon State University Press, 2000; Simon, James F. *Independent Journey: The Life of William O. Douglas*. New York: Harper & Row, 1980.

Alexander Tthesis

Driver's Privacy Protection Act

The Driver's Privacy Protection Act (DPPA) was passed in 1994 to protect personal information collected by a state's Department of Motor Vehicles (DMV). As of the DPPA's 1997 deadline, it is illegal for any DMV to release information about any individual in their database. The DPPA was enacted to protect private individuals from organizations or individuals using **personally identifiable information** such as name, **Social Security number**, or addresses in order to harass individuals or to commit a robbery or other violent crime. Moreover, supporters of the law argue that the DPPA provides important protections of individuals' right to privacy that more than 30 states were failing to enforce before the bill was passed. Violators face criminal fines and civil liability suits that can provide victims with actual and punitive damages as well as reimbursement of legal costs. The law has been amended to include more specific protections and has also faced several state challenges. In 2000 the U.S. Supreme Court upheld its constitutionality despite state challenges that the act violates state commerce



laws, with other state courts ruling that the law protects an individual's data only within DMV databases.

The DPPA gained both public and legislative support after a series of highly publicized cases, including the death of actress Rebecca Schaffer, where individuals used information obtained through DMVs to commit crimes and engage in forms of harassment. An obsessed fan used DMV records to obtain Shaffer's address, after which he continued to stalk her and finally murdered her. Other cases involved Operation Rescue members using DMV records to harass women who visit doctors known to perform **abortions**. Although a few states had already passed laws that protected driver information, the DPPA created a federal standard restricting access to these records. The DPPA ultimately passed as an amendment to the Violent Crime Control and Law Enforcement Act of 1994 (103 H.R. 355). The law limits access to the database to certain agencies and limited purposes, including legitimate local, state, and federal government functions; matters of motor vehicle safety; theft; emissions issues; product recalls; and motor vehicle market research and surveys. Individuals and groups may also acquire access to databases for legitimate business transactions initiated to verify the accuracy of personal information, for anonymous research activities and preparation of statistical reports, for insurance-related applications, for use by licensed investigators or security services, for the benefit of private toll transportation facilities, and for use by anyone who has written permission from an individual to release his or her information (18 U.S.C. §2721). Ironically, although the bill limits individual and group access to drivers' information, the bill would not have protected Shaffer, as her killer used a **private investigator** to obtain her home address.

Due to the popularity of the DPPA, the "Shelby Amendment" was added, requiring DMVs to get written permission before they can release or sell a driver's personal record to a third party. This amendment requires marketers to obtain a driver's consent before acquiring personal information for mass mailings.

As mentioned earlier, the DPPA has faced several state challenges. Critics argue that it threatens state constitutional powers with its prohibition of lucrative state expenditures. Previously, states made over a million dollars from selling names in DMV databases. South Carolina challenged the DPPA in 1998, arguing that the law violated principles of federalism. However, the Supreme Court unanimously upheld the constitutionality of the act in 2000 as a proper exercise of Congress's authority to regulate interstate commerce under the Commerce Clause (528 U.S. 14). In 2001 *Davies v. Freedom of Information Commission* challenged the act as limiting the right to freedom of information. The Connecticut Supreme Court ruled that the DPPA does not apply to other government agencies that receive personal information from the state DMV in the course of their normal governmental functions.

Suggested Reading: Asseo, Laurie. "U.S. Supreme Court Case Driven by Privacy vs. States' Rights Debate," *Legal Intelligencer* (November 11, 1999): 4; Electronic Privacy Information Center. *The Driver's Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record*. <http://www.epic.org/privacy/drivers>. Online, December 2005.

Evelyn A. Clark

Drug testing

A drug test is a process whereby a bodily fluid or material—typically urine, blood, or hair—is analyzed to determine whether traces of drugs are present. Most drug metabolites can be detected in urine for up to three days after the drug was used; others are detectable for as long as four weeks after last use (e.g., marijuana used by heavy or chronic smokers). Two primary methods of detecting drugs in urine dominate the testing industry: immunoassays and chromatography. The Enzyme-Multiplied Immunoassay Technique (EMIT), the Enzyme-Linked Immunosorbent Assay (ELISA), and the radioimmunoassay (RIA) are among the most commonly used screening methods. With these methods, a given urine sample is compared with a calibrator containing a known quantity of the drug for which tests are being conducted. If the sample is equal to or higher than the calibrator, the test result is positive. Although reliability at one time was a significant problem, improvements have resulted in current accuracy levels of 95 to 99 percent.

The Gas Chromatography/Mass Spectrometry (GC/MS) technique is the most accurate for detecting drugs in body fluids. To date, courts accept screening tests as 100 percent accurate as long as they are followed by a GC/MS corroboration. Although confirmatory tests cost considerably more than initial screenings—\$40 to \$75—about 70 percent of employers require them. However, 13 percent of employers repeat the procedure (such as EMIT) on the same sample, 5 percent test a new sample, and 7 percent perform no confirmatory test (and simply disqualify applicants or respond otherwise to positive-testing employees). Today there are over a dozen initial screening tests accepted by the scientific community, although three tests dominate private, public, and military applications: EMIT, RIA, and Thin-Layered Chromatography (TLC).

Although **urine analysis** is the testing procedure most commonly used, hair follicle testing, which is much more precise in detecting the long-term presence of drugs, is becoming more accepted. As the cost of hair testing decreases and as courts rule on its validity and reliability, hair rather than body fluids likely will become the preferred specimen for private and public agencies. Urine testing generally reveals drugs consumed within the past two or three days, and **blood testing**, which reveals current impairment, discloses drug use within the past 2 to 22 hours. Hair testing, by comparison, exposes drug use as distant as two months prior to testing, allowing greater surveillance of people's previous behaviors. Saliva testing also will likely become more widely used. A number of companies are manufacturing saliva testing mechanisms designed for the workplace as well as for criminal justice agencies, drug rehabilitation clinics, and hospital emergency and psychiatric wards. Their on-site advantages are also contributing to recent discussions about their potential for testing motorists during traffic stops. Drug metabolites in body sweat are tested for by means of a patch worn on the skin and are most commonly used with individuals on probation or parole. In time and with the development of increasingly sophisticated and less expensive techniques for drug testing, biological information other than that gleaned from urine may become preferred.

Drug testing in the United States was first imposed on those who had relinquished some of their personal liberties: members of the armed forces and jail inmates and **prisoners**. Since 1981 the military has conducted over a million urine analyses each year. About 71 percent of jails practice **surveillance** of inmates with



the use of drug testing procedures, and about 49 percent of adult probationers are subject to routine screening.

However, drug testing has quickly expanded to include individuals previously exempt. Workers and job applicants have been the main subjects. Students have been targeted as well, although to lesser extent. The drug testing industry has grown nearly exponentially because of its aggressive marketing strategies, and this growth has been accelerated by political campaigns, as well as judicial, executive, and legislative decisions.

On September 15, 1986, President Ronald Reagan issued Executive Order 12564: Drug-Free Federal Workplace, effective immediately. It required screening employees and job applicants, through testing, for illegal drug use. The order called for mandatory random testing in all agencies of the executive branch. Congress soon passed legislation requiring testing programs among federal agencies. The broadest action for private employees was the passage of the Drug-Free Workplace Act of 1988 (P.L. No. 100-690, Nov. 18, 1988), which requires employers with federal contracts worth at least \$100,000 and any recipient of a federal grant to institute a comprehensive “drug-free workplace” program. Although comprehensive, the act did not require employers to test employees or applicants.

On October 28, 1991, President George Bush signed the Omnibus Transportation Employee Testing Act of 1991 (P.L. No. 102-143, Oct. 28, 1991), stipulating the testing of employees in the Federal Aviation Administration, the Federal Highway Administration, the Federal Railroad Administration, and the Urban Mass Transportation Administration. The act, among other things, added alcohol to the list of drugs targeted for testing. This act preempted state laws and authorized both random and pre-employment drug and alcohol testing.

In challenges to drug testing policies, courts have weighed an individual’s “**reasonable expectation of privacy**” against the interests of public safety and security. Although privacy rights are not mentioned in the United States Constitution, the Supreme Court has ruled that they are implicit in the Bill of Rights and specifically the Fourth Amendment. Most challenges to drug testing have relied on issues of privacy and unreasonable searches. In 1989 the Supreme Court upheld a California District Court ruling that railroad workers can be subjected to random drug testing. The ruling, that drug testing is a reasonable search that does not violate the Fourth Amendment, affected public employees working for federal, state, county, and municipal governments (*Skinner v. Railway Labor Executives’ Ass’n*, **489 U.S. 602, 109 S.Ct. 1402, 1989**). Private employees were unaffected by the ruling since they, unlike public-sector workers, have no constitutional protection from searches and seizures from their employers. Writing for the majority, Justice Anthony Kennedy also upheld the use of the EMIT and GC/MS drug testing procedures (the ones most commonly used), claiming that they are “highly accurate.”

On the same day as the *Skinner* ruling, the Court, in a 5-4 decision in *National Treasury Employees Union v. Von Raab*, 109 S.Ct. 1384 (1989), held that Customs Service agents, like railroad workers, are subject to drug testing and that such procedures do not violate Fourth Amendment protections. The Court considered the necessity of agents having unimpeachable integrity along with the needs of the government, national security, and public safety. Writing for the minority in the *Von Raab* case, Justice Scalia stated that even “school crossing

guards” would be subject to drug testing under this ruling. Only six years later, in 1995, the Court upheld the testing of junior high school student-athletes, citing the existence of reasonable suspicion that student-athletes were both using and promoting drug use (*Vernonia School District v. Wayne Acton*, 515 U.S. 646, 1995). In June 2002, in a 5-4 decision, the Supreme Court, in *Board of Education of Independent School District Number 92 v. Earls*, upheld a drug testing program in Tecumseh, Oklahoma, compelling students who participate in any extracurricular activities (including the school choir, the marching band, and the academic team) to submit to urine tests. A positive finding or refusal to comply results in expulsion from extracurricular activities for the academic year.

Since 1989 federal circuit courts generally have relied on the *Skinner* ruling when upholding drug testing. Courts likewise have ruled that pre-employment drug testing does not violate Fifth Amendment guarantees. The Fifth Amendment protects individuals from being compelled to testify against themselves. The argument is that public-sector employers violate employees’ Fifth Amendment rights by subjecting them to drug testing, the results of which may be incriminating. Courts, however, have sided with employers over employees on two grounds. First, courts have ruled that the Fifth Amendment is limited to the government compelling individuals to *testify* against themselves. Requiring physical evidence such as blood, urine, and hair samples rather than the testimony of individuals is not considered a violation of their Fifth Amendment guarantees. Second, courts have ruled that the Fifth Amendment protects against self-incrimination only in *criminal proceedings*—processes that exclude drug testing.

These decisions in the executive, legislative, and judicial branches cleared the way for the wholesale adoption of workplace drug testing. States passed legislation creating drug-free workplaces and offering financial incentives to employers that participate. Some states offer employers credits on their workers’ insurance policies. Others support employers through public policies. For example, in the discharge of employees who are in violation of drug-free workplace programs, employers’ actions are considered reasonable and “for cause.” States also have shifted the legal burden of proof from employers to employees who are injured on the job and whose post-accident (and mandatory) drug screening results are positive. Thus, employers have a financial incentive directly from their states of residence to implementing drug-free workplace programs. Among companies that subject employees to drug testing, 53 percent do so because of government mandates and incentives.

Workplace drug testing increased from 21.5 percent of companies in 1987 to 84.8 percent of companies in 1993—a 250 percent increase. Drug testing has now leveled off or has decreased slightly, primarily among small businesses. Among Fortune 500 companies, about 40 percent of employees are subject to drug testing compared with 48 percent among Fortune 1000 firms. The larger the company, the more likely it is to use drug testing surveillance on applicants and employees. About 71 percent of worksites with more than 1000 employees conduct drug tests while 40 percent of worksites with 50 to 99 employees screen for drugs. Among companies with fewer than 50 employees, only 2 percent require drug testing.

The prevalence of drug testing varies widely by industry type. Blue-collar workers are much more likely to be subjected to drug testing than white-collar employees.



The workers most likely to be subjected to drug and alcohol screening are non-college-educated males who are full-time employees and union members. Drug testing varies by geographic region as well, with the southern United States reportedly conducting more drug testing than any other area in the country. Most drug testing programs require the worker or job applicant, in the presence of a monitor, to urinate into a specimen cup.

Employers currently rely on a number of procedures for testing both employees and those seeking work. Pre-employment testing (i.e., testing of job applicants) is considered a preventive strategy for employers since it denies employment to applicants identified as drug users. Pre-employment testing is the most broadly used type; 78 percent of companies require applicants to comply. Random or unannounced testing is designed to ferret out current drug users. It has become the most common testing procedure among current employees, with 46.7 percent of worksites using this method. It also remains the most controversial, as employees define it as an invasive procedure requiring no probable cause. Reasonable-cause testing is used when an employee's job performance suggests possible drug use. Since the legal stakes are higher for this type of testing, employers are cautioned to use it judiciously. Even with the recognized potential for litigation, it is the second most common testing procedure on employees, with 37 percent of worksites using this method. It also produces the highest percentage of positive findings. Post-accident testing is used in cases where employees have been involved in on-the-job accidents. Although employees may display no signs of inebriation or of being under the influence of alcohol or drugs, employers nonetheless test employees after on-the-job accidents. About 26 percent of worksites use this form of testing. Periodic testing is used on a regular schedule, usually in conjunction with physical examinations, which are required of some employees in specific occupations. Since employees must be given advance notice of such exams, few employees test positive, and only 13.7 percent of worksites use this procedure. Rehabilitation testing is used with employees who earlier tested positive and as a condition of continued employment are required to participate in counseling and periodic drug testing to monitor their sobriety and abstinence. Most current drug testing programs are designed to test all employees (e.g., random testing) and job applicants (e.g., pre-employment screening). Pre-employment screening currently is the most commonly used type of drug testing. Seventy-eight percent of companies require job applicant drug testing.

The drug testing industry is the quintessential example of modernity. The profound faith in technology, underlying philosophy of surveillance, ability to rapidly process large numbers of samples, and confidence in science as a means of social control characterized by the industry suggest modern strategies and ideologies for addressing complex social issues. Drug testing—the social surveillance of students, military personnel, prisoners, job applicants, and workers—is a component of general and dynamic processes of social control. Drug testing represents a fundamental shift in social relations and is one of an increasing number of intrusions into privacy. Previous generations of workers, students, military men and women, and inmates were subject to surveillance, yet control methods today are far more efficient, and many rely on biological science.

These modifications in some respects reflect changing technologies that offer heretofore unknown surveillance modes and strategies. In other words, they may be technologically determined modes of control. They also are part of larger surveillance-related developments in people's everyday lives, and particularly in the workplace. Beyond lengthy background investigations; several rounds of interviews; and polygraph, integrity, physical, and psychological screening, drug testing has quickly become a primary technique for distinguishing the reputable from the disreputable. As a means of differentiating, it is considerably less expensive than **background checks** or physical or psychological investigations. Also, its results, unlike those of polygraph exams, are admissible in court. Given drug testing's widespread use, it has become standard operating procedure in innumerable private and public settings.

See also: **Constitutional protections; Workplace privacy**

Suggested Reading: Coombs, Robert H., and Louis Joylon West (eds.). *Drug Testing: Issues and Options*. New York: Oxford University Press, 1991; Garland, David. *The Culture of Control*. Chicago: University of Chicago Press, 2001; Gilliom, John. *Surveillance, Privacy, and the Law*. Ann Arbor: University of Michigan Press, 1994; Lyon, David. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press, 1994; Staples, William G. *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. Landham, MD: Rowman & Littlefield, 2000; Tunnell, Kenneth D. *Pissing on Demand: Workplace Drug Testing and the Rise of the Detox Industry*. New York: New York University Press, 2004.

Kenneth D. Tunnell

E



Eavesdropping. *See* **Electronic surveillance; Manners**

***Eisenstadt v. Baird*, 405 U.S. 438 (1972)**

The Supreme Court case of *Eisenstadt v. Baird* began when William Baird gave away Emko vaginal foam to a woman following a Boston University lecture on birth control and overpopulation. Massachusetts charged Baird with a felony: distributing contraceptives to unmarried men or women. Under the law, only married couples could obtain birth control products, and only registered doctors or pharmacists could provide them. Baird was not an authorized distributor of contraceptives.

At the time, Massachusetts General Laws provided for a maximum five-year term of imprisonment for anyone who “gives away . . . any drug, medicine, instrument or article whatever for the prevention of conception,” except as prescribed by a registered physician for any married person. The State Supreme Judicial Court’s interpretation was that the violation of these provisions made it a felony for anyone, other than a registered physician or pharmacist acting in accordance with a physician’s order, to dispense any article with the intention that it be used for the prevention of conception.

According to the Supreme Court, the legislative purposes the statute was meant to serve were not altogether clear. In a previous decision, the State Supreme Judicial Court noted only the state’s interest in protecting the health of its citizens. In another decision the court found a second and more compelling ground for upholding the statute: to protect morals through “regulating the private sexual lives of single persons.” The Court of Appeals, however, did not consider the promotion of health or the protection of morals through the deterrence of fornication to be the legislative aim. Instead, the court concluded that the statutory goal was to limit contraception in and of itself. The court held that this purpose conflicted “with fundamental human rights” under *Griswold v. Connecticut*, 381 U.S. 479 (1965), where the Court struck down Connecticut’s prohibition against the use of contraceptives as an unconstitutional infringement of the right to marital privacy.

In *Eisenstadt*, the question the Court dealt with was, did the Massachusetts law violate the right to privacy acknowledged in *Griswold v. Connecticut* and protected from state intrusion by the Fourteenth Amendment?



In a 6-to-1 decision, the Court struck down the Massachusetts law, although not strictly on privacy grounds. The Court held that the law's distinction between single and married individuals failed to satisfy the "rational basis test" of the Fourteenth Amendment's Equal Protection Clause. Married couples were entitled to contraception under the Court's *Griswold* decision. Withholding that right from single persons without a rational basis proved the fatal flaw. Thus, the Court stepped away from the emphasis on marital privacy in *Griswold* to uphold a less restrictive right to privacy and to invalidate the Massachusetts statute. "If the right of privacy means anything," wrote Justice William J. Brennan, Jr., for the majority, "it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision to whether to bear or beget a child."

See also: **Family; Gender; Reproductive rights; *Roe v. Wade*, 410 U.S. 113 (1973); *Webster v. Reproductive Health Services*, 492 U.S. 490 (1989); Women and privacy**

Suggested Reading: Alderman, Ellen, and Caroline Kennedy. *The Right to Privacy*. New York: Alfred A. Knopf, 1995; Allen, Anita, and Erin Mack. "How Privacy Got Its Gender," *Northern Illinois University Law Review* 10 (1990): 441–454; Allen, Anita, and Erin Mack. *Uneasy Access: Privacy for Women in a Free Society*. Totowa, NJ: Rowman & Littlefield, 1988; Allen, Anita, and Erin Mack. *Why Privacy Isn't Everything: Feminist Reflections on Accountability for Private Life*. Lanham, MD: Rowman & Littlefield, 2003; Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won Before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Bodemheimer, Davis J., and James W. Ely, Jr., eds. *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993.

Tod J. Beavers

Electronic Communication Privacy Act of 1986

Electronic surveillance is a significant tool in modern law enforcement, bringing dimension to dialogues, minimizing interpretation ambiguity, and making recollection issues obsolete. When used appropriately, it has the power to bring down the most elusive criminals. There is little wiggle room for a defendant whose words are captured on tape. If used inappropriately, **surveillance** has the power to invade our privacy, stifle our creativity for fear of being exposed as different, and share our secrets with those who have no need to know. Mindful of the balance that must be struck between law enforcement's need to intercept the communications of wrongdoers and an individual's right to be free of unwarranted eavesdropping, the legislature enacted the Omnibus Safe Streets and Crime Control Act of 1968 and the Electronic Communication Privacy Act (ECPA) of 1986.

The ECPA consists of three subtitles and covers three specific types of communications: wire, oral, and electronic. The three subtitles are Title I, the Wiretap Act, which deals with the interception of communications that are in transmission; Title II, the Stored Communications Act, which covers the accessing of stored electronic communications and records; and Title III, the **Pen Register** Act, which applies to pen registers and trap-and-trace devices, which record phone numbers or address information (such as the "to" and "from" lines in an e-mail).

The types of communications covered by the ECPA are wire, oral, and electronic. A wire communication involves aural transfers, which are communications containing the human voice that travel through a wire or cable device at some point during their transmission. A landline or mobile telephone conversation taking place in real time is an example of this type of communication. An oral communication is one uttered by a person under circumstances such that the person has a reasonable expectation that the communication will not be overheard. In other words, the communicator must have a reasonable expectation of privacy in his or her conversation and the communication must be one that society is willing to protect. This definition applies to communications intercepted through bugs or other recording devices such as tape recorders that do not involve a wire transmission. Finally, electronic communications include all non-wire and non-oral communications: signals, images, and data that are transmitted through a medium such as wire, radio, electromagnetic, or photoelectronic. Prime examples of electronic communications are **electronic mail** messages, faxes, (electronic) pages, and text messages.

The extent to which audio and electronic communication surveillance occurs is reported annually to Congress through the Administrative Office of the United States Courts. Specifically, the Omnibus Crime Control and Safe Streets Act of 1968 requires that certain information—including the number and nature of federal and state applications for orders authorizing or approving the interception of wire, oral, or electronic communications; the offenses under investigation; the locations of intercepts; the cost of the surveillance; and the numbers of arrests, trials, and convictions that were a direct result of such surveillance—be reported annually. The 2004 report concluded that 1710 intercepts were authorized that year by state and federal courts, which was an increase of 19 percent compared with the number in 2003. Of the 47 jurisdictions (federal, state, the District of Columbia, and the Virgin Islands) that currently authorize this type of surveillance, 20 reported using it during 2004 as an investigative tool. Furthermore, the report showed that federal officials requested 730 intercept applications in 2004, which amounted to a 26 percent increase over the number requested in 2003.

Historically, **wiretapping** laws have required the consent of all parties before a communication could be intercepted. An example of a situation involving the consent of all parties is the use of a telephone answering machine. The machine owner has given his consent by attaching the machine to his phone and asking the caller to leave her message after the beep. The caller has given her consent to be intercepted by recording her message. Thus, both parties to the communication gave prior consent for the content of the interception to be captured.

Federal law and 35 states allow for the interception of wire communications if only one of the parties to the communication has given prior consent. However, the conditions for interception still vary significantly from jurisdiction to jurisdiction. For example, jurisdictions may define the term “party” as anyone involved a conversation or as law enforcement personnel only. Jurisdictions may limit the offenses for which interception is permissible to select crimes. Some jurisdictions limit the ability to record the intercepted communications. Some jurisdictions may allow interception for reasons of officer safety but for no other purpose, including its use as evidence in criminal or civil matters. Some jurisdictions may allow the interception of communications that are part of a videotaped car stop.



The ECPA requires law enforcement to obtain a court order with an accompanying affidavit based on an extensive list of legal requirements before the content of a communication can be captured. The list is extensive because wiretap surveillance poses a greater threat to privacy than the physical searches and seizures covered by the Fourth Amendment. Interception inevitably captures some communications of non-targets whether or not their communication is relevant to the investigation. Not every communication of a criminal suspect is criminal in nature. Further, unlike the typical **search warrant**—where officers announce, enter, search, and exit—electronic surveillance is conducted surreptitiously and is ongoing until the objectives of the investigation are met. In some cases the monitoring continues for months and involves thousands of communications.

The list of legal requirements includes proper authorization from the appropriate official; identification of the investigators, the crimes, and the parties to be intercepted with specificity; tripartite probable cause; a full and complete statement of the facts and circumstances relied on by the applicant to justify the belief that the order should be issued; the goals of the interception; the length of time for the interception, including when it will begin and end, the actual hours of interception per day, and the days of the week of interception; exhaustion and necessity; minimization; and the equipment and technology to be employed.

All electronic surveillance statutes require tripartite probable cause demonstrating a link between the interceptee, the device intercepted, and the offense. Specifically, before an *ex parte* order approving a wiretap may be issued, the judge must determine that (1) there is probable cause for belief that an individual is committing, has committed, or is about to commit certain enumerated offense(s); (2) there is probable cause to believe that communications relevant to the particular offense(s) will be intercepted; and (3) there is probable cause to believe that the facilities (devices) from which the communications will be intercepted are being, or are about to be, used in connection with the commission of the offense(s) or that they are commonly used, leased, or listed under the name of a person connected with the alleged offense(s). The standard for review of tripartite probable cause is exactly the same as that required by the Fourth Amendment for a search warrant. Therefore, courts are bound to consider only the facts contained within the four corners of the affidavit.

All electronic surveillance statutes require the issuing judge to review the affidavit to determine whether normal investigative procedures have been tried but failed, reasonably appear to be unlikely to succeed if they were tried, or are too dangerous. To satisfy this requirement (commonly referred to as the necessity/exhaustion requirement), the affidavit cannot be merely a boilerplate recitation of the difficulties of gathering usable evidence. The affidavit must include a complete statement providing detailed information about all prior interceptions on the named interceptees and the facility or device to be intercepted. It also must include all pertinent information relevant to the investigation, including possibly exculpatory information. However, some discretion is allowed in terms of disclosing the evidence in less than its entirety to establish probable cause, provided there is no effort to mislead the court toward approving a warrant that might otherwise not have been issued. For example, it has been held acceptable for the government to withhold information to protect the **confidentiality** of informants.

In evaluating the good faith efforts regarding the use of alternative methods of investigation, a reviewing court is guided by reasonableness; the police need not exhaust all conceivable techniques. Before granting the wiretap application, however, the issuing judge must determine that standard investigative techniques employing a normal amount of resources have failed to do the job within a reasonable period of time. Essentially, all that is required is that the investigators give serious consideration to non-wiretap techniques prior to applying for wiretap authority and that the court be informed of the reasons for the investigators' belief that such non-wiretap techniques have been or will likely be inadequate. In other words, the government must make a reasonable good faith effort to run the gamut of normal investigative procedures before employing an electronic surveillance technique. Other investigatory techniques typically employed are dialed number recorder (DNR)/trap-and-trace analysis; surveillance, mobile and stationary; trash or **garbage** runs; use of informants; criminal history checks; execution of search warrants; a grand jury investigation; use of **surveillance cameras**, mobile tracking devices, and pole cameras; toll record analysis; undercover investigations; and clone pagers.

The ECPA also requires that the interception of oral communications through wiretapping be conducted in such a way as to minimize the interception of communications not otherwise subject to interception. Interception is proper only if it is necessary to achieve the goals of the authorization. This does not require that all innocent or unrelated communications remain unmonitored. Rather, the statute requires that unnecessary intrusions on the privacy of the individuals being lawfully monitored be minimized to the greatest extent possible. Compliance is determined using a case-by-case reasonableness standard. Specifically, a minimization inquiry is not to be made in a fragmented manner, considering each interception alone. Instead, it requires an examination of the totality of the monitoring agents' conduct for the duration of the authorized interception. Minimization is satisfied if, on the whole, the agents have shown a high regard for the rights of privacy and have done all they reasonably could to avoid unnecessary intrusion.

The burden of proof for minimization is initially on the government to make a *prima facie* showing of compliance; the burden then switches to the defense for production and persuasion. The compliance standard for minimization is the overall reasonableness of the totality of the conduct of the monitoring agents in light of the purpose of the wiretap and the information available to the agents at the time of the interception. The more complex and widespread the investigation, the wider the latitude of eavesdropping allowed. Factors involved in this reasonableness determination include: the sophistication of the suspects and the counter-surveillance methods; whether coded conversations are used; the location and operation of the target telephone or device; the extent of judicial supervision; the duration of the wiretap; the purpose of the wiretap; the length of the calls monitored; the existence, or lack thereof, of a pattern of pertinent calls; the absence of privileged interceptions; and the proper handling of interception of windfall or other offenses.

The wiretap statute contains its own exclusionary rule providing that no intercepted communications, wire or oral, can be received in evidence if the communications were unlawfully intercepted, if the order was insufficient, or if the interception was not made in conformity with the order. Due to this clear legislative



intent to limit surveillance in order to protect privacy issues and to control law enforcement surveillance, a substantial compliance standard is mandated by most courts for each provision of the statute that is deemed to be a central or functional safeguard factor. In short, only surveillances that are narrowly focused with constitutionally acceptable, pre-approved judicial sanctions based on special showings of need are permissible.

The Stored Communications Act (SCA) (18 U.S.C. 2701–2711) governs law enforcement's access to stored, or temporarily stored, wire and electronic communications. This includes any backup copies of files in temporary electronic storage. Accordingly, it governs access to the subscriber records of various communications service providers, including Internet service providers (ISPs). If a communication is being transmitted from its origin to a destination, then the Wiretap Act applies. If it is stored in the computer of a provider of an electronic communication service (ECS) or a remote computing service (RCS), then the Stored Communications Act governs.

The Stored Communications Act is much less protective than the Wiretap Act. It includes no exclusionary provision and no minimization requirement, and it allows for little judicial supervision. The degree of privacy protection afforded customers and subscribers depends on whether the stored communication is considered content or non-content information and whether it is housed by an ECS or RCS provider. In determining whether the information sought is content or non-content, experts usually make the analogy to mail. The content is the actual letter, and the non-content is the envelope. Telephone companies and electronic mail companies generally act as ECS providers and a company's or university's server represents an RCS.

The SCA is not a catch-all statute designed to protect the privacy of all stored communications. It does not cover information stored on home computers, since that information is protected by the Fourth Amendment. The SCA protects only information held by third-party providers. It is essentially a Fourth Amendment type of protection for computer networks. The statute limits the government's ability to compel providers to disclose information stored by an ECS or RCS about their customers and subscribers.

Specifically, the statute restricts the ability of service providers, including ISPs, to voluntarily disclose information about their customers and subscribers to the government. (The Fourth Amendment is not applicable here because it would allow private providers to make such **disclosures** to third parties under the knowing exposure doctrine.) The SCA is a legislative attempt to protect the privacy of an individual's content information electronically stored by third parties. The Act mandates that some official action be taken before the disclosure can occur unless it falls within one of the eight specifically designated exceptions listed in 18 U.S.C.2702(b), including disclosure to the recipient of the communication, to the National Center for Missing and Exploited Children in connection with a report, and to a consenting originator.

The type of official action required for disclosure depends on whether the information is content or non-content, whether it is stored for less or more than 180 days, and whether the information is held by an ECS or RCS provider. A warrant is necessary to compel an ECS provider to disclose the contents of communications held in storage for 180 days or less (18 U.S.C. 2703(a)). To force an ECS provider to disclose content in electronic storage for more than 180 days or to compel an

RCS provider to disclose content at any time, the government has several options: a search warrant, with no notification to the subscriber or customer (18 U.S.C. 2703(b)); a court order combined with prior notice to the subscriber or customer (which can be delayed in some circumstances) (18 U.S.C. 2705); or an administrative, grand jury, or trial subpoena with prior notice to the subscriber or customer (18 U.S.C. 2703(b)).

A court order requires that the government provide specific and articulable facts showing that there are reasonable (not probable) grounds to believe that the information sought is “relevant and material to an ongoing criminal investigation” (18 U.S.C. 2703(d)). A subpoena requires only that the government is seeking relevant information and that the request is not overly broad.

Non-content, or envelope-type, information may be disclosed more readily through a mere subpoena, as it is deemed less private than content information. Many argue, however, that non-content disclosure does reveal private information. From the packaging of mail delivered to a home, one can identify an individual’s doctors, interests, associates’ names, political affiliations, and perhaps sexual preferences; a subpoena is all that is required. Non-content information amounts to basic subscriber information of the sort included in pen register data: name; address; local and long-distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and the means and source of payment for such service (including any **credit card** or bank account numbers) (18 U.S.C. 2703(c)(2)).

The Pen Register Act regulates the government’s use of pen registers and trap-and-trace processes. Pen registers provide real-time information as to the date and time the phone is off hook, numbers dialed, the date and time a call is terminated, the duration of the call and, if it is an incoming call, whether it was answered. Trap-and-trace processes capture in real time the telephone number of the device calling the target phone (caller ID). Trap-and-trace devices are geographically limited in scope.

Pen registers are not protected by the Fourth Amendment. A person has no reasonable expectation of privacy in terms of this information because the information is available and accessible to a third party, such as the telephone company. Furthermore, pen registers presumably capture only non-content information. Although the installation and use of a pen register does not constitute a search under Fourth Amendment criteria requiring a warrant, most jurisdictions, including federal jurisdictions, require a court order before installation. The order required is of the type described under the SCA, certifying that the information sought is relevant and material to an ongoing criminal investigation. Certification by the government means only that the information likely to be obtained is relevant to the investigation. Thus, the court order should include the identity of the law enforcement officer making the application, the identity of the agency conducting the investigation, and a statement under oath by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the agency.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT



Act) expanded the definition of pen registers and trap-and-trace devices to include addressing information on e-mails and to Internet Protocol (IP) addresses. Whereas previously pen registers recorded only numbers dialed on the telephone line, the definition now includes all forms of transmission (“dialing, routing, addressing, or signaling information”). The effect of this change is that e-mail headers (i.e., the address information), IP addresses, and Uniform Resource Locators (URLs) now fall under this definition. The concern is that the information revealed from IP addresses and URLs is more content-like than non-content-like. IP addresses and URLs reveal significant information about users, including what their interests are and where they shop. This concern has not been addressed to date.

In summary, a court order certifying that the information likely to be obtained by such installation and use is relevant to an ongoing investigation is all that is required for its release. The orders can last up to 60 days and are not reviewed. This differs greatly from a warrant, where a return is required. Neither the Stored Communications Act nor the Pen Register Act contains an exclusionary rule. Thus, an individual has no recourse when the government illegally collects information.

Suggested Reading: Dash, Samuel, Richard Schwartz, and Robert Knowlton. *The Eavesdroppers*. New Brunswick, NJ: Rutgers University Press, 1959; Dempsey, James X. “Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy,” *Albany Law Journal of Science & Technology* 8 (1997): 70–71; Diffie, Whitfield, and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press, 1999; Electronic Privacy Information Center. <http://www.epic.org>. Online, March 2006; Goldberg, Carole. *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security*. New York: W.W. Norton, 2002.

Jill Joline Myers

Electronic mail

Electronic mail (“e-mail”) refers to messages transmitted through the **Internet** or some other network. In modern implementations, e-mail messages are usually delivered very quickly, although not quite in real time, unlike instant messaging (IM) and similar communication methods. Internet users commonly treat e-mail as the online equivalent of postal mail, unaware of its implications for privacy and security.

Third-party monitoring of e-mail is commonplace and can occur without the knowledge of either party to a communication. Other privacy issues relate to the technical mechanisms employed by marketers and others to monitor the reception and disposition of e-mail messages, the storage and retention of e-mail messages, and the actions of individual e-mail users. In addition, e-mail is commonly used to transmit intrusive and unwanted advertisements and other unsolicited messages called **spam**.

The standard protocol for sending Internet e-mail is the Simple Mail Transfer Protocol (SMTP). The Post Office Protocol version 3 (POP3) and the Internet Message Access Protocol (IMAP) are the most common protocols used for accessing received e-mail messages. Typically, the sender uses e-mail client software to compose a message. That software then transmits the message through an SMTP server, usually one operated by the sender’s own Internet access provider, which

transmits the message to an SMTP server designated to receive messages on behalf of the recipient. The message is held there until it is retrieved by the recipient.

The header of a message and its envelope both contain addressing information, although most e-mail clients display only the header. The “from” and “to” fields in the header normally contain the e-mail addresses of the sender and recipient, respectively, and sometimes their names as well. However, these fields do not control the delivery of a message, and they can easily be altered by the sender. Another means of concealing the address of a recipient (for example, from other recipients) is to place it in the “bcc” (blind carbon copy) field rather than the “to” field. In 2001 a large pharmaceutical manufacturer sent a form e-mail message to hundreds of consumers who had agreed to receive e-mail reminders about an antidepressant drug. The company inadvertently included the recipient’s address in the “to” field instead of the “bcc” field, causing all of the addresses to be exposed to each recipient.

Extensions to the SMTP protocol can be used to authenticate the source of a message or encrypt its content. E-mail messages may be sent pseudonymously or anonymously by routing them through a remailer that strips or alters identifying information before forwarding each message and, optionally, encrypts the message content.

An e-mail message may be sent in plain text or in various enhanced formats such as HTML, and may include file attachments and (depending on the format) embedded images and even program code. Current e-mail clients may disable certain enhanced features because of their privacy and security implications. For example, a sender may embed a link to an image located on the sender’s web server in an HTML e-mail message in order to monitor whether and when the message is opened or previewed by the recipient. If the recipient’s e-mail client were to retrieve the image from the sender’s web server and display the message, the access log for that server would reveal the date and time that the message was opened, the IP address from which the image was requested, and other information the sender might find useful.

Some e-mail systems provide senders with the ability to track delivery of messages, control message retention or forwarding, and even recall messages after they have been sent. Although standard Internet e-mail does not intrinsically support these functions, they can be implemented by e-mail client software or various work-arounds.

User actions can have many privacy-related consequences, often unintended. For example, an e-mail message can be forwarded by its recipient to a third party without the sender’s knowledge or consent. Although such forwarding may be considered a breach of “netiquette,” e-mail users may give little thought to the original sender’s privacy or other rights in the message content. A related concern arises when a forwarded message contains the e-mail addresses of many other recipients, who may not be aware that their addresses are being circulated widely.

The “reply to all” function available in many e-mail clients causes the user’s reply to be directed to all of the recipients of the original message as well as its sender. Frequently, users will inadvertently use “reply to all” when intending only a private “reply.” Similarly, a subscriber to an Internet mailing list who desires to respond only to the individual who posted a particular message may inadvertently send a reply to the entire list either by using the “reply to all” function or (if

the listserver is configured to direct replies to the entire list) by merely selecting “reply” without first checking the “reply-to” address in the posted message.

A different user error led to unanticipated consequences in *McVeigh v. Cohen* (1998). A noncommissioned naval officer mistakenly used the wrong AOL account name when sending a message to the wife of a fellow crew member. The account name he used was linked to a profile that listed his marital status as “gay.” The Navy then initiated discharge proceedings for homosexual conduct, based on the statement in his online profile, although a court later enjoined the proceedings.

In the United States, federal laws protect the privacy of e-mail. The most important of these, the **Electronic Communication Privacy Act of 1986 (ECPA)**, makes it illegal to intercept an e-mail message. This prohibition applies to law enforcement officials as well as private entities. However, there are many exceptions to this prohibition; for example, an e-mail service provider may view messages when necessary for purposes related to the operation of the service.

In *United States v. Councilman* (2005), the United States Court of Appeals for the First Circuit ruled that the interception provisions in ECPA apply to e-mail in temporary, transient storage. In *Councilman*, an Internet service provider routinely scanned its customers’ e-mail in order to obtain a commercial advantage. The court rejected the provider’s claim that a less protective standard should apply to e-mail messages in temporary storage than to those “in transit.”

Law enforcement officials can access e-mail messages with a warrant or court order, and in some instances even without an order or warrant. Such access was expanded under the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)**, enacted in the aftermath of 9/11. In 2000 it was revealed that the **Federal Bureau of Investigation (FBI)** had developed an automated system for scanning e-mail messages using hardware and software installed at the premises of a suspect’s Internet service provider. The system, originally named **Carnivore** and later renamed DCS1000, was widely criticized by privacy advocates and civil libertarians. Critics charged that the system would facilitate broad privacy violations and lacked accountability; the FBI claimed that it protected privacy by intercepting only those communications that were within the scope of a court order. The government had effectively abandoned Carnivore by 2003, although other mechanisms for intercepting and monitoring e-mail remain in use.

A seemingly nonobjectionable exception to ECPA permits the interception of e-mail with the consent of the sender or recipient. Some Internet providers routinely require such consent as a term of service, however, and courts generally have held that an employer has the right to access messages sent or received using its e-mail systems, at least if the employer has informed employees that their e-mail will be monitored. Surveys of employers in the United States reveal that monitoring of employee e-mail has become the rule rather than the exception, especially at larger firms.

In *Smyth v. Pillsbury Co.* (1996), a federal court in Pennsylvania rejected an employee’s claim that he had been wrongfully discharged on the basis of “inappropriate and unprofessional comments” he had made in e-mail messages to his supervisor. The company had assured its employees that their e-mail would be **confidential** and that the company would not intercept it or use it as grounds for termination or reprimand. The court held that the employee had lost any **reasonable**

expectation of privacy in regard to his comments when he sent them over the company's e-mail system, and that the company's interception of his messages was not a substantial invasion of his privacy.

Storage and archiving of e-mail messages can greatly increase the likelihood that third parties will gain access to their content. Declining data storage costs have removed much of the incentive to delete unneeded messages, while technological advances have made it easier to recover messages that have been deleted and those that exist only in otherwise obsolete backup archives. Meanwhile, businesses increasingly are adopting uniform policies on electronic document retention, largely in response to changes in the legal environment.

In *Zubulake v. UBS Warburg LLC* (2004), an employment discrimination case against a large investment brokerage firm, employees of the firm had deleted e-mail messages relevant to the case even after being instructed to retain them by the firm's lawyers. Many of the relevant messages eventually were retrieved, and the court instructed the jury to infer that the remaining missing messages contained material damaging to the firm's case. The plaintiff ultimately won damages of nearly \$30 million.

In *Arthur Andersen LLP v. United States* (2005), the Supreme Court reversed Arthur Andersen's conviction for obstruction of justice, which was based largely on the accounting firm's destruction of electronic records. Legislation enacted in the wake of the Enron/Andersen scandal has imposed stricter document retention requirements on businesses, particularly in the banking and financial services sector.

Individuals with personal e-mail accounts also have privacy interests that are affected by the storage and retention of e-mail. In 2004, when Hotmail and other web-based e-mail providers generally offered fairly limited storage capacities, Google's GMail service began offering 1 GB in free storage along with advanced search capabilities, encouraging users to keep old messages rather than deleting them to free up space. Although Google's privacy policy limits the use and **disclosure** of stored e-mail messages, it is clear that long-term retention of e-mail messages increases the opportunities for a breach of privacy.

See also: **Communications Assistance for Law Enforcement Act (CALEA); Electronic surveillance**

Suggested Reading: Computer Professionals for Social Responsibility. <http://www.cpsr.org>. Online, March 2006; Electronic Privacy Information Center. <http://www.epic.org>. Online, March 2006; Klensin, J. *Simple Mail Transfer Protocol* (Network Working Group RFC 2821, April 2001). <http://www.ietf.org/rfc/rfc2821.txt>. Online, November 2005; Resnick, P. *Internet Message Format* (Network Working Group RFC 2822, April 2001). <http://www.ietf.org/rfc/rfc2822.txt>. Online, November 2005; Straub, Detmar W., Jr., and William D. Nance. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study, *MIS Quarterly* 14 (1990): 45–60.

David E. Sorkin

Electronic surveillance

Widespread electronic surveillance, whether conducted by the government, corporations, or individuals, has obvious consequences for individual privacy. Technological innovations have enabled the use of **surveillance** without the need for

physical proximity to a subject. Since the presence and use of such technology are often difficult to detect, a subject under surveillance may find that conversations, e-mails, and activities that were assumed to be private communications or actions were in fact observed and tracked. Although such messages and acts may be protected by privacy rights, these traditionally have had to be balanced against an often-conflicting public interest, such as the need to obtain evidence of criminal wrongdoing or to strengthen national security.

The term “electronic surveillance” does not necessarily correspond to a legal definition. As a descriptive phrase, it is extremely broad; as reflected in the legislative framework, however, it is used generally to delineate the means and techniques of surveillance, rather than to characterize the information obtained thereby. This usage thus includes within its purview **wiretapping**, “bugging,” and the electronic interception of **e-mail**.

Wiretapping can be done either mechanically or, given modern telephony, digitally. The former involves placing a listening device on physical equipment such as a handset, and either connecting directly to the telephone line or mechanically switching the telephone signals. With the development of digital telephony, which is utilized by cable service companies, and **Internet** telephony, the difficulties and detection risks of physical or mechanical tapping can be minimized, as a remote **computer** can be used to perform the requisite signal switching easily and effectively. Wiretapping and bugging, whether mechanical or digital, are means by which the contents of a communication can be detected and recorded. Digital interceptions can, however, also record “logs,” such as a list indicating the number and duration of the calls made and received. Telephone service companies also routinely log non-content data for billing and other subscriber-related purposes. These records may be subject to disclosure in response to a subpoena or other court order.

The “traditional” means of electronic interception reflected a distinction between content and non-content communications, in that pen registers and trap-and-trace devices work differently than wiretaps. A **pen register** is an electronic device that records the numbers dialed from a telephone; a trap-and-trace device is similar except that it records the incoming dialed numbers to a telephone. As reliance on the use of computers and the Internet has grown, it has become possible to collect more and increasingly varied kinds of non-content data (often referred to as “transactional data” or “traffic data,” to distinguish such information from the actual contents of a communication). Transactional data include the date and time of a communication, its duration, and the kind of telephone dialing information collected by pen/trap devices. On the Internet, which transmits information in the form of digital bit streams and data “packets” that are automatically re-assembled at the destination computer, transactional information also includes routing information and the identifying Internet Protocol (IP) “address” of the sending and receiving computer. In essence, devices that enable the monitoring and recording of transactional data are utilized to identify the source, destination, and other information regarding the transmission of a communication.

“Packet sniffer” software and “black box” devices that are attached to a computer network and that detect, filter, intercept, and record data passing across the network are readily and commercially available. Such technology, considered tools for network analysis, are useful for troubleshooting and technical maintenance;

however, they also facilitate the monitoring of e-mails, Internet chat sessions, file-sharing activity, and other communications that pass through the network. The **Carnivore** software suite that was utilized by the U.S. **Federal Bureau of Investigation (FBI)** is an example of packet sniffer technology, relying on sophisticated filtering to isolate, intercept, and analyze data packets transmitted across an Internet service provider's (ISP's) network.

This category of surveillance includes keystroke-logging devices (which record every stroke of a computer user's keyboard entries). **Keystroke loggers** can take the form of hardware devices or software; in the latter form, they can be installed by way of a "Trojan horse" or other software virus. The FBI has successfully utilized keystroke loggers to obtain encrypted computer passwords of suspects in criminal investigations.

Other forms of computer and online tracking technology include "cookies" and "web bugs" (also known as "web beacons" or "clear gifs"), used mainly by Internet marketers and advertisers. A cookie is a data file that is stored on the user's computer and sends back information about that user's online activity with regard to particular websites and web pages (such as when they were accessed and for how long). Cookies are useful for gathering information about users' web browsing habits and preferences, and they can also store registration, online shopping, and other user data. A web bug is an invisible image embedded in a web page or an e-mail that is downloaded when the page or e-mail is opened by a computer user. Although similar to cookies in that they provide information about when a user visits a website, web bugs embedded in e-mails can generate wider privacy concerns, as they also provide information about the user's computer (e.g., its IP address and web server).

The term "spyware" is used generally to refer to software that exists on a computer's hard drive unbeknownst to the user and that surreptitiously monitors the user's computer activity; it may also alter or activate certain computer functions at a third party's behest (such functionality classifying it also as "malware," or malicious software). A good deal of "adware," or software that displays advertising to a user, is also commonly categorized as spyware because it is often installed without the user's knowledge, though it may not amount to malware. Spyware, particularly adware, usually includes a monitoring function, which can vary from monitoring the user's online browsing activity to redirecting the user to different websites (usually as part of an advertising network utilizing the spyware in question).

These devices are used to detect the presence and availability of wireless networks and activity within those networks. With the proliferation of wireless networks in homes, schools, offices, and elsewhere, there has been a corresponding increase in the establishment and availability of wireless access points (WAPs), including free WAPs offered by commercial establishments to their customers. This has facilitated the practice of "war driving," where a laptop enabled with the right software can be used to detect a wireless computer network, to log on to it, and even to intercept data traveling across that network.

"Locational data," similar to "transactional data" in that they do not generally relate to the contents of a communication, disclose the geographical location of a user or computer. Locational data can be obtained by utilizing the **Global Positioning System (GPS)** or devices that rely on triangulation between a wireless **cellular**

telephone and cellular signal towers, as does the E-911 feature included in U.S. cellular phones, as mandated by the Federal Communications Commission.

Mobile or cellular telephones utilize a wireless network comprising various base stations linked to a traditional telephone network and communicating through electromagnetic radio waves. Although different providers may use different technological standards for communications, digital technology such as GSM (Global System for Mobile Communications) is used widely. In addition to speech, mobile telephones support other services, such as text messaging, Internet access, and the exchange of video and photo files. Tapping into a mobile telephone network allows the collection of transactional as well as locational data, since it is possible to identify the base station for the call in question. Content data can also be intercepted, and, as new technology (such as 3G, or third-generation, mobile telephone technology) enabling the transfer of more types of files gains ground, the kinds of content data that can be intercepted will also grow. These new technologies rely on the transmission of data stored on a mobile device ("tag") equipped with a transponder that responds to radio frequency signals sent by a transceiver. **Radio frequency identification** (RFID) allows the transmission of locational and transactional information in the form of data stored on the tag; because the tag can be attached to any person or object, an RFID system enables mobile tracking.

Data mining is an analytical tool that uses statistical modeling, computational techniques, and search functionality to analyze, extract, compare, and link vast amounts of data within and across databases. Previously disparate or unconnected data can be compiled and analyzed, and patterns discerned.

A significant issue for privacy in relation to some of these new techniques is the possibility that they can be used in combination. For example, locational data can be combined with a user's web browsing patterns (obtained by some other method), placed into a database, and analyzed using a variety of software and techniques, including data mining. This ability poses a challenge for the legal regulation of electronic surveillance, which traditionally has largely focused on, and applied differing standards based on, distinctions between content and non-content data, and between data being intercepted while in transmission and its interception thereafter (i.e., in electronic storage).

A few differences between the more traditional forms of electronic surveillance (such as wiretapping, bugging, and the use of pen registers and trap-and-trace devices) and methods involving the Internet should also be noted in this context. First, it is easy to make a distinction between the contents of a communication and the transactional data surrounding it, such as the telephone number dialed or the duration of the call. This distinction is less clearcut in the case of Internet communications. For example, the subject line of an e-mail communication can reveal much about the contents of the e-mail itself, and some pen/trap devices can capture dialing signals that are content-related (such as credit card numbers). Second, tracking a computer user across the Internet (such as by means of the websites visited) can disclose information that is not limited to facts regarding location and destination, but that is more personal in nature, such as the user's online shopping behavior, interests, and habits. Third, the availability and adoption of data mining technology raises the possibility not only that databases containing personal or private information can be created, but also that vast amounts of information can be

combed, compiled, linked, and profiled in a way not previously technologically feasible. The implications include the risk that existing laws will prove insufficiently flexible or technology-neutral to cope with the new technology (and its allowance for electronic surveillance on a scale and with an ease not previously possible) and that the broad potential capacity for greater electronic surveillance mandates a reexamination of the appropriate balance to be struck between privacy protection and the need to prevent legitimate government or corporate objectives from being impeded by overzealous regulation of new technology.

Electronic surveillance that does not capture the contents of a communication is dealt with by specific provisions and statutes. The Pen/Trap Statute prohibits the use of pen/trap devices except through a court order or under the **Foreign Intelligence Surveillance Act of 1978 (FISA)**. The Stored Communications Act criminalizes unauthorized access to or alteration of wire or electronic communications in “electronic storage” by anyone other than the systems provider or the user who originated the communication or for whom the communication was intended, except under a warrant or court order. These legislative measures thus allow the U.S. government, upon a court’s authorization, to obtain transactional, traffic-related, and similar data through electronic surveillance, and to gain access to the contents of wire and electronic communications after their transmission.

The same technology that permits government surveillance can be used by private corporations and individuals to obtain information surreptitiously. One key difference between government (public-sector) surveillance and private-sector monitoring is the lack of Fourth Amendment protection for subjects of the latter. Although the provisions of the Wiretap Act prohibiting intentional interceptions of content-based transmissions apply to private-sector surveillance, its exceptions allow limited monitoring. For example, interception is permitted with the consent (express or implied) of at least one of the parties to the communication, or if the interception is “a necessary incident to the rendition of the service or to the protection of the rights or property of the provider of the service.” The consent exception has been invoked in some cases involving the use of cookies and similar technology by Internet advertisers to monitor the web browsing habits of computer users. Because Internet advertising relies on a network of individual websites to which the advertisers serve up their advertising, U.S. courts have held that the provisions of the **Electronic Communication Privacy Act of 1986 (ECPA)** regarding consent require only the consent of the individual “client” website, not of the individual users of each of those websites, and that consent pertains to the placing of the advertisements, not of the cookies carried by them to an individual user’s computer. For this reason, it has been problematic for individual users to rely on the ECPA to protect them against Internet marketers.

Electronic surveillance is generally viewed as an indispensable tool for criminal investigations and law enforcement. Both legislators and the courts have displayed some measure of nimbleness in enacting, amending, and interpreting the law to accommodate this need while remaining cognizant of the corresponding risk of loss of privacy. In the United States, the need to balance privacy concerns with the needs of law enforcement can be seen in the various procedural safeguards in the wiretap statutes and the courts’ role in interpreting the Constitution. Although recent legislation, such as the **Uniting and Strengthening America by Providing**

Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) and similar laws in other jurisdictions, seems to have tipped the balance in the direction of greater surveillance, this shift may be justified on the grounds of national security in the face of a growing threat of terrorism. The challenge will be to continue to maintain the appropriate balance, to the extent necessary and proportionate to the perceived public policy threat justifying a potential encroachment on privacy. In addition, any future amendments to electronic surveillance legislation should be mindful that new technology challenges the boundaries of legal distinctions between the interceptions of different kinds of data. These issues should remain uppermost in the minds of policymakers, particularly if greater surveillance powers continue to be granted by law, since at some point the pressing public policy need for such powers may well diminish or disappear altogether. Consequently, the difficulties inherent in attempting to craft a balance between individual privacy and increased surveillance must be confronted.

See also: **Airborne surveillance and intelligence; Anti-wiretap statutes; Communications Assistance for Law Enforcement Act (CALEA); National Security Agency; Surveillance cameras**

Suggested Reading: Bryant, Susan. "Electronic Surveillance in the Workplace," *Canadian Journal of Communication* (1995). <http://www.cjc-online.ca>. Online, February 2006; Center for Democracy & Technology. *Electronic Surveillance*. http://www.cdt.org/wiretap/wiretap_overview.html. Online, March 2006; Diffie, Whitfield, and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press, 1999; Dempsey, James X. "Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy," *Albany Law Journal of Science & Technology* 8 (1997): 70–71; Flaherty, David H. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill: University of North Carolina Press, 1992; Ottensmeyer, Edward J., and Mark A. Heroux. "Ethics, Public Policy, and Managing Advanced Technologies: The Case of Electronic Surveillance," *Journal of Business Ethics* 10 (1991): 519–526; Schneier, Bruce, and David Banisar. *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance*. Hoboken, NJ: Wiley, 1997; Surveillance and Society. *Resource Base*. <http://www.surveillance-and-society.org/resources.htm>. Online, March 2006.

Mary W. S. Wong

Electronic toll collection

Electronic toll collection is a system that allows government agencies and municipalities to collect tolls from commuters electronically without the need for drivers to stop and collect a toll ticket or pay the booth operator. Electronic toll systems are in place in different countries around the world and allow traffic to flow more easily through toll areas. These **radio frequency identification (RFID)** systems work by using radio signals to communicate between a toll booth and a transponder positioned on an **automobile**. The transponder is a small plastic device that contains electronic information about the owner. An antenna at the toll booth sends out a radio frequency that activates the transponder as it approaches. The transponder

then sends back information that the toll antenna reads. The system charges the commuter's account by using the toll booth through which the automobile first passed along with the final toll booth passed through to calculate the total toll. The transponder is associated with a credit card or bank account that is kept on file and from which funds are deducted.

Some systems are also equipped with video cameras that can take pictures of the cars that pass through a toll booth and their license plates. When a vehicle without a transponder drives through the toll booth, the camera will take a picture of the car and its license plate; it will then mail a ticket to the owner of the vehicle. The cameras are also used to catch drivers who try to use transponders that have been reported stolen. Although the primary functions of the system are to facilitate the collection of tolls and to avoid slowing traffic, it can also be used to gather information about those that pass through it.

One concern is the monitoring of specific driving patterns of individual commuters using this collection system. Since the transponder contains information about the driver of the vehicle needed for billing purposes (such as a home address), it would be easy to track how far a driver commutes from home each day. From this a driving pattern could be established for all commuters who use the electronic toll collection system. This information could be used by agencies such as insurance companies to determine rates for drivers based on where and how far they drive. Car rental companies could also use this information. In places where video cameras are installed, there will also be a picture of the car and license plate to go along with the commuter's account information carried in the transponder.

Another concern is keeping the information that is carried on the transponders secure. Because transponders carry personal information about their owners, many motorists want to make sure that information is not used for purposes other than collecting the appropriate toll.

Suggested Reading: Al-Deek, H. M., A. A. Mohamed, and A. E. Radwan, "Operational Benefits of Electronic Toll Collection: Case Study," *Journal of Transportation Engineering* 123 (1997): 467–477; Zimmerman, Carol A., Mala Raman, William J. Mallett, and Craig Roberts. *Sharing Data for Traveler Information: Practices and Policies of Public Agencies*. <http://www.ops.fhwa.dot.gov/travelinfo/resources/datashare/datshare.htm>. Online, March 2006.

Jose L. Martinez

European Data Protection Directive

The European Data Protection Directive is an abbreviated reference to what is officially titled the "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." Adopted October 25, 1998, the directive comprises of a set of data protection laws consisting of 34 articles that reflect the consensus achieved among the then 15 members of the European Union over eight years of negotiation. Designed to harmonize and coordinate the flow of information, particularly personal data, across the borders of EU member states, the directive provides a unified, comprehensive framework for data protection legislation and practices in both the public and private sectors in each



EU member state, including countries that joined after the adoption of the directive. Updates on the implementation of the EU directive in the 25 member countries are available on the data protection website of the European Commission.

The directive is important not only because it provides a regulatory framework for privacy regulation in 25 EU member countries, but also because it sets privacy standards internationally that emphasize the rights of individuals to their personal information as an unalienable human right.

Of the main stakeholders involved in the use of personal data—individuals, governments, and businesses—the directive focuses on the right of individuals to control the collection, distribution, and use of their personal information—a traditional human right in many EU member countries. This individual right is protected in particular through the directive’s stipulations regarding the principles of openness, access and correction, collection limitation and finality, accuracy, security, and enforcement or redress—often considered important fair information principles.

According to the directive (Article 18[1]), anyone collecting and processing personal information from individuals (the so-called data controller) must register with the public data protection authority. Furthermore, data protection legislation of member states must include a requirement for open information about the collection of personal data. At a minimum, before collecting any personal information from individuals, the data controller must openly provide the identity and contact information of the controller, the purpose of the data collection and processing, a description of the categories of the data to be collected, the recipients of the collected data, possible transfers of the collected data to entities outside the EU, and measures taken to ensure the security of the data. Finally, toward the objective of openness, the data controller must ensure that “the data subject has unambiguously given his consent” (Article 7a) before any data processing can begin, including the transfer of data to third parties. Few exceptions apply to this rule.

The EU directive stipulates that individuals must be provided with access to personal data collected about them “without constraint at reasonable intervals and without excessive delay or expense” (Article 12). The directive also states that any changes individuals request about the personal data collected from them must be passed on to third parties to whom the data may have been exposed. According to the directive, individuals in EU member countries must also have the right “as appropriate” to correct the data collected from them, stop the processing of their personal data, or even demand that their personal data be removed from databases.

To ensure the control of individuals over their personal data, the EU directive requires that personal data collection from individuals in EU member countries be limited to specific and clearly articulated purposes. Article 6[1b] states that data must be “collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes.” In other words, data can be collected only to the extent that the collection is in line with the specified purposes. Moreover, if an entity that has collected personal data would like to use the data for a purpose not specified in the original data collection process, and to which individuals therefore did not consent, the entity must request renewed, unambiguous consent from those individuals to the new use of their personal data. Data can, however, be used for statistical or scholarly purposes as long as member states establish guidelines for such usage that are line with the directive.

In addition, the directive limits the types of the data that can be collected from individuals in EU member states. For example, data that reveal an individual's ethnic origin, race, political conviction, religious beliefs, or health and sexuality cannot be collected unless the entity collecting such information has the right to do so in the member country (e.g., for the performance of government services, employment, etc.).

The principle of accuracy is an important component of the directive's overall emphasis on data quality. According to Article 6[1]d, those who collect personal data from individuals must ensure that such data be "accurate, and where necessary, kept up to date." If the accuracy of the data cannot be confirmed, the data must be erased. The directive states, "Every reasonable step must be taken to ensure that data which are inaccurate and incomplete . . . are erased or rectified."

To protect the rights of individuals regarding their own personal information, the EU directive requires that those who collect personal data from individuals ensure that these data are kept secure. Data controllers must implement "appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access" (Article 17[1]). In essence, the entity collecting personal data is responsible for protecting the data from unlawful uses, manipulation, or loss.

Although redress does not fall under the usual set of "fair information principles," it is an important principle for adequate data protection according to the EU directive. Redress is to be guaranteed by public independent authorities: "Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of . . . this Directive. These authorities shall act with complete independence" (Article 28[1]). The purpose of such an independent mechanism is to ensure that individuals have recourse if they feel that their right to their personal data has been infringed. Thus, EU member countries must not only verify the independence of their data protection authorities, but also bestow on them the power to investigate claims of data protection violations, to intervene and stop the collection of personal data, and to initiate legal procedures against violators of data protection rights.

Based on the recognition that data from EU citizens is collected by entities not only in the EU but also from countries outside the EU, the directive stipulates that personal data about EU citizens can be transferred only to those countries that offer individuals "adequate" protection of their right to their personal information. As stated in Article 25[1], "the Member States shall provide that the transfer to a third country of personal data . . . may take place only if . . . the third country in question ensures an adequate level of protection." For example, a business traveler from a country without adequate protection may not take data about business or customer contacts collected in EU member countries outside the EU. By barring the transfer of personal data from EU citizens to businesses and other entities in countries without levels of privacy protection deemed appropriate by the EU, the directive sets de facto standards for data protection internationally. Accordingly, countries such as Canada, Australia, and Japan have implemented data protection laws that provide similar levels of protection for personal data. Others—in particular the United States—have worked out special agreements with the EU so that U.S. businesses can claim compliance with these principles.



See also: **Computers; Internet; Safe harbor principles**

Suggested Reading: Bennett, Colin J., and Charles D. Raab. "The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response," *Information Society* 13 (1997): 245–263; European Commission, Justice and Home Affairs. *Data Protection*. http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm. Online, March 2006; Farrell, Henry. "Negotiating Privacy across Arenas: The EU-US 'Safe Harbor' Discussions." In A. H  ritier (ed.), *Common Goods: Reinventing European and International Governance*, pp. 101–123. Lanham, MD: Rowman and Littlefield, 2002; Regan, Priscilla. "Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows," *Journal of Social Issues* 59 (2003): 263–282; Starke-Meyerring, Doreen, D. Burk, and Laura Gurak. "Americans and Internet Privacy: A *Safe Harbor* of Their Own?" In Philip Howard and Steve Jones (eds.), *Society Online: The Internet in Context*, pp. 275–293. Thousand Oaks, CA: Sage, 2004; Swire, Peter, and Robert Litan. *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*. Washington, DC: Brookings Institution, 1998.

Doreen Starke-Meyerring

F



Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) is the principal federal statute regulating the activities of credit bureaus and users of credit reports. Credit bureaus are private companies that maintain computerized records of consumers' credit histories (known as credit or consumer reports). There are three national credit reporting companies, each of which keeps reports on millions of consumers. Reports include information on consumer debts, payment habits, bank accounts, employment, and other personal information. Credit bureaus issue reports to employers, **credit card** companies, insurers, banks, and other businesses upon request and payment of an issuance fee. The businesses then use the information to make decisions about hiring, extensions of credit, issuance of insurance policies, and other matters of consumer concern. The FCRA establishes the rights of consumers whose credit reports are maintained by credit bureaus and ensures that reports are reasonably accurate and released only for purposes permitted by the law.

Enacted in 1970 as a new title to the Consumer Credit Protection Act of 1968, the FCRA was drafted to accommodate the sometimes conflicting goals of facilitating the free flow of information about consumers while ensuring the issuance of substantially accurate reports. The law attempts to balance the interests of consumers in having accurate credit reports against the desire of the business community to obtain quick and inexpensive data necessary to make informed commercial decisions. Thus, while the law tries to ensure that credit bureaus issue consumer reports fairly, accurately, and with respect for the consumer's right to privacy, it does not mandate completely accurate credit reports or give consumers control over who may see their reports. The FCRA provides a base level of consumer protection that relies on consumers monitoring their reports and correcting inaccuracies as they find them.

To prove a credit bureau's violation of the accuracy requirements imposed by the FCRA, a consumer first must establish that the report is materially incorrect. Early court decisions applied a narrow test of accuracy and rejected claims that the information contained in a report, while technically correct, was misleading, incomplete, or irrelevant. These decisions were subject to criticism, and courts in recent years have upheld consumer claims when reports are technically accurate



but misleading. When information is so incomplete as to be misleading and when clarifying information is readily obtainable, courts may find that the accuracy requirement of the FCRA has been violated.

Even if a consumer can establish that the report contains inaccurate or extremely misleading information, the credit bureau still may not have violated the act. The FCRA does not mandate accurate credit reports, only that credit bureaus maintain “reasonable procedures” to assure “maximum possible accuracy.” In any action against a credit bureau for inaccurate reporting, the consumer has the additional burden of proving that the bureau did not have reasonable procedures in place. While the law does not specify the precise procedures a bureau must establish, the Federal Trade Commission (FTC) has issued guidelines and general standards that bureaus are expected to follow. For example, bureaus should implement procedures to ensure that its employees are properly trained to create, update, and release consumer reports, and that data are properly recorded and reproduced. Agencies that transmit data electronically over long distances (the dominant method under current practice) must ensure that the information is properly converted to computer format and that it is neither modified nor susceptible to unauthorized access during transmission. As with the FCRA in general, determining the reasonableness of reporting procedures requires balancing the credit bureau’s interest in minimizing time and expense against the consumer’s interest in accuracy.

Studies have shown that a significant percentage of the credit reports existing in credit bureau databases contain erroneous information. The most common errors include mistaken information about the status of an account or payment history, information about one consumer mixed with data on a different individual, and the failure of the credit reporting agency to remove obsolete information as required by the FCRA.

Credit bureaus cannot be guarantors of completely accurate information. Bureaus obtain most of the information in credit reports from outside sources, typically businesses that extend credit and provide payment histories to the bureau for inclusion in consumers’ files. The FTC and the courts have concluded, however, that credit bureaus are not merely conduits of information. If the bureau should reasonably be aware of errors that indicate systemic problems or a pattern of unreliability with a particular source of information, the bureau should evaluate its procedures and implement cost-effective adjustments. In addition, the law requires periodic review of data to determine whether information has become obsolete or misleading with the passage of time.

Except in transactions involving large amounts of money, credit bureaus may not disclose adverse information that is more than 7 years old (10 years for information about bankruptcies). There is no requirement that a credit bureau delete obsolete information from its files, only that it not include such information in a report unless the monetary thresholds are satisfied. Consumers can enforce this part of the FCRA with relative ease because, unlike the disclosure of inaccurate information, a bureau’s improper disclosure of obsolete information automatically violates the FCRA regardless of the reasonableness of the agency’s procedures. While instances of unlawful disclosure of obsolete information are not uncommon, many of the disputes over this section of the FCRA center on whether the credit bureau

had reasonable grounds to believe that the information was being disclosed in connection with one of the specified exempt transactions involving large sums of money.

The only way consumers can ensure that their credit files are completely accurate is to discover and correct errors themselves. The FCRA facilitates this task by giving consumers the right to learn the contents of their credit bureau files. The FCRA requires that information in a consumer's file be available upon proper identification. The consumer has a right to receive one free copy from each of the three major credit bureaus per year (and more than one copy in some states).

Before credit reports were available on the **Internet**, only a small percentage of consumers reviewed their reports on a regular basis. Today, most consumers are aware that credit reports exist and that they have a right to access them. In addition, when a creditor, employer, or insurance company uses negative credit information to make an adverse decision, the FCRA requires that the consumer be informed of his right to review the report that influenced the decision. The user of the report must inform the consumer that a report was considered and must provide the contact information of the bureau issuing the report. This information prompts many consumers to contact the credit bureau and request a copy of the report.

A credit bureau can only disclose the information in its own file. Other credit bureaus may have files containing information compiled from the same or different sources. Thus, even if the consumer discovers and corrects erroneous information in the file of the one bureau contacted, the same data may be present in the files of other bureaus that potential creditors might use.

If a consumer questions the accuracy of a report and believes that additional information would correct an error or clarify a misleading statement, the bureau must make a good faith investigation of the claim. According to the FTC, at a minimum, the bureau must verify the information within a reasonable time by checking back with the original source and confirming the data. An exception to the investigation requirement is when the bureau has reason to believe that the consumer's dispute is frivolous or irrelevant. If, after the investigation, the bureau agrees with the consumer and finds the information to be inaccurate, the bureau must delete the data from its files. If the consumer is not satisfied with the outcome of the investigation, the consumer may file with the bureau a brief statement clarifying his or her side of the dispute. In subsequent reports, the bureau must note that the item is disputed and must provide either the consumer's statement or a clear summary of the dispute along with the report.

If the investigation results in the deletion of information or the inclusion of a consumer's statement of dispute, the consumer still must contact the other two major credit bureaus to correct erroneous information that may be in their files.

To protect consumer privacy, credit bureaus are prohibited from releasing credit reports except for specific purposes. Permissible purposes include applications for credit, insurance, employment, and housing rentals. Reports can also be issued for review of existing accounts (for example, to a creditor or insurer deciding whether to retain the consumer as a customer), and for a promotion or retention decision by an employer. Other permitted uses include court orders, law enforcement, child support payment determinations, and professional licensing



decisions. The law also allows release of a report generally for any “legitimate” business need in a transaction initiated by the consumer for personal, **family**, or household purposes.

The FCRA was amended in 2003 to help consumers address problems associated with **identity fraud** and theft. If consumers believe that someone is opening accounts in their names or is otherwise impersonating them, they can request that “fraud alerts” be placed on their credit reports. A fraud alert indicates that a consumer does not authorize new credit or increases in credit limits on an existing account. A consumer may include a telephone contact number that must be called to identify the consumer before any new account is opened. The law also requires merchants to truncate credit and debit card numbers on electronically printed receipts, thus reducing the risk of stolen card numbers, and includes new rights that help consumers remedy the effects of identity theft and restore their credit histories.

See also: **Banking and financial records**

Suggested Reading : Camden, Bonnie G. “Fair Credit Reporting Act: What You Don’t Know May Hurt You,” *University of Cincinnati Law Review* 57 (1988): 267–298; Electronic Privacy Information Center. *Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report*. www.epic.org/privacy/fcra/. Online, March 2006; Rodriguez, Anthony, Carolyn Carter, Willard Ogburn, Joanne Faulkner, Elizabeth De Armond, Richard Rubin, and Chi Chi Wu. *Fair Credit Reporting*, 5th ed. Boston: National Consumer Law Center, 2002 (2005 Supp.); Seidel, Joseph L. “The Consumer Credit Reporting Reform Act: Information Sharing and Preemption,” *North Carolina Banking Institute* 2 (April 1998): 79–95.

James P. Nehf

Fair information practices

Fair information practices (FIPs) are a set of principles for defining and addressing concerns about privacy of personal information. In most countries with privacy laws, FIPs are officially acknowledged as core privacy principles and incorporated in privacy and data protection laws. The international policy convergence around FIPs as core elements for information privacy has remained in place since the late 1970s. United States privacy laws, which are much less comprehensive in scope than laws in other countries, often reflect some FIPs elements. However, FIPs principles are much less universally recognized and followed.

Fair information practices were invented by a U.S. government advisory committee in a 1973 report issued by the Secretary’s Advisory Committee on Automated Personal Data Systems. Elliot Richardson, secretary of the Department of Health, Education and Welfare, established the committee in response to the growing use of automated data systems containing information about individuals.

The central contribution of the advisory committee was the development of a code of fair information practices for automated personal data systems. According to Committee Chairman Willis Ware, the name Code of Fair Information Practices was inspired by the Code of Fair Labor Practices. According to the committee’s original formulation of the code,

Safeguards for personal privacy based on our concept of mutuality in record keeping would require adherence by record-keeping organizations to certain fundamental principles of fair information practice:

- There must be no personal-data record-keeping systems whose very existence is secret;
- There must be a way for an individual to find out what information about him is in a record and how it is used;
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent;
- There must be a way for an individual to correct or amend a record of identifiable information about himself; and
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

The first formal statutory implementation of FIPs came in the **Privacy Act of 1974** (5 U.S.C. §552a), a law applicable to federal agencies. The act reflects the committee's recommendations for a federal privacy statute. However, the first statutory mention of FIPs did not come until 2002, when Congress established a Department of Homeland Security Privacy Office with responsibility for ensuring compliance with fair information practices as set out in the Privacy Act.

Around the same time that the U.S. enacted the Privacy Act of 1974, European countries began to pass national privacy laws applicable to the public and private sectors, beginning with Sweden in 1973 and the Federal Republic of Germany in 1977. Both countries' laws were consistent with or relied upon FIPs. Other European countries enacted comparable privacy laws in the late 1970s and early 1980s.

As privacy laws spread within Europe, international institutions began to address privacy and the international implications of privacy regulation. The Council of Europe adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data in 1980. The Organization for Economic Cooperation and Development (OECD) proposed similar privacy guidelines around the same time.

FIPs provided core principles for both documents, but both organizations revised and extended the original U.S. statement of FIPs. The work of the Council of Europe and the OECD contributed to the international spread of FIPs as core privacy policies. Of the two early-1980s international privacy documents, the OECD Privacy Guidelines are cited most often.

The eight principles set out by the OECD are:

Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.



Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: (a) with the consent of the data subject; or (b) by the authority of law.

Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle: An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

Accountability Principle: A data controller should be accountable for complying with measures, which give effect to the principles stated above.

The reliance on FIPs by the European Union in its 1985 European Data Protection Directive ensured the spread of FIPs throughout Europe.

Different statements of FIPs sometimes appear disparate, but the content is frequently similar. However, statutory implementations of the principles may vary in different countries and in different sectors. The international agreement on basic principles should not obscure the complexity of the policies, the considerable variation in their application, and the controversy about their implementation in different contexts and by different record keepers.

In the United States, law occasionally requires elements of FIPs, but private-sector compliance, while slowly increasing, is mostly voluntary and sporadic. Also, shortened or incomplete versions of FIPs have sometimes been offered in the United States by federal agencies or trade associations. The United States is a significant laggard among industrialized nations in implementation of FIPs.

Critics of FIPs can be found on both sides. Some believe that FIPs are too weak, allow too many exemptions, do not require a privacy agency, and have failed to keep pace with information technology. Critics from a business perspective often

prefer to limit FIPs to reduced elements of notice, consent, and accountability. They complain that other elements are unworkable, expensive, or inconsistent with openness or free-speech principles.

In 1999 Justice Michael Kirby of the High Court of Australia and former chair of the OECD committee that developed the 1980 guidelines spoke at an international privacy conference. He noted the many changes brought about by new computer and communication technologies and suggested that it might be time for a review of the guidelines.

See also: **Opt-in vs. opt-out; Privacy notices**

Suggested Reading: Bennett, Colin J. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca, NY: Cornell University Press, 1992; Council of Europe. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. 20 I. L. M. 317 (1981). <http://conventions.coe.int/treaty/en/treaties/html/108.htm>. Online, July 2005; European Union. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. Council Directive 95/46/EC, 1995 O. J. (L 281) 31. http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm. Online, July 2005; Kirby, Michael. *Privacy Protection—A New Beginning*. Speech before the 21st International Conference on Privacy and Personal Data Protection (1999). <http://www.pco.org.hk/english/infocentre/conference.html>. Online, July 2005; Organization for Economic Cooperation and Development. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. 20 I. L. M. 422 (1981), O. E. C. D. Doc. C (80) 58 (Final) (October 1, 1980). http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html. Online, July 2005; U.S. Department of Health, Education, and Welfare. Secretary's Advisory Committee on Automated Personal Data Systems. *Records, Computers, and the Rights of Citizens* (1973). <http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm>. Online, July 2005.

Robert Gellman

Family

Privacy within family law has two fundamental yet interrelated meanings. First, privacy can mean privatization, the use of internal rather than external norms, and thus, the legal ability of those within the relationship to control their own rights and responsibilities, such as through prenuptial contracts, cohabitation agreements, or separation agreements. There has been a general movement since the last third of the twentieth century to allow for increased private contracting before, during, and at the end of marriage, as well as between cohabiting couples. States have adopted different standards for judging these contracts, sometimes applying general standards of contract law, while at other times stressing the nature of the fiduciary relationship between marital partners. While these contracts have been upheld when they relate to obligations between intimate partners, courts have been far stricter when these agreements affect the rights of children through child support or child custody, generally holding that the state must decide these issues under a “best interest of the child” test.



Second, privacy can denote a protected sphere. The right to engage in any activities that one chooses within that sphere. Older understandings of marital privacy were summarized by Blackstone as involving the wife's legal existence being "suspended" during the course of the marriage, with the husband responsible for protecting his wife during her coverture. Based on this reasoning, a wife could not testify against her husband in court because she did not have a separate legal identity from him. As another example, because of the wife's legal disabilities during marriage, there was a specific doctrine—the "necessaries doctrine"—that allowed her to buy necessities from a third party, using her husband's credit. If the husband refused to pay for the necessities, the creditor could sue the husband for the debt. As women have become able to maintain their own separate existence during marriage, the conceptions of marital privacy have changed.

Based on contemporary privacy law, this entry discusses two different aspects of family privacy: (1) the marital relationship and (2) the parent-child relationship. A third form of familial privacy related to sexual decisionmaking outside of marriage is discussed elsewhere. The constitutional development of marital relationship privacy involves two distinct elements: the right to marry and the right to sexual privacy for marital decisionmaking.

The first form of marital privacy protects the very decision of whom to marry. State laws generally establish who may marry whom, prohibiting, for example, polygamous and incestuous marriages. Although the Supreme Court had frequently discussed the right to marry, it was only in 1967 that the Court addressed the nature of the right itself, striking down Virginia's anti-miscegenation law in *Loving v. Virginia*, 388 U.S. 1 (1967). In subsequent cases, the Court established the quasi-fundamental nature of the right (for heterosexuals) to marry. This form of marital privacy has become increasingly controversial in the context of same-sex marriage, where advocates argue that individuals should have the freedom to choose their partners. In *Goodridge et al. v. Department of Public Health* (2003), finding a right to same-sex marriage, the Massachusetts Supreme Judicial Court reiterated that individuals are protected against burdensome regulations of their right to marry, finding that the Massachusetts constitution prevented undue governmental interference with issues of "personal liberty." On the other hand, other courts have distinguished the fundamental nature of the right to marry a person of the opposite sex, which is historically protected, from the option of marrying a person of the same sex, which has not been a traditionally protected legal right. Courts have repeatedly held that the right to marital privacy does not extend to polygamous or incestuous relationships.

The second form of marital privacy involves the right to relational privacy; this right is most frequently addressed in the context of sexual decisionmaking. Perhaps the first reference in Supreme Court jurisprudence to the privacy of the marital relation occurs in the 1885 bigamy prosecution of *Cannon v. United States*. Angus Cannon was unable to offer testimony that he had not "cohabited," in a sexual sense, with a particular woman, because the Court was so protective of marital privacy.

The concept of marital privacy was also important in other nineteenth-century courts. Marital privacy was repeatedly used as a justification for failing to prosecute spousal violence. Rather than sustaining the eighteenth-century notion of marital unity, nineteenth-century courts began to use marital privacy as the theory for

protecting against intervention in the ongoing family. By contrast, divorce courts often inquired into minute details of marriages; once the marriage ended, courts felt free to examine the marital relationship in surprising detail.

It was only in 1965, in *Griswold v. Connecticut*, 381 U.S. 479, that the Court directly addressed the concept of marital privacy, locating it in the penumbras of various constitutional rights. *Griswold* involved the provision of contraceptives to a married couple in violation of a Connecticut statute that criminalized the using, or helping others to use, contraceptives. Seven years later, in *Eisenstadt v. Baird*, 405 U.S. 438 (1972), a contraceptive case involving unmarried people, the Court found that the right to privacy was not restricted to the confines of marriage, and that, although it attached to marital couples, it also attached to individuals who might comprise a couple. In 2003, in *Lawrence v. Texas*, 539 U.S. 558, the Court allowed the right of privacy to protect same-sex sexual intimacy.

Because marital privacy applies both to the couple and to the individuals involved in a marriage, a wife is not required to inform her husband, much less receive his consent, before having an abortion. The Supreme Court recognized, in *Planned Parenthood of Southeastern Pennsylvania v. Casey* (1992), that while both marital partners have similar interests in living children, state abortion regulations have a much stronger effect on the wife's liberty interest than on the husband's.

Ultimately, the constitutionally developed right to marital privacy protects the relationship between husband and wife from undue interference. It creates and preserves a “**zone of privacy**” surrounding the marital relationship, specifically in the context of sexual decisionmaking, but also more generally in its affirmation of other constitutional protections for the **home** and the family.

Turning to the second aspect of family relationship privacy, there are several different categories of parent-child privacy that courts have defined and protected. First, there is a right to raise children, including the authority to direct their religious and educational upbringing, which has been repeatedly recognized by the Supreme Court. Second, there is, at least under certain circumstances, a right to establish a relationship with a child that is explicit in cases involving unwed fathers.

One critical aspect of parent-child relational privacy concerns the right to raise a child in the manner that one chooses. In *Meyer v. Nebraska* (1923), the Court asserted that the right of liberty “denotes not merely freedom from bodily restraint but also the right of the individual to contract, to engage in any of the common occupations of life . . . to marry, establish a home and bring up children.”

Parental autonomy is not absolute. Indeed, although courts defer to the notion of parental control, the state can remove children from their parents' care for abuse and neglect, require children to attend some form of schooling, and establish a minimum work age for children. Moreover, just as with respect to other privacy rights, the constitutional reasoning that supports parental autonomy is somewhat sparse, even if it is grounded in pragmatic concerns. In *Meyer*, the Court explained that it had never posited a definitive explanation of the liberty guaranteed by the Fourteenth Amendment, but that “without doubt,” it included



the right to raise children. On the other hand, regardless of their legal basis, the cases can be seen as establishing a precedent for privacy.

A second aspect of parent-child privacy concerns the rights of men to have relationships with their children: a married man has the right to a relationship with a child, and an unmarried man has an enforceable right against an unmarried mother to establish a relationship with their child. In a series of cases beginning with *Stanley v. Illinois* in 1972, the Supreme Court considered the rights of unwed fathers. Generally, the Court has protected the rights of unwed fathers when they have lived with or established a substantial relationship with their children, unless the unwed father is asserting rights against an “intact” family.

In the first case, *Stanley v. Illinois*, the Court used procedural due process to find that an intact biological family could not be broken up without a hearing on the unfitness of the parents. The father in that case had lived sporadically with his children. Six years later, the Court held in *Quilloin v. Walcott*, that an unwed father who had not lived with his children could be denied parental rights based on application of the best interest standard. Allowing the new husband of the biological mother to adopt the children would help preserve an existing family unit, and because the biological father had never lived with the child or the mother, the Court held that the state could deem his rights inferior to the best interests of the child. One year later, however, the Court struck down a statute that precluded an unwed father from objecting to the adoption of his children since he had maintained a substantial relationship, had lived with and had acknowledged paternity of his children.

Then, in *Michael H. v. Gerald D.*, the Supreme Court upheld the constitutionality of a California statute that presumed that a child born to a married woman, who was cohabiting with her husband, was a child of the marriage, unless the presumption was challenged within two years. In that case, a man not married to the mother had a 98.07 percent probability of being the biological father; he sought to be declared the father under California law. Even though he had some established relationship to both the mother and the child, and had lived with them both, he had no constitutionally recognized legal rights as a father. A plurality of the Court opined that the family unit traditionally given respect did not include an unwed father who sought to establish a relationship with his child when the mother was married to someone else.

The unwed child cases can be reconciled to mean three things. First, unwed fathers have the opportunity, in certain circumstances, to establish relationships with their children. Second, preservation of the traditional family unit takes priority over the rights of even the unwed biological fathers who do establish a relationship with their children. Third, although a relationship may exist between an unwed father and his child, legal rights as a father may not always be recognized.

See also: **Children’s Online Privacy Protection Act of 1998 (COPPA); Privacy, definition of; Privacy, philosophical foundations of; Public/private dichotomy; Women and privacy**

Suggested Reading. Alderman, Ellen, and Caroline Kennedy. *The Right to Privacy*. New York: Alfred A. Knopf, 1995; Allen, Anita L. *Uneasy Access: Privacy for Women in a Free Society*. Totowa, NJ: Rowman and Littlefield, 1988; Ariès, Philippe, and Georges Duby (series eds.). *A History of Private Life*, vols. I–V.

Cambridge, MA: Belknap Press, 1992; Coontz, Stephanie. *Marriage, a History: From Obedience to Intimacy, or How Love Conquered Marriage*. New York: Viking Press, 2005; Cott, Nancy, and Lawrence Friedman. *Private Lives: Families, Individuals, and the Law*. Cambridge, MA: Harvard University Press, 2005; Eichbaum, June A. "Towards an Autonomy-Based Theory of Constitutional Privacy: Beyond the Ideology of Familial Privacy," *Harvard Civil Rights-Civil Liberties Law Review* 14 (1979): 361–384; Hartog, Hendrik. *Man and Wife in America*. Cambridge, MA: Harvard University Press, 2000; Mello, Michael. *Legalizing Gay Marriage*. Philadelphia, PA: Temple University Press, 2004.

Naomi Cahn

Family Educational Rights and Privacy Act (FERPA)

Few privacy laws affect the lives of parents and students on an everyday basis as does the Family Educational Rights and Privacy Act (FERPA). FERPA affords parents the right to inspect and review their children's education records; the right to seek to amend information in the records they believe to be inaccurate, misleading, or a violation of privacy; and the right to consent to the disclosure of **personally identifiable information** from the education records. When a student turns 18 years old or enters a postsecondary institution at any age, the rights under FERPA transfer from that student's parents to the student ("eligible student"). The FERPA statutory citation is 20 U.S.C. §1232g and its regulatory citation is 34 C.F.R. Part 99.

FERPA was one of the first federal privacy statutes passed by Congress. Senator James L. Buckley of New York was the main architect and legislative sponsor of FERPA, adding the provisions as an amendment to a pending education bill in the summer of 1974. By introducing this legislation, Buckley sought to address what he viewed as a violation of the rights of parents, who were being denied access to information schools maintained on their children, and to address a routine lack of privacy of students' education records. President Ford signed FERPA into law on August 21, 1974, with an effective date of November 19, 1974. On December 31, 1974, Senator Buckley and Senator Claiborne Pell of Rhode Island cosponsored major amendments to FERPA to address ambiguities that had arisen about the new requirements in the four months after its passage, making the changes retroactive to its effective date.

Simply put, FERPA protects the privacy of education records and the privacy interests of parents in their children's education records. FERPA does this by conditioning the receipt of federal education dollars by educational agencies and institutions on the condition of compliance with FERPA's requirements. As a general rule, FERPA applies to all public school districts and virtually all postsecondary institutions, public and private. Private schools at the K-12 level, for the most part, are not recipients of U.S. Department of Education funds and are, thus, not subject to FERPA.

The requirements of FERPA center on the definition of "education records." The term is broadly defined to mean all records that contain information directly related to a student and that are maintained by the educational agency or institution or by a party acting for the agency or institution. While parents and eligible students must provide consent before personally identifiable information from



education records is released, there are a number of exceptions to the general consent rule. Most of these exceptions are commonsense **disclosures** that allow schools to carry out the business of educating students, such as release of student information to school officials who have a legitimate educational interest; transfer of a student's records to a new school or college; disclosure of necessary information to state and federal education authorities for an audit or evaluation of education programs or for the enforcement of federal legal requirements that relate to education programs; disclosure of "directory information" (such as name, address, and major) on students for school yearbooks, plays, and sports events; and the release of information to appropriate authorities to address health or safety emergencies. At the postsecondary level, even though the rights under FERPA belong to the student, there are several exceptions to the general consent rule that permit colleges and universities to share information with parents without the eligible student's consent, most notably, an exception that allows disclosures to parents of students who are claimed as dependents for federal income tax purposes.

There is no specific exception to FERPA's general consent rule for the disclosure to noneducational agencies, although some of the exceptions could apply under certain circumstances. For instance, a student's health records, including immunization records, that are maintained by a school are considered education records and may not be disclosed to a local or state health department without consent. However, a school could use FERPA's health or safety emergency exception to disclose personally identifiable information from students' education records to local or state health authorities in a situation that presents imminent danger to students or other members of the school community, such as an outbreak of an epidemic.

Also, there is no specific exception in FERPA for disclosing education records to local or state law enforcement authorities, yet FERPA permits school officials to comply with lawfully issued subpoenas and court orders, as long as certain conditions are met. In addition, records that are created by a school's campus law enforcement unit for the purpose of maintaining a safe campus and reporting crime are not considered education records and, thus, may be shared with outside law enforcement authorities.

The Individuals with Disabilities Education Act (IDEA) works hand-in-hand with FERPA to protect the privacy of education records of students with disabilities. School officials must take into consideration both FERPA and IDEA when making decisions about disclosing education records of disabled students. IDEA contains safeguards and provisions not found in FERPA that afford additional rights to parents of students covered by IDEA.

The FERPA statute and regulations contain administrative enforcement provisions, including a complaint procedure under which parents and eligible students may file complaints with the U.S. Department of Education. A unique aspect of the FERPA enforcement provisions is the requirement that the department seek voluntary compliance from schools before proceeding with enforcement actions, such as withholding federal funds. Perhaps Congress was incorporating into FERPA a fundamental respect for the long-established view that local and state governments are to control education matters. Whatever the reason, it has worked well. For the most part, schools want to be in compliance with FERPA, and routinely request training

on the law and seek out technical assistance from the department regarding its application.

FERPA has been amended by the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)** to permit schools to disclose personally identifiable information on students to the U. S. attorney general in compliance with an ex parte order, a court order that is issued without the consent or knowledge of the parent or student, related to anti-terrorism activities. One of the more interesting aspects of FERPA is how it applies to disclosures that concern national security. Historically, FERPA has always permitted schools to disclose personally identifiable information from education records in order to comply with lawfully issued subpoenas and court orders, as long as the school made a reasonable attempt to notify the parents or students whose records were being requested, prior to compliance. In 1994 Congress amended that provision to permit educational agencies and institutions to disclose education records in order to comply with court orders or subpoenas issued for law enforcement purposes, without the required notification, if the court or issuing agency so ordered. More than likely, Congress made this initial change in order to assist law enforcement authorities with investigations concerning illegal drugs.

Today, education officials routinely address competing interests of privacy versus accountability, privacy versus safe campuses, privacy versus national security, and privacy versus an increasing demand for information. All in all, FERPA has worked well, and has provided parents and students with valuable privacy rights with regard to education records.

(The views expressed in the article do not necessarily represent those of the Department of Education or the United States government.)

Suggested Reading: Bakst, Daren, and Sylvia Burgess. *Privacy in the 21st Century: An Annual Review and Compendium for Higher Education Leaders*. Palm Beach Gardens, FL: Council on Law in Higher Education, 2002; *Brief of Eagle Forum Education and Legal Defense Fund as Amicus Curiae, Owasso Indep. Sch. Dist. No. 1-001 v. Falvo*, 534 U.S. 426 (2002) (No. 00-1073); O'Donnell, Margaret. "FERPA: Only a Piece of the Privacy Puzzle," *Journal of College and University Law* 29 (2003): 679-717.

Ellen Campbell

Federal Bureau of Investigation (FBI)

Created in July 1908 as the investigative division of the Department of Justice, the Bureau of Investigation (renamed the Federal Bureau of Investigation in 1935) has experienced a steady increase in its role and authority. At the time of its creation, the bureau had one supervisor and nine agents; by 2003 its personnel had increased to 27,856 (11,776 agents and 16,080 support staff). This growth captures the significant change in public policy and popular values that evolved during the twentieth century: the rejection of a states' rights tradition that feared centralized power, and thus viewed law enforcement as a local and state responsibility, to the acceptance of the need for and value of an inherently secret federal police force.

The resultant growth in FBI resources (with FBI appropriations increasing from an estimated \$329,824 in 1911 to \$4.3 billion in 2003) was accompanied by an



unprecedented increase in FBI investigative capabilities. This growth was accomplished through technological innovations such as **wiretapping**, bugging, data banks, and **computers**, as well as the use of break-ins to photograph confidential records, all of which posed potential threats to privacy rights. A more powerful FBI could obtain and then act upon information about the noncriminal personal and political activities of individuals and of the organizations with which they were affiliated.

Congress's enactment of legislation expanding federal responsibilities and **surveillance** authority compounded this privacy problem. These laws included criminalizing prostitution in 1910, proscribing pornography (as early as 1878), legalizing wiretapping and bugging in 1968, and authorizing roving wiretaps and computer, credit, and library searches without having to meet a "probable cause" standard of a federal law violation in 2001.

As one byproduct, FBI investigations of so-called White-Slave Traffic Act (also known as the Mann Act, 1910) cases moved beyond organized prostitution and resulted in FBI agents monitoring and maintaining information about illicit sexual conduct. For example, in 1925, FBI officials established a discrete "obscene file" to centralize and maintain a permanent collection of obscene and pornographic literature, paraphernalia, and films. These anti-obscenity initiatives became catalysts for a more benign view of the FBI. In 1946, FBI director **J. Edgar Hoover** extolled the "potential publicity value" of obscene literature investigations, observing that such investigations could also help curb "juvenile delinquency" and stymie "local vice and crime," because these were "stimulated through the circulation of pornography." The potential for abusing this information was furthered by new technology (wiretaps, bugs, databases, and computers) with FBI officials instituting a **National Crime Information Center** in 1967 that had terminal connections to all arrest and identification records developed by local and state police agencies. Nonetheless, the most far-reaching development affecting privacy rights stemmed from secret initiatives instituted in response to security concerns triggered by World War II, the Cold War, and the terrorist attack of September 11, 2001.

The perceived subversive threat posed by Nazi Germany and Soviet Russia, which culminated in U.S. military involvement in World War II and in the containment and nuclear deterrent policies of the Cold War, reshaped the FBI's role and contributed to Congress's and the public's acceptance of the need for secrecy. In August 1936, in an effort to anticipate espionage or sabotage, President Franklin Roosevelt issued a secret oral directive authorizing the FBI to conduct "intelligence" investigations. Intelligence investigations differed from criminal investigations, which were predicated on a probable cause standard, in that they were based on mere suspicion about an individual or organization, owing to ideology or sympathies. Four years later, in May 1940, Roosevelt issued a secret directive authorizing FBI "national defense" wiretapping, which was banned by a 1934 law. Meanwhile, on his own, J. Edgar Hoover authorized FBI break-in and bugging activities, dating from 1942 and in violation of the Fourth Amendment.

Intelligence investigations, moreover, led to the creation and maintenance of files that contained derogatory personal and political information and that were not finite in duration. A criminal investigation could be initiated on the premise that the subject was suspected of planning to violate (or had violated) a federal statute. Such investigations continued until prosecution was effected or when no

(or insufficient) evidence of a federal crime was uncovered; in both instances, the file then would be closed. Intelligence investigations, in contrast, did not focus solely on conduct but focused as well on intent, resulting in the collection of information about the subject's personal character, associations, social attitudes, and political activities. These investigations were not finite, and the resultant files were not necessarily closed should no evidence be uncovered of criminal conduct, such as espionage, sabotage, or terrorism.

Furthermore, the FBI began to maintain files on individuals whose names came up as a result of their association with the subjects of criminal or intelligence investigations. A file would be opened on an individual named in an ongoing investigation. Similarly obtained information would subsequently be added to the file. As a result, the FBI retained information on hundreds of thousands of individuals who might never have been directly investigated. The scope and contents of FBI records are suggested by released FBI files on prominent Americans, including First Lady Eleanor Roosevelt, Illinois governor and Democratic presidential nominee Adlai Stevenson, presidents John Kennedy and Dwight Eisenhower, Under Secretary of State Sumner Welles, anti-Vietnam War activist John Kerry, folk singer Pete Seeger, and feminist activist Gloria Steinem.

Significantly, information obtained through intelligence investigations could not be used for prosecutive purposes, whether because it was obtained through illegal investigative techniques or because it did not confirm a violation of a federal statute. Most FBI intelligence investigations uncovered no information about planned espionage, sabotage, or terrorist activities, but only about the subject's personal conduct and political activities. This violation of privacy rights was soon compounded by FBI officials' alternative tactics of using this information to contain or discredit radical activists and even prominent citizens.

At first informally and episodically, FBI officials in time sought to ensure that such sensitive information could be disseminated more efficiently. Beginning in February 1946, FBI officials launched an "educational" campaign to "influence public opinion" by using carefully orchestrated and camouflaged leaks through "available channels"; i.e., to favored reporters, columnists, editors, congressional committees, members of Congress, and prominent citizens. Specific recipients included conservative reporters such as Walter Trohan and Don Whitehead, members of Congress such as Senator Joseph McCarthy and then Congressmen Richard Nixon, congressional committees including the **House Un-American Activities Committee** and the Senate Internal Security Subcommittee, as well as trusted state officials and prominent citizens. FBI officials even devised formal programs to contain or discredit individuals whose political activities or personal conduct they deemed abhorrent. These formal programs included the **Counter Intelligence Program (COINTELPRO)** (1956), Sex Deviate (1951), Responsibilities (1951), and Mass Media (1955).

The origin and evolving purpose of the Sex Deviate program highlights the privacy problem posed by FBI officials' intrusive and secret methods. FBI agents began to collect and maintain information on homosexuals dating from 1937. Until 1951 no action was apparently taken as a result of this collection activity. In 1950, in a companion investigation to that triggered in response to Senator Joseph McCarthy's charges of "known Communists in the State Department," a special Senate commit-



tee launched an investigation into allegations of homosexuals in the State Department, based on the premise that the employment of homosexuals posed a security risk because of their vulnerability to blackmail. In response, in June 1951, FBI officials launched a code-named Sex Deviate program with the goal of purging suspected homosexuals from employment in the federal bureaucracy, judiciary, and Congress. By 1954, FBI officials also began disseminating information about suspected homosexuals to, at least, “proper” university and police officials “in appropriate instances where the best interests of the Bureau is [sic] served.”

Dating from 1940, moreover, FBI officials regularly forwarded reports (some volunteered, others in response to requests) to the White House about presidents’ political critics, including dispatching a special squad to the 1964 Democratic National Convention to monitor the contacts and report on the plans of civil rights activists aligned with the Mississippi Freedom Democratic Party. FBI officials also conducted leak investigations at White House request and (again at White House request) conducted “name checks” on specified reporters (Harrison Salisbury, Peter Lisagor, Ben Gilbert, Joseph Alsop); that is, they compiled memoranda summarizing all information in FBI files about the individual. A particularly egregious such action involved a November 1970 Nixon White House request that the FBI forward a list (and all relevant information) of homosexuals and “any other stuff” on members of the Washington press corps.

FBI dissemination activities could have posed a potential political problem for FBI officials because they contradicted their own protestations that FBI files were confidential, and that FBI investigations were confined to violations of federal statutes. FBI officials could be confident that their dissemination practices would not be compromised by White House officials who shared a mutual interest in maintaining secrecy. In the cases of the media and Congress, FBI officials adopted precautions to preclude discovery. First, they only leaked information to reporters or members of Congress whom they deemed reliable and who promised not to disclose FBI assistance because they shared a common political interest. In those cases when the recipient violated the condition of **confidentiality**, FBI officials severed relations, as in the case of Senator McCarthy in 1953, and in the case of the Senate Internal Security Subcommittee in 1954. Furthermore, FBI officials never provided recipients with FBI files or official memoranda. The relevant information was conveyed in a “blind memorandum” form. Blind memoranda were prepared on plain white, non-letterhead stationary, allowing FBI officials to deny truthfully that no official FBI record had been leaked.

Three examples capture the varied and problematic nature of the privacy threats posed by these covert practices. The first involved Hollywood actor Rock Hudson. In 1965 FBI officials uncovered information that the Hollywood actor was homosexual. They shared this discovery with President Lyndon Johnson, but while privately expressing concern that Hudson might play an FBI agent in a movie, there is no direct evidence that they sought to influence Hudson’s acting career.

The same was not true, however, for syndicated columnist Joseph Alsop. Having learned in 1957 that Alsop had been compromised in a homosexual tryst in Moscow, FBI officials briefed senior Eisenhower administration officials (Attorney General Herbert Brownell and White House aide Sherman Adams) about this matter as well as other information that the FBI had uncovered about Alsop’s sexual

proclivities. Infuriated by a series of columns that Alsop had recently published criticizing the Eisenhower administration's fiscal conservatism for contributing to a "missile gap," then Attorney General William Rogers contacted the FBI in 1959 to obtain a full report on Alsop's homosexuality, emphasizing his intention to share this information with senior Eisenhower administration officials and stressing that he would not "take responsibility for such information not going further." Briefed on this matter, Nathan Twining, the chairman of the Joint Chiefs of Staff, subsequently emphasized to Rogers the need to ensure that the publishers of Alsop's column learn of this information.

The third and most egregious example involved Civil Rights leader Martin Luther King, Jr. From wiretaps of King's office and residence and then bugs installed in King's hotel rooms as he traveled around the country, FBI officials learned of King's illicit sexual activities. In an effort to contain and discredit the civil rights leader, triggered in part by antipathy on learning that King would receive the Nobel Peace Prize, FBI officials unsuccessfully sought to interest various reporters in this scandalous information, and then sent a composite tape and an anonymous letter to King's residence, threatening to expose King's "hideous abominations" in an attempt to intimidate the civil rights leader or even provoke him to commit suicide. The letter ended, "You are done. There is but one way out for you. You better take it before your filthy fraudulent self is bared to the nation."

The scope of the FBI's violations of privacy rights and abuses of power became known only in the 1970s, as the result of the first-ever congressional investigation of the U.S. intelligence community, with special House and Senate committees obtaining access to heretofore secret agency records, and then as the result of the release of FBI records obtained under the **Freedom of Information Act**, which was amended in 1974. While the revelations contributed to a healthy skepticism of the FBI and a scaling back of FBI activities, Congress did not enact a legislative charter defining the parameters of the FBI's authority. As one consequence, the principal restrictions precluding future violations of privacy rights derived from executive guidelines. And, while Attorney General Edward Levi instituted relatively strict guidelines in 1976 intended to preclude "security" investigations from spilling over into monitoring political and personal conduct, these restrictions were rescinded by more permissive guidelines instituted by Attorney General William French Smith in 1983, ostensibly to address a new "domestic security" threat of terrorism.

While fears of domestic terrorism only became a major national concern following the September 11, 2001, terrorist attack on the World Trade Center and the Pentagon, FBI investigations of alleged terrorists had earlier spilled over into monitoring political conduct, as in the case of a 1981–1985 investigation of the Committee in Support of the People of El Salvador (CISPES), an activist organization critical of the Reagan Administration's Central America policy. In the years after 2001, and more intensely following the U.S. invasion of Iraq in 2003, FBI investigations have closely monitored Arab American citizens and alien residents and critics of the Iraq war. In contrast to Cold War investigations, these investigations could lawfully employ intrusive investigative techniques that had been authorized under the **Uniting and Strengthening America by Providing Appropriate**



Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act).

Once again, these investigations were not confined to suspected criminals (in this case, terrorists). The overwhelming majority of the alien residents detained in 2001 were found only to have overstayed their visas or relied on forged documents. Furthermore, although FBI officials during the period October 2001 through December 2002 recommended indictments in 98 terrorist cases, Justice Department attorneys brought charges in only 60 of the cases, rejecting the others either because of the “lack of evidence of criminal intent” or because a federal crime had not been committed. Of the 60 cases prosecuted, only 16 resulted in convictions. In one of these cases, however, Justice Department attorneys subsequently petitioned the court to drop the convictions of two defendants, conceding that exculpatory evidence had been withheld from defense attorneys and that a key government witness was unreliable. A grand jury investigation, aborted in 2004, moreover, confirmed that the targets of this inquiry were either students at Drake University or Des Moines, Iowa, peace activists who had organized a conference to rally opposition to the Iraq war. Publicity about the target of the subpoena led the United States Attorney in Des Moines to suspend this grand jury proceeding.

Because of stringent secrecy restrictions, it is impossible to evaluate the scope and impact on privacy rights of the FBI’s expanded surveillance instituted in the aftermath of the 2001 terrorist attack. The Des Moines grand jury proceeding is tantalizingly suggestive, and the targets of FBI surveillance knowable because of a decision to convene a grand jury investigation. Left unresolved is the question whether this instance of FBI surveillance of student and peace activists was atypical and whether, rather than attempting to prosecute dissidents, covert dissemination activities were undertaken as had been done during the Cold War.

See also: **Constitutional protections; Internal Security Act of 1950; McCarthyism; Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities**

Suggested Reading: Cunningham, David, and Barb Browning. “The Emergence of Worthy Targets: Official Frames and Deviance Narratives within the FBI,” *Sociological Forum* 19 (2004): 347–369; Federal Bureau of Investigation. <http://www.fbi.gov/>. Online, March 2006; Goldstein, Robert Justin. “The FBI and American Politics Textbooks,” *Political Science* 18 (1985): 237–246; PBS Now. *Going Undercover/Criminalizing Dissent?*; <http://www.pbs.org/now/politics/cointelpro.html>. Online, March 2006; Theoharis, Athan. *The FBI and American Democracy: A Brief Critical History*. Lawrence: University Press of Kansas, 2004; Transactional Records Access Clearinghouse. *TRACFBI*. <http://trac.syr.edu/tracfbi/>. Online, March 2006; Wolf, Paul. *COINTELPRO*. <http://www.icdc.com/~paulwolf/cointelpro/cointel.htm>. Online, March 2006.

Athan Theoharis

Fetal privacy. *See* Assisted reproductive technologies; Reproductive rights.

Financial Services Modernization Act of 1999

On May 6, 1999, the United States Congress effectively repealed the Glass-Steagall Act of 1933 by enacting the Gramm-Leach-Bliley Act (GLB Act). Thus, the barriers set up by the Glass-Steagall Act between commercial and investment banking companies were removed to pave the way for increased competitiveness and efficiency in the financial marketplace. For this reason, the GLB Act is often referred to as the Financial Services Modernization Act of 1999, as it recognizes the changes occurring in the financial services industry since the Great Depression. The three privacy components of this legislation are known as the Financial Privacy Rule, the Safeguards Rule, and the pretexting provisions.

The Financial Privacy Rule prevents the **disclosure** of collected nonpublic financial information to third-party companies without consent from the customer. The law states that all financial institutions must disclose their policy related to the sharing of private personal information and allows customers the option to prevent this information sharing in certain situations. In addition, customers must receive a copy of this policy statement no less than once every 12 months from their financial institution. In addition to the federal agencies assigned with enforcing these privacy requirements, state governments have been empowered to oversee financial service activities.

The Safeguards Rule states that financial institutions must create, implement, and sustain controls to keep their customer information secure. The Safeguards Rule applies to all customer financial information regardless of its source. This is applicable to financial institutions collecting and maintaining information on their own customers as well as other companies that use this information. Credit bureaus are required to maintain the same preventive safety measures concerning information pertaining to an individual's finances as apply to primary financial institutions.

Under Section 304 of the GLB Act, pretexting provisions protect customers of the financial institution from other individuals and entities that procure information pertaining to their personal finances using deceptive practices. If an individual is pretexting, he or she is providing fraudulent information in an attempt to acquire another individual's private financial data. Soliciting a third party to engage in pretexting is also illegal. Companies engaging in pretexting and selling this confidential information are subject to legal action under this legislation. Additionally, the victim may sue the pretexting individual or company in civil court for monetary damages.

The passage of this legislation poses some privacy issues to consumers by allowing the same holding companies to engage in a wide array of financial activities. Some examples of this broad scope include insurance underwriting, commercial banking and lending products, credit counseling, tax preparation, and investment products and advice as allowed after review by the Federal Reserve Board. If the holding company is deemed to be well managed and stable, the Federal Reserve Board may grant these extended services to holding companies of financial institutions.

This is just one of many bills that have been passed in recent years in an effort to help protect people from identity theft and unwanted usage of their personal information. This legislation enables federal and local agencies to penalize those misusing



nonpublic financial information. It also provides the victimized individual with a method to claim damages in certain situations of negligence or fraud.

See also: **Banking and financial records; Fair Credit Reporting Act; Identity fraud**

Suggested Reading: Broome, Lissa, and Jerry W. Markham. "Banking and Insurance: Before and after the Gramm-Leach-Bliley Act," *Journal of Corporation Law* 25 (2000). www.uiowa.edu/~lawjcl. Online, December 2005; Carey, Rick. "Protecting Privacy: The Gramm-Leach-Bliley Act Takes Effect," *CPA Journal* 72 (2002): 14.

Christine Berry Lloyd

Fingerprints and fingerprinting

Fingerprinting is the world's most widely used, and certainly one of its most trusted, biometric identifiers. Biometric identifiers use bodily attributes to link human bodies to archival records maintained by some organization, usually an agent of the state.

Fingerprints are representations of "friction ridge skin," a corrugated type of skin that covers the fingers, palms, and soles. This skin falls into general pattern types. The most common pattern types are called arches, loops, and whorls. The general patterns may be divided into varying numbers of subpatterns. Further variation may be found in the abrupt ending and bifurcation of ridges at seemingly random intervals.

It is widely assumed that each individual finger has a unique pattern of friction ridge skin. It has also been shown that the general topography of the friction ridge skin remains persistent throughout an individual's lifetime. An image of friction ridge skin can be created using ink or a **computer** scanning device in order to store a record of the individual's friction ridge skin for retrieval at a later date. Since the record is based on a purportedly nonrepeating, persistent, and difficult-to-alter bodily attribute, such records are considered less vulnerable to fraud or deceit than records based on such information as name or an identification number. Such a record-keeping system has numerous potential uses in governance and other areas.

Fingerprints have been used since ancient times in China, India, Japan, and elsewhere as signs or seals on documents. Not until the nineteenth century were finger prints adapted for bureaucratic record keeping. The initial developments in using fingerprints for record keeping took place primarily in India. Fingerprints were first used as signatures on contracts and for pensioner identification. Single prints were also used to identify opium cultivators, emigrants, and government workers. Using sets of ten prints for criminal records soon followed.

In order for states to use fingerprints for bureaucratic record keeping, it was necessary to devise a system of indexing records according to fingerprint patterns. Only with such a system could fingerprinting be used to correctly identify an individual employing an alias or using fraudulent documents. After initial researches by Henry Faulds and Francis Galton, working classification systems were devised almost simultaneously in 1894–1895 by Edward Henry, a British colonial official stationed in India, and Juan Vucetich, a police official in La Plata, Argentina.

There are three primary uses of finger prints. Deliberately recorded fingerprints may be used for *verification*. In such applications, the user claims a certain identity, and then the person's fingerprints are checked against a fingerprint record in order to verify that the person is who he or she claims to be. Such a use is common in banking and security, and for control of state disbursements. Deliberately recorded fingerprints may also be used for *archival* purposes. In such uses, an individual's fingerprints are checked against a database of fingerprint records indexed according to fingerprint pattern type. The archivist may then be able to determine whether the individual has a record in the database even if the individual gives false information. The most common such use is for criminal record keeping. Accidentally left fingerprints may also be used for *forensic* purposes. A fingerprint left at the scene of crime may be checked against a database or the prints of a group of suspects in order to associate an individual with a crime. This last use has fewer privacy implications.

The inclusion of citizens' bodily information in a government database raises a number of privacy issues. The creation of criminal records based on fingerprints has generated little opposition since convicted criminals were thought to be entitled to reduced privacy rights. U.S. law has been divided on whether the retention of fingerprint records of individuals who were arrested but not convicted (or of those convicted for juvenile offenses) constitutes an invasion of privacy that outweighs the state's issue in retaining such records. The predominant, though by no means universal, view is that retention is permissible. Arguments that fingerprint records violate the Fifth Amendment ban against self-incrimination also have not been successful. In fact, John Wigmore, a leading U.S. evidence scholar, has concluded that a person's fingerprint "is not testimony about his body, but his body itself."

Critics of **DNA** databanks today tend to cite "genetic exceptionalism" to argue, incorrectly, that fingerprints, unlike DNA, contains only identifying information, not information about race, gender, disease, or behavioral propensities. In fact, weak correlations have been found between each of these characteristics and fingerprint pattern types, but the correlations have not been strong enough to support any sort of action. The popular conception of fingerprints as being devoid of anything other than individualizing information has made fingerprinting immune to the sorts of privacy criticisms that have been based on the presence of hereditary, medical, and behavioral information contained in DNA.

Fingerprint databases had potential utility in many more areas than criminal identification. Early enthusiasts named banking, disaster victim identification, immigration, entitlement control, and protection against kidnapping or amnesia as areas of utility, and even promoted "universal identification." Fingerprints, however, rapidly acquired a "criminal stigma" that damped public enthusiasm for such uses. Among the most enthusiastic proponents of universal identification were Vucetich and his protégé Luis Reyna Almandos. After some initial progress, Argentines rebelled against the idea of universal identification, and Vucetich's reputation as a national hero was damaged by his efforts.

In the United States, government bureaucrats did succeed in creating fingerprint databases for immigrants, armed services personnel, civil servants, and schoolteachers. During the 1930s, police and government groups pushed universal identification.

But American citizens rejected the idea of universal identification, and three bills containing the idea failed to pass Congress between 1935 and 1943.

The idea of universal citizen fingerprint identification has not seriously been considered since that time. However, the U.S. government has continued to collect noncriminal fingerprints by exploiting the fingerprinting of the special categories discussed above. The U.S. **Federal Bureau of Investigation (FBI)**, whose fingerprint repository constitutes the largest biometric database in the world, recently announced that its civilian fingerprint file had surpassed its criminal file in size. Each file contains over 40 million records, and approximately 7000 records are added each day.

The digital storage of fingerprint records and recent developments in automated fingerprint search and retrieval software has greatly enhanced the potential utility of fingerprint databases for a multitude of purposes. Biometric identification is increasingly being proposed as a security solution in the post-9/11 world. For example, many states now record fingerprints in conjunction with issuing drivers' licenses, and some **credit card** companies and banks offer to encode fingerprints on cards as a security measure. Cheap fingerprint scanners that can authenticate identity are now used to control access to **homes, automobiles**, secure areas, and personal computers. Given these developments, collecting, storing, and using fingerprints will continue to raise privacy issues for a long time to come.

See also: *Davis v. Mississippi*, 394 U.S. 721 (1969)

Suggested Reading : Cole, Simon A. *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Cambridge, MA: Harvard University Press, 2001; Dilworth, Donald C. (ed.). *Identification Wanted: Development of the American Criminal Identification System, 1893–1943*. Gaithersburg, MD: International Association of Chiefs of Police, 1977; German, Ed. *Latent Print Examination*. onin.com/fp; Rodriguez, Julia. "South Atlantic Crossings: Fingerprints, Science, and the State in Turn-of-the-Century Argentina," *American Historical Review* 109, no. 2 (2004): 387–416; Sengoopta, Chandak. *Imprint of the Raj: The Emergence of Fingerprinting in India and Its Voyage to Britain*. London: Macmillan, 2002; Wigmore, John Henry. *A Treatise on the Anglo-American System of Evidence in Trials at Common Law Including the Statutes and Judicial Decisions of All Jurisdictions of the United States and Canada*, vol. 1, 2nd ed., 5 vols. Boston: Little, Brown, 1923.

Simon A. Cole

Florida v. Bostick, 501 U.S. 429 (1991)

In an effort to curb drug trafficking in Broward County, Florida, Sheriff's Department officers routinely and regularly boarded buses at scheduled stops to question passengers and seek their permission to search their luggage. Programs such as the one in Broward County have been implemented across the United States by various law enforcement agencies, and have led to the use of **surveillance** at bus stations, train depots, and airports. Law enforcement officers, stationed at these various locations, routinely approach individuals at random or because they vaguely suspect criminal activity or the presence of illegal drugs.

In this case, Terrance Bostick purchased a bus ticket from Miami to Atlanta. At a stop in Fort Lauderdale, two officers from the Sheriff's Department boarded the bus wearing jackets with insignias and badges, and one carried a zippered pouch easily recognizable as containing a pistol. The officers approached Bostick and, after matching his identification with his ticket, explained their presence as narcotics officers in search of illegal substances. After advising Bostick of his right to refuse, they sought permission to search his luggage. He gave his permission. The officers discovered cocaine in his second bag and placed him under arrest for drug trafficking.

At his trial, Bostick made a motion to suppress the cocaine on the grounds that it had been seized in violation of his Fourth Amendment rights. The motion was denied, and the Florida Court of Appeals affirmed the decision. The Florida Supreme Court, on certification, adopted a per se rule that the Sheriff's Department practice of bus checking was unconstitutional since a reasonable passenger would not have felt free to leave to avoid questioning. The United States Supreme Court granted certiorari to determine whether Florida's per se rule was consistent with Fourth Amendment jurisprudence.

The issue before the Supreme Court was whether a police encounter on a bus like the one in *Bostick* constituted an illegal search and seizure. In Justice O'Connor's opinion, she asserted the state conceded that the officers lacked the reasonable suspicion required to justify a seizure, and that if a seizure did in fact take place, the drugs must be suppressed as tainted fruit, pursuant to the fruits of the poisonous tree doctrine.

In the Court's analysis, O'Connor sets forth that a seizure does not occur simply because a police officer approaches an individual and asks a few questions, because it is consensual in nature and the individual is not being confined or detained. Citing a string of cases such as *Terry v. Ohio*, 392 U.S. 1 (1968), *California v. Hodari D.*, and *Florida v. Boyner*, O'Connor pointed out that the Court has consistently held that mere questioning does not trigger Fourth Amendment scrutiny unless it loses its consensual nature, and that law enforcement officers do not violate Fourth Amendment rights by merely approaching an individual on the street or in another public place, or by asking the individual if he or she is willing to answer some questions and then putting questions to the individual if the person is willing to listen. In the eyes of the Court, Bostick's encounter was no different than if he had been approached in the terminal or on a public sidewalk, and thus the fact that it occurred in the cramped confines of a bus made no difference.

In his argument to the Court, Bostick stated that a reasonable bus passenger would not have felt free to leave under the circumstances of this case because there was nowhere to go on the bus, especially since the officers towered over the seats and there was little or no room to move about. The Court disregarded Bostick's argument, stating that the confinement of the bus was a natural product of Bostick's decision to take a common carrier, and not the result of police conduct. Thus, his freedom of movement was restricted by a factor independent of police actions. Bostick was completely within his rights to disembark the bus and simply refuse to answer the officers' questions, even though it would have required more effort than walking past or ignoring an approaching officer. Given such reasoning, the Court



remanded the decision back to the Florida Supreme Court to determine the seizure question under the correct legal standard.

In the dissent's opinion, Justice Marshall agreed with the framing of the question to determine whether or not a seizure has taken place, but he disagreed with the majority's affirmative response. Marshall suggested that sitting on a bus and attempting to disregard a police inquiry is not the same as being stopped on the street. Had Bostick disembarked from the bus, it would have caused him either an economic loss—his luggage or the money used to purchase the ticket—or the inconvenience of having to obtain new transportation, or both.

Finally, the dissent argued that just because a person enters a room with only one exit does not give the police the right to enter the room and block the only exit. Nor is it permissible for an officer to exploit a person based on his or her decision to expose himself or herself to public or personal constraints. By consciously singling out persons who undertake interstate or intrastate travel, officers who conduct suspicionless, dragnet-style sweeps put passengers in the situation of having to choose between cooperating with an inquiry or exiting the bus. It is because of this forced choice that the dissent held the opinion that the conduct of the officers in the case of Bostick violated the Fourth Amendment.

See also: **Constitutional protections; Search warrant**

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

Matthew M. Dwyer

Foreign Intelligence Surveillance Act of 1978 (FISA)

The Foreign Intelligence Surveillance Act of 1978 (FISA), 18 U.S.C. 1801–1871, established a Foreign Intelligence Surveillance Court (FISC) to decide government applications to conduct **electronic surveillance** in the United States against foreign powers or their agents. “Agents” include persons engaged in international terrorism. The FISC’s approval authority has since been extended to cover surreptitious physical searches (“black bag jobs”), **pen registers** (capturing outgoing noncontent dialing, routing, addressing, or signaling telephone information), trap-and-trace devices (capturing noncontent incoming electronic impulses that identify the originating number), and compelled disclosure of “tangible records” by record holders such as telephone companies, banks, travel agencies, and libraries. The FISC is comprised of sitting federal judges who meet secretly at the Department of Justice. FISA targets are unrepresented in its proceedings.

FISA was enacted after the Supreme Court suggested that Congress constitutionally may enact lower standards for collecting foreign intelligence than for collecting criminal evidence. Congress authorized the FISC to approve electronic surveillance on a finding of probable cause to believe that the target was a foreign power or agent, and that the location of the **surveillance** was used by that power or agent. This standard is less exacting than the traditional finding of probable cause to believe that evidence of a crime will be found. The government must also certify, inter alia, that “a significant purpose” of the surveillance is obtaining foreign intelligence, and the government must state that it will follow procedures to “minimize” the acquisition and retention of information and limit the dissemination of nonpublicly available information about U.S. citizens and permanent resident aliens (“United States persons”).

The FISC may approve pen registers, trap-and-trace devices, and compulsory **disclosure** of tangible records following an even lower standard. The government must only certify to the FISC that the information is relevant to an investigation to obtain foreign intelligence that does not concern a United States person, or relevant for an investigation to protect against international terrorism or clandestine intelligence activities. This “mere relevancy” standard reflects Supreme Court decisions suggesting that people waive privacy protections of information they voluntarily convey to third parties such as telephone companies or banks.

No United States person may be considered a foreign power or agent, nor may the government investigate such a person, solely on the basis of First Amendment activities. On the other hand, FISA lets the government collect transactional information about even innocent U.S. citizens who are not foreign agents as long as the government asserts that the information is for a terrorism investigation.

Critics assert that FISA is a sham, emphasizing that through 2004 the FISC denied only 4 of 18,732 applications, and that the “mere relevancy” standard is toothless. FISA defenders respond that any prior judicial approval is better than none, and that the mere prospect of judicial decision disciplines the executive decisionmaking process.

*See also: **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)***

Suggested Reading : Bazan, Elizabeth B. *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions*. Congressional Research Service, Library of Congress, 2004; Federation of American Scientists. *Foreign Intelligence Surveillance Act*. www.fas.org/irp/agency/doj/fisa. Online, November 2005; Swire, Peter. “The System of Foreign Intelligence Surveillance Law,” *George Washington University Law Review* 72 (2004): 306–72.

Peter Raven-Hansen

Freedom of association

Associations require privacy from government intrusion. If the government prevents people from associating or tells them how and for what reasons they can act together as a group, associations cannot thrive. Associational freedom is especially important for unpopular or minority groups.



Freedom of association is not among the specific protections of the Constitution of the United States. However, the Supreme Court has recognized a right of association under the First Amendment. In early cases involving freedom of association, the Supreme Court found that government interference with membership in associations undermined the ability of people to engage in political advocacy. In more recent years, groups have asserted freedom of association as a defense against the application of laws prohibiting them from discriminating in their selection of members. While the Supreme Court has rejected claims that associations have a right to refuse to admit women as members, the Court has upheld the right of the Boy Scouts of America to discharge a gay Eagle Scout. In addition to the First Amendment protection for freedom of association, the Supreme Court has recognized that the Constitution also protects intimate associations, especially **families**.

Among the protections of the First Amendment are the freedom of speech and the right to assemble. The Supreme Court has interpreted the First Amendment to include also the freedom of expressive association: the right to associate for the advancement of beliefs and ideals. On this understanding, associations are constitutionally protected because they empower citizens to exert political influence and to keep government in check.

In the 1958 case of *NAACP v. Alabama*, 357 U.S. 44 (1958), the first case clearly recognizing this constitutional freedom, the Supreme Court held that requiring the NAACP to divulge its membership list to the government violated the members' associational rights. If the government was entitled to know the identities of the members, people would be less willing to participate, and the organization would be less able to engage in political advocacy. Nonetheless, three years after the *NAACP* case, the Supreme Court in *Communist Party of the United States v. Subversive Activities Control Board* (1961) upheld a federal order requiring the Communist Party to disclose its membership list.

In a series of subsequent cases, the Court followed the rationale of the *NAACP* case and recognized several ways in which government action unduly burdens the freedom of association. One way is by imposing burdens on specific kinds of associations. In *Healey v. James* (1972), the Court ruled that the Central Connecticut State College could not deny recognition and the use of campus facilities to a local chapter of Students for a Democratic Society (SDS). The Court found that withholding these privileges from one specific kind of organization without sufficient justification abridged the students' First Amendment rights to freedom of association.

Government action might also infringe associational freedom by imposing burdens on individuals because of their associational ties—thereby making membership more difficult. In *Shelton v. Tucker* (1960), the Supreme Court held unconstitutional an Arkansas statute that required teachers employed in a state-supported school or college to file an annual affidavit listing every organization to which a teacher had belonged or had contributed during the preceding five years. While the Court recognized that public schools have a legitimate interest in screening their teachers, the broad **disclosure** requirement unduly impaired the teachers' freedom of association because it required revealing membership in associations that did not bear on a teacher's fitness to teach.

A different way in which the government might infringe on associational freedom is by requiring membership in an association in order to receive a governmental benefit. Not all such schemes are impermissible. For instance, the Supreme Court has held that the government can legitimately restrict licenses to practice law to lawyers who join a professional bar association, although where an individual's political interests are implicated, the government has less power to compel membership in an organization. However, the Court has been less willing to sanction compelled membership that implicates political interests. In *Elrod v. Burns* (1976) the Court held unconstitutional the actions of a sheriff who discharged a series of public employees, including low-level security officers, because they were not Democrats. While the Court recognized that some kinds of government employment involving policymaking could legitimately require party loyalty, broader dismissals of this kind undermined associational freedom. Similarly in *Branti v. Finkel* (1980) the Court found unconstitutional the actions of a county public defender in discharging assistant public defenders because they were Republicans. Party affiliation had no legitimate bearing on serving as an assistant public defender, and so the government could not penalize Republicans by terminating their employment.

Freedom of association has arisen in cases involving unions. In early cases, courts viewed associations among co-workers as unlawful conspiracies. However, since the passage of the National Labor Relations Act in 1935, federal statutory law has safeguarded the rights of employees to associate in unions and to engage in collective bargaining with their employers. Employees can be required, pursuant to union-shop provisions, to join a union as a condition of employment, to finance activities of the union, and to be bound by agreements the union reaches with an employer. The Supreme Court has upheld these aspects of federal law while recognizing they implicate First Amendment interests.

Employees cannot, however, be forced to support a union's political speech. In the case of *Abood v. Detroit Board of Education* (1977), the Court held that non-union teachers in a public school could not be required, under an agency-shop provision of a collective bargain agreement between the union and the employer school board, to finance the expressive activities of the union. The union was only entitled to collect funds for advocacy from members who were willing to contribute, and noncontributing members could not be threatened with the loss of their jobs. A similar principle applies to bar associations. In *Keller v. State Bar of California* (1990), the Court held that although a bar association may use collected dues to fund activities germane to regulating the legal profession and improving the quality of legal services, where bar membership is required to practice law, the association may not use dues to fund more ideological activities. Bar members cannot be required, for example, to finance literature on the bar association's position on gun control laws.

Freedom of association has also arisen in cases involving political parties. In a series of cases addressing the procedures for selecting party delegates, the Supreme Court has underscored the associational rights of political parties and their members. In *Kusper v. Pontikes* (1973) the Supreme Court stated that the right to associate with the political party of one's choice is a basic constitutional freedom, and it struck down an Illinois statute prohibiting a voter from voting in the primary of one party within twenty-three months of voting in another party's primary. In *Cousins*



v. Wigoda (1975) the Court held that a state court injunction prohibiting a rival set of delegates from attending the 1972 Democratic National Convention violated the associational freedom of the enjoined delegates and of the National Democratic Party. In several subsequent cases, the Court invalidated on freedom of association grounds, legislative interference with the selection of convention delegates. The Supreme Court has also invoked associational freedom in invalidating governmental impediments to the formation of new political parties.

Political parties have at times sought the right to exclude individuals who apply to join, raising the issue of the extent of a party's freedom to choose its members. In a series of cases beginning in 1927, the Supreme Court invalidated efforts by the Texas Democratic Party to exclude African Americans from voting in the state Democratic primary elections. However, in these so-called White Primary Cases, the Court viewed the party's regulation of the primary as so closely tied to the general election process that it was governmental action rather than private associational activity. The Court therefore avoided determining whether the associational freedom of political parties extends to race-based discrimination in membership or other kinds of limitations on who may join.

An association's freedom to select its members free from government interference was central to two cases in the 1980s involving the ability of the Jaycees and Rotary to deny membership to women. In *Roberts v. United States Jaycees* (1984), the all-male Jaycees asserted that the application of the Minnesota statute prohibiting sex discrimination violated the organization's freedom of association. The Supreme Court disagreed and held that Minnesota could require the Jaycees to admit women as full members of the organization. The Court recognized that the Jaycees had a right of expressive association and that the organization engaged in expressive activities because it took public positions on issues and engaged in civic, charitable, lobbying, fundraising, and other activities worthy of constitutional protection under the First Amendment. In addition, the Court recognized that forcing a group to accept members it does not desire is an intrusion on the group and may impair the ability of the original members to express only those views that brought them together. Freedom of association, the Court said, presupposes a freedom not to associate. Nonetheless, the Court held, requiring the Jaycees to admit women did not unduly burden its associational freedom because the presence of women would not alter any message the Jaycees sought to communicate. The Jaycees could refuse members who did not share the organization's views. But the organization could not simply assume that women held contrary views and thereby exclude them wholesale from membership. There was no evidence that application of the anti-discrimination law would alter the Jaycees' expression, and to conclude otherwise required reliance on impermissible assumptions about the opinions of women. In a subsequent case, *Board of Directors of Rotary International v. Rotary Club of Duarte* (1987), the Supreme Court applied the same analysis and held that Rotary had no First Amendment right to exclude women in violation of the California Unruh Act. The Court concluded that the Act did not violate Rotary's First Amendment interests because there was nothing about the inclusion of women that would affect the organization's expression.

The Court's more recent decision in *Boy Scouts of America v. Dale* (2000) is difficult to reconcile with these two cases. James Dale, an Eagle Scout, had been

expelled as a member of the Boy Scouts of America (BSA) and as assistant scoutmaster of Monmouth Council, New Jersey, because he was gay. Monmouth Council officials learned of Dale's sexual orientation when they read in a newspaper about his role as co-president of the Rutgers University Lesbian/Gay Alliance. Dale claimed that in dismissing him, the BSA had violated a New Jersey law prohibiting discrimination on the basis of sexual orientation. The United States Supreme Court held that the application of the New Jersey statute to the BSA would violate its right of expressive association. The Court viewed the Boy Scouts as an expressive association: it instills values in its members and promotes its views in the broader community. Deferring to the BSA's assertion that its message included a disapproval of homosexuality—even though that message was not the organization's central purpose and some Scouts disagreed with the official position—the Court found that Dale's presence as an assistant scoutmaster would unduly burden the organization's expression. The BSA would be seen as approving of homosexuality if it was forced to allow gay leaders. The government, therefore, could not require the organization to abide by the nondiscrimination law. Some commentators view the Court's decision to extend associational freedom beyond its origin as a political right.

After the *Dale* case, to claim a right of expressive association, an organization must engage in some form of public or private expression. An organization does not have to associate for the purpose of disseminating a certain message in order to be entitled to First Amendment protection. The organization must merely engage in expressive activity that could be impaired. The First Amendment prohibits application of an anti-discrimination statute to compel an association to admit an individual as a member if the presence of that individual would significantly affect the association's ability to advocate its public or private viewpoints. In making that determination, deference is given to the association as to the nature of its expression and as to what would impair that expression. In addition to government regulations compelling an association to admit members, associational freedom might be infringed by government action imposing other kinds of burdens on associations or their members.

In the fall of 2005, the Supreme Court was called on to apply these standards to determine whether the faculty members of private law schools have an associational right to exclude from campus military recruiters who, in accordance with the governmental ban on openly gay individuals serving in the military, refuse to abide by the schools' policies of non-discrimination. A decision in that case is expected in 2006.

In addition to the First Amendment freedom of expressive association, the Supreme Court has recognized that there exists a constitutionally protected freedom of intimate association. The Constitution safeguards a **zone of privacy**, the Court has reasoned, in which highly personal relationships are protected from government intrusion. This is because personal bonds cultivate and transmit shared ideals and beliefs and provide a buffer between individuals and the power of the state, and because individuals derive emotional enrichment from close ties with others. Protecting intimate relationships from unwarranted state interference therefore safeguards people's ability to develop their identities and is an important component of liberty.



Freedom of intimate association is, however, quite narrow. The Supreme Court has found that marriage, parent-child, and similar familial relationships merit protection. The Court has also at times suggested that some small-scale, selective, and highly personal groups other than **families** might be sufficiently intimate to deserve constitutional protection. However, the Court has never specifically recognized a right of intimate association as belonging to any group or organization beyond the family setting.

See also: Constitutional protections

Suggested Reading : Abernathy, M. Glenn. *The Right of Assembly and Association*, 2nd rev. ed. Columbia, SC: University of South Carolina Press, 1981; Gutmann, Amy (ed.). *Freedom of Association*. Princeton, NJ: Princeton University Press, 1998; Mazzone, Jason. "Freedom's Associations," *Washington Law Review* 77 (2002): 639–767.

Jason Mazzone

Freedom of Information Act

The Freedom of Information Act is a federal law that gives any person the right to obtain public records from United States government agencies. The law's underlying rationale is that democracy works most effectively when the public has as much information as possible about the government, provided that disclosure will not harm the nation or individuals. In the forty years since the Freedom of Information Act's passage, the law has helped reveal fraud, waste, and corruption in the federal government. Coupled with the Privacy Act of 1974, the Freedom of Information Act gives people the right to obtain agency records about themselves and the inner workings of the government. Citizens submitted 3,266,394 Freedom of Information and Privacy Act requests in fiscal year 2003 alone, more than in any previous year.

President Lyndon Johnson reluctantly signed the Freedom of Information Act into law in 1966, noting his concern that the public's right to know could affect national security and privacy interests. Nearly a decade later, Congress overrode a presidential veto to bolster the law in the wake of the Watergate scandal and President Nixon's resignation. Changes to the law in 1974 significantly improved the public's ability to obtain information from the government. The Freedom of Information Act was amended again in 1986, when Congress exempted some **Central Intelligence Agency (CIA)** records from the law's provisions, and in 1996, when it was modified to include electronic records. The Freedom of Information Act creates a right of access to records maintained by administrative agencies, federal corporations, and other entities that perform work on behalf of the federal government. The law does not apply to records of the president, Congress, courts, private companies, or individuals. It also does not reach records held by state or local governments, although many of these entities have enacted their own open-government laws. More than fifty countries around the globe have enacted similar government transparency laws. The world's oldest freedom of information law was enacted by Sweden in 1766.

The Freedom of Information Act requires federal agencies to make information available to the public in three ways. First, each agency must publish information

about itself, as well as inform the public about how it can obtain information, make submissions or requests, or obtain agency decisions.

Second, the Freedom of Information Act requires that agencies make certain kinds of agency documents and records automatically available to the public. Categories of information covered by this requirement include certain statements of policy, interpretations, and administrative and staff manuals, as well as copies of records released to requesters that are likely to be requested by others. Each agency must make this information available in electronic form and hard copy. Most agencies meet this requirement by posting material on the **Internet** and maintaining it in reading rooms open to the public.

Third, agencies must disclose records in response to requests from the public. The law presumes that all material must be given to the public unless it is specifically exempted from disclosure. Records may be withheld from the public when they are (1) classified national defense or foreign policy information, (2) related only to an agency's internal rules and practices, (3) specifically exempted from disclosure by another law, (4) confidential business information such as trade secrets, and commercial or financial information, (5) interagency or intra-agency records that would be privileged in a lawsuit, (6) personal information that would invade a person's privacy if disclosed, (7) law enforcement records, (8) information used by an agency to regulate or oversee financial institutions, and (9) oil well data. These exemptions are to be construed by an agency as narrowly as possible.

Once an agency receives a Freedom of Information Act request, it must inform the requester within 20 working days whether or not it will release the requested information, and if not, the reasons why. A requester who receives a negative determination may file an appeal to ask the agency to reconsider. The agency must respond to the appeal within 20 working days. If dissatisfied with the result, the requester may file a lawsuit in federal court to enforce his or her rights.

An agency may make arrangements to process requests according to the amount of time or effort such requests will involve. For example, while an agency might typically process requests on a "first in, first out" basis, it might address a request for a specific record more quickly than a request for hundreds of records. Furthermore, if a requester can demonstrate a "compelling need" for agency records, the agency will give the request special priority and process it "as soon as practicable."

An agency may charge reasonable fees for the work involved in processing a Freedom of Information Act request. A requester who seeks documents for commercial use may be charged for the time and resources an agency spends searching for records, duplicating them, and reviewing them for information that should be withheld. An agency may only charge a fee for duplication costs when the request is from the news media or an institution whose purpose is scholarly or scientific research, and the request is not made for a commercial purpose. A noncommercial request from anyone else is subject to reasonable search and duplication fees. An agency may entirely or partially waive duplication fees if the requester shows that release of the records is in the public interest.

The Freedom of Information Act has interesting implications for personal privacy. While the goal of the law is government transparency, records sometimes contain intimate details about government employees and private citizens. Often it is clear that such information should be shielded from the public to protect an



individual's privacy. In other situations, however, an individual's personal information can actually contribute to the public's understanding of government operations. In these cases, it is less obvious whether the information should be made public or withheld in the interest of privacy.

The Freedom of Information Act provides two distinct exemptions for personal information. The law shields personal information in government records when disclosure "would constitute a clearly unwarranted invasion of personal privacy." The law also provides a specific exemption for personal information in law enforcement records when disclosure "could reasonably be expected to constitute an unwarranted invasion of personal privacy." Because association with a law enforcement activity can cause embarrassment and stigma, a person's privacy interest in the personal information contained in these records is typically more compelling than the interest in the personal information included in more routine government records. In fact, the Supreme Court has found that this privacy interest is so substantial that it may be claimed by close family members after a person's death.

Regardless of the type of government record that contains personal information, personal details will be released only if the public's interest in disclosure outweighs the individual's privacy interest in the information. Agencies cannot use personal privacy as a basis to withhold information individuals have requested about themselves.

See also: **Open meetings laws; Personally identifiable information**

Suggested Reading : Banisar, David. *The FreedomInfo.org Global Survey: Freedom of Information and Access to Government Records around the World*. http://www.freedominfo.org/survey/global_survey2004.pdf. Online, March 2006; Hammit, Harry, David L. Sobel, and Tiffany A. Stedman (eds.). *Litigation under the Federal Open Government Laws 2004*. Washington, DC: EPIC, 2004; Herbert, Foerstel. *Freedom of Information and the Right to Know: The Origins and Applications of the Freedom of Information Act*. Westport, CT: Greenwood Press, 1999; U.S. Department of Justice. *Basic Freedom of Information Act Training Manual*. <http://www.usdoj.gov/oip/trainingmaterials.htm>. Online, March 2006.

Marcia Hofmann

G



Garbage

Renowned archaeologist Emil Haury proclaimed, “If you want to know what is really going on in a community, look at its garbage.” Garbage offers a peek into the private lives of people and a glimpse of activities occurring behind the walls of a building. Garbage bins contain a wealth of items like food, clothing, and appliances; however, garbage is also a source of information providing insight into more personal matters through mail, memos, identifications, passwords, and **credit card** data. Supreme Court Justice White eloquently described garbage as revealing the “tell-tale items on the road map of life in the previous week.”

Most people never consider that the sensitive items they toss in the trash will be recovered. They should. There is no recognizable expectation of privacy in discarded materials left for collection. Trash reveals the intimacies of individuals’ lives, including eating, health, hygiene, political and sexual practices, financial dealings, personal relationships, reading, and recreational habits.

Although the most common item found in landfills is paper, there is no limit to the wealth of items and information set aside as trash. In fact, the culling through garbage is so pervasive as a means of collecting information that it has been given the scientific-sounding slang name of “garbology.” The actual practice of rummaging through commercial or residential trash to find useful discarded items or to extract confidential data and security-compromising information is called “dumpster diving.” Trash so defines a society and so exposes human activity that it is no wonder that trash is regularly studied and examined by anthropologists to learn about human behavior, by law enforcement to expose criminal behavior, and by reporters, thieves, and spies to gather confidential tidbits, steal identities and acquire trade secrets, respectively.

The extent to which the information and items referred to as garbage are protected from intrusive study and examination is a matter addressed by both the judicial and legislative branches. Until 1967, **constitutional protections** regarding privacy under the Fourth Amendment focused on arcane concepts of property and possessory interests in certain places: persons (their bodies and clothing), **homes** (apartments, motel rooms, businesses, barns), papers (documents, letters), and effects (cars, packages, luggage). The Supreme Court decision in the case

Katz v. United States, 389 U.S. 347 (1967) dramatically altered that principle by holding that the “Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public may be constitutionally protected” (*Katz* (1967), 361). A person’s entitlement to protection was not absolute or unlimited. Protection required both an actual, subjective expectation of privacy, and an objective, **reasonable expectation of privacy** that society as a whole would be willing to accept.

In *California v. Greenwood*, 486 U.S. 35 (1988), Justice White addressed this entitlement to privacy protection as it applies to garbage utilizing *Katz*’s two-prong test. White concluded that although individuals may have a subjective expectation of privacy in their garbage, it was not an objectively reasonable expectation of privacy that society was prepared to recognize. In other words, society is not about to manifest a constitutional protection of privacy to discarded trash. White provided three reasons for his conclusion: (1) It is common knowledge that plastic garbage bags left on a public street for collection are readily accessible to animals, children, scavengers, snoops, and other members of the public. (2) The items are placed there for the express purpose of conveying the bags to a third party, the trash collector, who might sort through them or permit others, such as the police, to do so. Finally (3) it is not reasonable to expect the police to avert their eyes from evidence of criminal activity that other members of the public may observe.

This decision to afford no constitutionally protected privacy interest in the content of trash left at the curb for garbage collectors was consistent with other recent Supreme Court holdings concerning the exposure of activities to third parties or items visible to the public. For example, there is no expectation of privacy in telephone numbers conveyed to a telephone company, to financial documents conveyed through a bank, or to activities in a backyard that are exposed to persons in aircrafts.

Justice White’s decision was firmly premised on the belief that society does not recognize a reasonable expectation of privacy regarding trash left for collection in an area accessible to the public. His decision was not predicated, as commonly believed, on the doctrine of abandonment. Abandoned property is not subject to Fourth Amendment protection because that protection only extends to places and items for which a person has a subjectively reasonable expectation of privacy, and no person can have a subjectively reasonable expectation of privacy about an item that has been abandoned. In fact, according to the rationale in *Greenwood*, a person’s subjective expectation of privacy is irrelevant to the holding concerning garbage and the right to privacy.

This distinction between the abandonment approach and the reasonable expectation of privacy approach is crucial. Many people, including Justice Brennan in his fervent dissent in *Greenwood*, subjectively believe that “the aspects of their private lives that are concealed safely in a trash bag will not become public” (*Greenwood* (1988), 46.) To that end, many like *Greenwood* are careful to conceal their trash even from the trash collector by using opaque, sealed bags. Others go to the extent of shredding their documents, burning their refuse, or co-mingling their waste with others. Still others, primarily business enterprises, in an effort to

prevent **industrial espionage**, provide physical security barriers like razor ribbon fences, security guards and dogs, and locks on their garbage containers. Individuals and businesses going to such lengths are hoping to limit access to the trash. All of these extra security and concealment practices, while effectively increasing one's subjectively reasonable expectation of privacy in one's garbage, do nothing to afford privacy protection in the content of the garbage. In the end, society will not objectively find a reasonable expectation of privacy in items left for collection by others.

In fact, because of the theoretical distinction made by the *Greenwood* holding, a person does not have the ability to protect his or her trash from intrusive examination. There is no distinction between private trash (trash that is meant to be kept secret until destroyed) and public trash (trash that is abandoned to the public). Once garbage is placed in the public domain, regardless of whether it is concealed in opaque, secured bags, shredded into potentially undecipherable 5/32-inch pieces, or placed in a locked storage receptacle, the garbage is still subjected to public disclosure. Hence, there is no privacy protection preserved. The concept may be illuminated by making the analogy between the disposing of trash and other scenarios. Just as a person engaging in a private conversation in a public setting or a home is subjected to the possibility that the conversation may be overheard by others if that person speaks too loudly, the disposing of trash in public poses the risk that it may be rummaged through and deciphered once it is placed on the curbside. In both situations, the expectation of privacy has been effectively eliminated by the individual's own action of speaking too loudly or placing the garbage out for collection.

The concept was exemplified in *United States v. Scott*, 486 U.S. 35 (1988). Therein, the shredding of tax documents into tiny strips did not deter the police from seizing the bits from the trash without a warrant, piecing the minute segments together, and using the evidence against Scott at trial. The mere fact that a person shredded the garbage before placing it outside of a home does not create a reasonable heightened expectation of privacy under the Fourth Amendment. The garbage was still discarded in an area particularly suited for public inspection and consumption. At most, the shredding made it less likely that third parties would be able to ascertain meaning from the documents. The Fourth Amendment does not afford protection even when a third party expends the effort and expense to solve the jigsaw puzzle created by shredding.

The *Greenwood* decision and its successors forewarned the industrial world that trade secrets placed in the trash in a discernible form were not legally protected either. Although dumpster diving is believed to be the number one method of business and personal espionage, the failure to take adequate precautions to protect a trade secret from clandestine trash searches precludes recovery even against one who may have used improper means to obtain it. Upon intentional, inadvertent, or accidental disclosure, the information ceases to be a trade secret and becomes public information. The fact that the information was disposed of in a manner constituting evidence of a subjective desire or hope that the contents would be unintelligible to competitive third parties does not change the fact that, as a result of the company's own actions, the trade secret was placed in the public domain.

A Pennsylvania manufacturing business learned this lesson the hard way when a competitor business ordered its salesperson to steal all of the other company's trash set out for collection in order to acquire its trade secrets. In *Frank W. Winne & Son, Inc. v. Palmer*, U.S. Dist. 11183 (1991), the result, both here and in the previously cited situations, was a failed attempt at **secrecy** by reason of underestimating a third party's (police or industrial spies) resourcefulness. It was not an invasion of constitutionally protected privacy. There is no constitutional protection from scrutiny as to information received from a failed attempt at secrecy. Simply stated, the test for determining legitimacy of an expectation of privacy is not whether the individual chooses to conceal private activity, but instead whether the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment. To that end, the public exposure of the trash bested Greenwood's, Winne's, and Scott's actions.

Horrific stories concerning wastebasket recovery applications abound. In *Greenwood*, the Court cited an incident in which a reporter seized the garbage bags of then Secretary of State Henry Kissinger and searched them to create a "newsworthy" and embarrassing story. Dumpster diving is commonly practiced by competitors seeking trade secret information and by watchdog groups hoping for information on organizations they are investigating. Some companies, like Weird Stuff, Inc., tout themselves as being in the business of salvaging and reselling discarded software, which they openly admit to obtaining by the practice of dumpster diving (*Novell, Inc. v. Weird Stuff, Inc.*, U.S. Dist. N.D. Cal. (1993)). The practice of raiding refuse makes consumer privacy obsolete and identity theft an easy task. Companies even advertise their dumpster-diving expertise in trade journals and on the **Internet**. They list their skills as high-tech forms of corporate espionage and publish instruction manuals on how to reconstruct shredded documents.

Congress's enactment of the Economic Espionage Act of 1996 (18 U.S.C. 1831–1839, enacting P.L. 104–294 (1996)) clearly reflects the national concern with trade secret theft and corporate dumpster-diving practices. The implementation of hefty criminal sanctions for those convicted of economic espionage (15 years) and the potential of a \$10 million fine for corporations that sponsor such activity highlight the abuse of clandestine trash searches further.

As the list of concerns mounts regarding the potential for exposure of private information through garbage disposal, a number of solutions have been devised. Effective June 1, 2005, the Federal Trade Commission (FTC) promulgated a rule requiring that whenever a business organization disposes of confidential personal information about employees, applicants, customers, and so forth, the organization must do so properly by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. Although the new rule (16 C. F.R. 683.3(a)) does not obligate businesses to either maintain or dispose of consumer or personal information in a certain time or in a specific manner, it does require that if the material is disposed, it will be disposed properly with privacy rights ensured. Of significant importance is the provision within the rule requiring the removal and disposal of all personal information from computers before the hard drives may be discarded or donated.

Since the *Greenwood* decision declined to provide privacy protection for garbage under the U.S. Constitution, several states and a village have provided their

own privacy protection for trash. For instance, the Village of Hamburg, New York, has increased awareness of the public quality of trash by requiring residents to stash curbside garbage in clear plastic bags so that officials may monitor those who do not comply with recycling laws. The mandate was deemed constitutional because it notified residents of their reduced right to privacy in garbage, and the law bore a reasonable relationship to the public goal of ensuring compliance without necessarily requiring physically ripping apart each bag to examine the contents.

New Jersey courts deemed that a person does have a **reasonable expectation of privacy** in the garbage left at curbside because the New Jersey Constitution requires only that an expectation of privacy be reasonable as established by general social norms. Thus, since most people in New Jersey rarely expose the content of the information in their trash to the public, that expectation of privacy is reasonable. Likewise, in *State v. Boland*, 115 Wn. 2d 571 (1990), the Supreme Court of Washington rejected the *Greenwood* approach. The state of Washington's constitution explicitly protects a citizen's private affairs, and since local ordinances govern and regulate trash collection, the state's citizens maintain a reasonable expectation of privacy that their trash will be collected and culled only by sanitation workers.

Other states have established constitutional protections from trash searches. The Vermont Constitution protects as private trash co-mingled with another's resulting from apartment-living status. However, in Washington, D.C., in the *Danai v. Canal Square Associates*, 862 A.2d 395, DC (2004) decision, the court held otherwise. The state of Hawaii recognizes a person's expectation of privacy in trash placed in an employer's receptacle. Connecticut passed groundbreaking legislation in 1997 when it revised Connecticut's trade secret law by designating dumpster diving as a form of espionage and an improper means of obtaining trade secrets. Although the law does not technically affect the public nature of garbage, it does afford trade secret owners with some protection. All of these state decisions (with the exception of *Danai*) suggest that a person's privacy interest in garbage demands a greater protection than the federal provision dictates.

Suggested Reading: Association of Science-Technology Centers Incorporated and the Smithsonian Institution Traveling Exhibition Service. *The Rotten Truth about Garbage* (1998). <http://alliedwasteservicesofcontracostacounty.com>. Online, March 2006; Baguchinsky, Jill. *Adventures in Garbology: What Trash Can Tell Us*. Ft. Myers, FL: Florida Gulf Coast University, 1999. <http://itech.fgcu.edu/&/issues/vol2/issue2/garbology.htm>. Online, March 2006; Rathje, William, and Cullen Murphy. *Rubbish! The Archaeology of Garbage*. Tucson, AZ: University of Arizona Press, 2001; Sherry, John. *Contemporary Marketing and Consumer Behavior: An Anthropological Sources Book*. Thousand Oaks, CA: Sage, 1995; U.S. Environmental Protection Agency. *Trends in MSW Generation 1960–2003*. <http://www.epa.gov/epaoswer/non-hw/muncpl/facts.htm>. Online, March 2006.

Jill Joline Myers

Gender

During the 1970s, when the women's liberation movement peaked in the United States, the slogan "the personal is political" became a popular feminist refrain. While most feminists adopted this motto in order to stress that traditionally "private" matters such as rape, domestic violence, and **sexual harassment** needed to be addressed on a

public level, it has been seen as a sign that feminists are, if not absolutely opposed, then at least highly suspicious of the right to privacy. While some feminists, such as Catherine Mackinnon, have denounced privacy as an inherently patriarchal value, an examination of mainstream feminist positions going back to the nineteenth century shows that women's rights advocates have generally struggled not to eradicate the boundaries between public and private, but to liberate women from their historical confinement in the private domain. Above all, feminists have stressed that sexual equality will not be achieved until there is general recognition of the role of gender in defining both the general concept of privacy and the traditional divisions between the public and private spheres.

In the United States, the women's rights movement preceded the Civil War, but it was not until the postwar period, after black men won the franchise and the word "male" had been specifically applied to voters in the Fourteenth Amendment, that the fight for women's suffrage became a militant national campaign. Throughout this era, however, the more women agitated for admission to public life, the more they were told that nature had designed them to devote themselves to homemaking, child-rearing, and other ostensibly sacred domestic duties. For example, when the Supreme Court upheld an Illinois court's rejection of Myra Bradwell's application to practice law in *Bradwell v. Illinois*, 83 U.S. 130 (1873), Justice Joseph P. Bradley, writing for the majority, held that it would be a violation not merely of social convention but of divine law if women tried to find fulfillment in the public sphere. "The civil law, as well as nature herself, has always recognized a wide difference in the respective spheres and destinies of man and woman," Bradley famously insisted, and "the constitution of the **family** organization, which is founded in the divine ordinance, as well as in the nature of things, indicates the domestic sphere as that which properly belongs to the domain and functions of womanhood."

In sanctifying women's place within the private realm, Bradley fell into step with the cult of domesticity that consumed nineteenth-century American society and shaped popular perceptions of privacy well into the twentieth century. Throughout this period, as modern methods of manufacture stoked the home-building, household goods, and advertising industries, an obsession with the material and moral ingredients required to make a happy **home** took hold of the country. Books, pamphlets, magazines, newspapers, and almost every other conceivable publication offered seemingly endless instruction on how to achieve domestic well-being. The most common admonitions were directed at women, drumming in the message that their first responsibility was to attend to the needs of their husbands and children, a duty that could best be carried out within a clean, well-organized, smartly equipped, and tastefully decorated private home. The cult of domesticity thus reinforced the doctrine of separate spheres by defining the home as the site of women's highest calling, and it also raised the value of privacy by popularizing the notion that every family ought to occupy its own private refuge, a haven that, if it were filled with the right consumer goods, would enable every family member to attain the moral attributes appropriate to his or her gender-specific position in the world.

The impact of the cult of domesticity is apparent in **Louis Brandeis** and Samuel Warren's essay, "The Right to Privacy," which was published in the *Harvard Law Review* in 1890 and went on to become one of the most influential and frequently cited articles in American legal history. In constructing the first systematic case for

a legal right to privacy, Brandeis and Warren complained that devices such as the telegraph and instantaneous photography had made it increasingly difficult for men to shield themselves and their dependents from public exposure and shame. Consequently, quoting Lord Coke's dictum that "every man's house is his castle," the authors maintained that the home, an evermore necessary refuge from industrial civilization, would cease to serve its purpose unless the heads of families were provided with more effective means to safeguard the sanctity of their homes.

Among the various examples they used to illustrate why men required these new protections, Brandeis and Warren singled out newspaper stories about sexual misconduct and intimate relations as an especially virulent blight on modern consciousness. In their view, the press needed to be prevented from circulating details about sexual transgressions, not so much because these revelations shamed the girls and women who were the usual victims, but more because such publicity dishonored the men who were supposed to protect them. To support this type of censorship, the authors pointed to legal fictions commonly used to address "intrusions by seduction upon the honor of the family," that is, cases of statutory rape or child molestation, which enabled fathers to collect damages against guilty parties without actually specifying the nature of the violation. Such legal devices conformed to social propriety, Brandeis and Warren maintained, because they allowed men to avenge outrages to their honor and reputation, but did not require further disclosure of ostensibly unspeakable crimes.

Although it took decades for courts to embrace the broad range of privacy protections envisioned in "The Right to Privacy," the notion that sexual misconduct should not be the subject of news reporting or public discussion became a widely accepted social convention for most of the twentieth century. Whereas nineteenth-century newspapers had routinely published accounts of rape and sexual molestation, usually providing the names and addresses of both perpetrators and victims, these stories became less common with the evolution of **journalism** as a profession and the rise of newspapers such as the *New York Times*. Articles on sexual wrongdoing did not vanish altogether, but in general, in stories in which the mention of sexual assault and misconduct could not be avoided, as in cases involving additional crimes, reporters resorted to euphemisms such as "nameless outrage," "violation of the home," or even "outrage against her husband" to refer to sexual attacks on women.

The effect of this configuration of the right to privacy was not only to reinforce barriers to women's participation in public life, but also to make it difficult or impossible for them to escape violence, injury, and oppression in the domestic sphere. The curtain that privacy defenders drew around the family home was not lifted after women won the vote in 1920, and the gentlemen's agreement that generally precluded reporting on sexual transgressions remained in place until the late 1970s. Likewise, the idea that women might forsake domestic duties in order to assume more active roles in public remains controversial today. Advocates for sexual equality, consequently, did not specifically oppose the right to privacy, but they protested the ways in which it barred women from the public stage while also obscuring their experience in the private domain.

The nineteenth-century doctrine of separate spheres has in important respects lost its grip on popular consciousness, thanks in large part to the efforts of 1970s

women's liberationists to subject previously private matters such as rape and domestic violence, as well as the unequal division of labor within the home, to the public scrutiny that privacy defenders such as Brandeis and Warren strove to avoid. Sexual inequality, well-known feminists such as Betty Freidan and Gloria Steinem argued, stemmed not only from the active exclusion of women from the higher levels of business, academia, and government, but also from the dependency, boredom, and in many cases, physical and emotional pain they suffered within the home.

In stark opposition to idealized conceptions of the domestic circle as the space in which women realize their deepest wishes by ministering to the needs their families, many 1970s feminists derided the life of the typical housewife as a brainless existence built on sexual submission, vapid consumption, and deep-seated anxiety about meaningless routines. Women's rights activists declared, first in consciousness-raising groups and then in public demonstrations, that sexual equality would not be achieved until women enjoyed parity on both sides of the **public/private dichotomy**, not only receiving equal pay for equal work, access to higher education, and unfettered opportunity in every profession, but also casting off primary responsibility for childrearing and other domestic cares.

Ironically, at the very moment women's liberationists began to issue public demands for freedom from the restrictive bonds of conventional marriage, exit from the stultifying dreariness of housework, and relief from sole responsibility for child care, the Supreme Court responded to the pressures of the sexual revolution by reasserting the conventional divisions between public and private life. In *Griswold v. Connecticut*, 381 U.S. 479 (1965), the Court ruled that the decision to obtain and use contraceptives falls within the boundaries of marital privacy. Citing the "penumbras," or shadows, cast by various amendments to the Constitution, **William O. Douglas**, who wrote the majority opinion, argued that the choices made by married couples in respect to family planning are contained within a **zone of privacy** into which the government should not intrude. The privacy claims that belong to married couples stood on special ground, Douglas argued, because the marriage bond involves principles that predate the Bill of Rights and pertain to a relationship that is as significant, if not more significant, than any other: "Marriage is a coming together for better or for worse, hopefully enduring, and intimate to the degree of being sacred . . . it is an association for as noble a purpose as any involved in our prior decisions."

A few years after *Griswold* was decided, in *Eisenstadt v. Baird*, 405 U.S. 438 (1972), the Court abruptly dropped its previous focus on marital privacy and held that unmarried persons should have equal access to contraceptives because the right to privacy belongs to individuals rather than to married couples. The Court did not explain why the right of association, which had been accorded such high status in *Griswold*, was no longer relevant. Instead, Justice William J. Brennan, who wrote the majority opinion, simply declared, "If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child."

Eisenstadt set the stage for *Roe v. Wade*, 410 U.S. 113 (1973), in which the Court found that a limited right to **abortion** is included in women's general right to

privacy, although the state may step in to regulate or prevent late-stage terminations of pregnancy. While these rulings were welcomed by feminists because they gave women some control over sexual reproduction, they were seen by many as inherently problematic because the Court failed to address the role of gender in limiting women's ability to make choices within the domestic sphere and in constricting women's access to the material means required to translate their choices into action. The principle of government noninterference that informed *Roe's* reliance on the privacy right was and has remained especially burdensome for poor and marginalized women because they have always been more likely to require public assistance to access medical services, more likely to be caught in dependent relationships, and generally less likely to be able to assert their political rights. However, when women's liberationists pressed for abortion on demand during the late 1970s, the Supreme Court answered in *Harris v. McRae*, 448 U.S. 297 (1980) that the government had no obligation to provide financial assistance to women who would otherwise be unable to afford medically necessary abortions.

Without pretending that the oppressive elements within prevailing perceptions of privacy have been entirely resolved, feminist theorists, most notably law professor Anita Allen-Castellitto, have argued that it makes more sense to re-envision privacy from a feminist perspective than to jettison it altogether as incompatible with equal rights. On the one hand, feminists such as Allen observe, exposing the private sphere to greater public scrutiny and regulation is bound to hurt women if the gender-based assumptions that frequently shape this exposure go unrecognized. On the other, promoting the notion that "the personal is political" without reservation seems to preclude even the possibility that women might enjoy a considerable degree of dignity and autonomy within the realm of home and family.

The solution, according to these feminist reconstructionists, is to formulate a more nuanced and accurate view of privacy, one that takes account of the real relief that may be gained from protection from public intrusion without denying the subjugation, loneliness, abuse, deprivation, and violence that too many women endure in their homes. "Choice," which is the shorthand typically used to refer to reproductive freedom and most closely tied to women's right to privacy, is, after all, a painfully empty concept to those who have no means to act upon their decisions. At the same time, a world in which women have even less control over personal information and less control over intimate relations, like one in which they have less control over reproductive choices, would clearly not bring them any closer to genuine equality in either the private or the public spheres. Thus, while there is no settled view of privacy among present-day feminists, there is general agreement that it will not become a truly positive value until it is paired with an understanding of the gender-specific limits that are still placed on women's agency on both sides of the public/private divide.

See also: **Women and privacy; Sexual violence**

Suggested Reading: Allen, Anita, and Erin Mack. "How Privacy Got Its Gender," *Northern Illinois University Law Review* 10 (1990): 441–454; Duke University Library. *Documents from the Women's Liberation Movement*. <http://scriptorium.lib.duke.edu/wlm/>. Online, March 2006; Landes, Joan B. (ed.). *Feminism, the Public and the Private*. New York: Oxford University Press, 1998; MacKinnon, Catherine. *Feminism Unmodified*. Cambridge, MA: Harvard University Press, 1987; McClain,



Linda C. "Reconstructive Tasks for a Liberal Feminist Conception of Privacy," *William and Mary Law Review* 40 (1999).

Susan E. Gallagher

Genetic information and testing

Genetic testing can be defined as any technique that can be used to gain information about aspects of an individual that are influenced, caused by, or controlled by genes. Defined this broadly, it encompasses methodologies not reliant on laboratory analyses or technology, such as the compilation of a detailed **family** medical history. In common usage, however, genetic testing usually refers more narrowly to processes used to determine the structure of an individual's genes and includes molecular testing (examination of DNA or RNA), microscopic examination of chromosomes, and biochemical tests that determine the presence or absence of gene products (proteins).

The privacy implications of genetic testing can vary as well as the technique employed. Depending upon the purpose of a genetic test and the surrounding circumstances, testing and the resultant information may have a profound impact on individual and family privacy or none at all. Perhaps most critical to this determination is the degree to which the identity of the individual who is being tested is linked to specimens and information throughout testing activities. These activities include the collecting of specimens or samples for testing, storage of samples (pre- and posttesting), the analysis itself, the storage of genetic information generated from the analysis (**DNA banking**), and **disclosures** of samples and data to third parties.

The informational value of a DNA sample can increase after the sample is collected from an individual because scientific breakthroughs in deciphering the genetic code and understanding the function of genes are continually being made. The scope of genetic tests now available illustrates the informational value of samples that have already been collected and hints at the range of information that might be culled from them in the future. In health care, genetic testing is used to identify predispositions to rare genetic diseases (e.g., Huntington's Disease), to predict response to drugs, to estimate risks for developing common illnesses (e.g., some cancers), and to determine carrier status for reproductive purposes. Outside of medicine, it is employed to identify bodily remains, connect individuals to criminal acts, and determine **paternity**. It has been incorporated into genealogical research and is used for marketing nutritional supplements and skin-care products to consumers. In the future it may be used to identify predispositions to injury or to screen for cognitive abilities and other traits unrelated to health.

Of course, not all the genetic information produced from testing is highly private, powerful, or sensitive; some genetic information is quite benign or obvious. But because much genetic information is highly personal, prolonged storage of, and easy accessibility to, identifiable samples (and genetic data) present significant risks to individual privacy. As this entry will illustrate, varying degrees of legal protections are available to mitigate those privacy risks, and just as there is no single comprehensive privacy law in the United States, there is no single comprehensive genetic testing or genetic privacy law. Consequently, one can best categorize the laws pertaining to genetic privacy as a patchwork of rights and protections that derive from constitutions,

statutes, regulations, and common law. Identifying and summarizing laws that regulate genetic testing and related privacy interests is further complicated by the fact that laws that do not explicitly refer to genetic testing or genetic information may nevertheless be interpreted to also apply to such matters.

Although there is no explicit provision in the U.S. Constitution that recognizes a right to privacy, a number of federal constitutional provisions have been interpreted to protect certain aspects of individual privacy from interference by state or federal government. When state governments exercise their authority through laws that restrict individual decisions, affected individuals may look to constitutional rights to privacy in formulating a challenge to that authority. Every state has enacted laws that authorize the compulsory collection and testing of DNA by law enforcement officials, although who can be compelled to provide samples varies from state to state. All states compel collection of samples from felony sex offenders, a majority of states extend their authority to include all convicted felons, and approximately half of the states authorize collection from individuals convicted of misdemeanors. A few states go so far as to include those arrested on suspicion of committing a crime (e.g., Texas). States contribute the genetic data generated under these laws to the Combined DNA Index System (CODIS), which is also the repository of genetic information about individuals convicted of violent crimes under federal law. CODIS is maintained by the **Federal Bureau of Investigation (FBI)**, and it enables federal, state, and local crime labs to exchange and compare DNA profiles electronically.

The type of genetic profiling authorized under these statutes involves decoding regions on the human genome that are sufficiently unique so as to be useful for identification purposes but which are not generally thought to contain information associated with any known physical or mental traits. When most of these laws authorizing such DNA profiling were enacted, the privacy interests affected by such testing were therefore viewed as deriving primarily from the compulsory aspect of the testing, rather than from the nature of the information produced. But more recently, studies have questioned whether the regions of DNA involved should be viewed as “junk DNA” that is devoid of any personal information. Therefore, in the future when more is known about how DNA functions, the privacy implications of such testing may come to be viewed differently. The constitutional challenges raised thus far in regard to such forensic testing have been based on the Fourth Amendment guarantees against unreasonable search and seizures and the protection of personal security. The Supreme Court has yet to review and rule on the constitutionality of any of these statutes. But the federal circuit courts that have reviewed these Fourth Amendment claims have declined to find any of these statutes to be in violation of the U. S. Constitution.

Genetic testing conducted by governmental agents for entirely different purposes has also been challenged on constitutional grounds. In 1995 employees in a federally funded research laboratory brought a lawsuit against their employers claiming that they had been subjected to nonconsensual testing for several conditions, including sickle-cell trait, and that the testing violated (in addition to some other statutes) their rights to privacy as guaranteed by the constitutions of California and the United States. The trial court dismissed the plaintiffs' claims, but in *Norman-Bloodsaw v. Lawrence Berkeley Laboratory*, 135 F3d 1260 (9th circuit



Feb. 3, 1998), the circuit court reinstated the constitutional claims, recognizing that few subject areas are more personal and more likely to implicate privacy interests than one's health or genetic makeup. As a result, the case went back to the trial court. Neither the California Supreme Court nor the U.S. Supreme Court has subsequently addressed or ruled on the privacy issues raised in the *Bloodsaw* case. Therefore, the relationship between constitutionally protected rights to privacy and secret or nonconsensual, genetic testing of governmental employees has yet to be authoritatively defined by any court.

Regardless of whether the U.S. Constitution places restrictions on how the government obtains, uses, or disseminates genetic information, an executive order issued by President Clinton in February 2000 limits the use of genetic testing in federal employment. Under Executive Order 13145, federal employers are prohibited from discriminating against their employees on the basis of genetic information and are further prohibited (with a few exceptions) from disclosing genetic information about an employee or any member of a federal employee's family. As long as this order remains in effect, the genetic privacy of federal employees is protected to the extent that they should not be subjected to nonconsensual genetic testing at work.

In the 1970s states began enacting laws to protect individuals with specific genetic traits from being discriminated against on the basis of those traits. Typically, these statutes addressed sickle-cell disease, thalassemia, Tay Sachs, and cystic fibrosis as the traits of concern, and extended protection to individuals who either had these genetic conditions or were carriers of the conditions. For the most part these laws regulate how information regarding the traits could be used in the employment and insurance arenas; they do not restrict how the information might be acquired in the first place, nor do they restrict disclosures or sharing of information about these, or any other genetic diseases, outside of employment or insurance. Consequently, they provide little in the way of privacy protections, even for those affected by one of the named conditions.

A second wave of genetic legislation that began across states in the early 1990s had the primary purpose of protecting economic interests that might be affected as a result of the expansion of genetic testing and thereby greater opportunities for genetic discrimination. These statutes mainly focused on regulating uses of genetic information in health insurance and employment, and incorporated privacy protections to varying degrees. Wisconsin is credited with being the first state to generally ban genetic discrimination in employment and to ban genetic discrimination in health insurance. By 2000, a majority of states had enacted genetic anti-discrimination laws that apply to health insurance and employment practices. Commonly, these statutes regulate the extent to which an insurer or employer can request or require that individuals disclose genetic information to them or undergo testing that would generate genetic information. Thus, these laws are based on the notion that genetic information should be treated differently from other personal or health information, but many states limit this policy of so-called genetic exceptionalism to the realms of insurance or employment. Consequently, they might guard against situations where an insurer or an employer would know more about an individual's genetic information than the individual would know, or would choose to know, about himself or

herself, but they do not provide any privacy protections for genetic testing or genetic information that results from occurrences elsewhere.

States also determine the impact of statutory rules through the definitions that are employed within a statute. Here, the scope of definitions employed for genetic testing and genetic information affects the reach of protections that statutory rules provide. Some states, like New Mexico, define genetic information broadly to include information about the genetic makeup of a person or members of a person's family; information resulting from genetic testing, genetic analysis, or DNA composition; information that an individual has participated in genetic research; or information related to the use of genetic services. Other states define it more narrowly. For example, Maryland defines genetic testing as laboratory tests of human chromosomes or DNA, thus excluding any other methods by which genetic information can be generated.

Some states have taken a wide view toward protecting genetic privacy and regulate genetic testing regardless of where it occurs. For example, Illinois prohibits genetic testing by anyone (not just health insurers or employers) without the individual's informed and written consent. These states also treat information derived from genetic testing as confidential and privileged, and as a general rule permit releases of genetic information only to the individual tested or to persons specifically authorized in writing by that individual to receive the information.

Another factor influencing the impact of state regulation of genetic testing and information is the inclusion in some statutes of what are referred to as sunset provisions. As a result, in those states, additional action is required by the state legislature for the rules to remain in effect after the specified date. For example, in Massachusetts the rules governing genetic testing and use of genetic information in life and disability insurance expired at the end of 2005, but rules governing genetic testing (and disclosures of genetic information) within health care are not subject to the sunset provision and consequently remain in effect.

In order to thoroughly protect privacy, however, legislation should also address routine destruction of samples as well as routine destruction of genetic information that is maintained in an individually identifiable form, include stringent penalties, and provide for strict enforcement. While some states provide statutory penalties, most often in the form of monetary fines for violations, and grant enforcement authority to one or more state agencies, few require routine destruction of samples in order to guard against unauthorized testing.

The impact that state insurance laws described above can have on protecting privacy is further tempered by the Employee Retirement Income Security Act of 1974 (ERISA), a federal statute that removes some employee benefit plans (including health plans) from the reach of state insurance laws. Therefore, individuals in states that have enacted such laws may not be protected by them, depending upon how they obtain their health insurance coverage. Several bills that would remedy this disparity have been introduced in Congress. One such proposal, the Genetic Information Non-Discrimination Act of 2005 (S.306), passed the Senate in February 2005. An identical bill was introduced in the House shortly thereafter and referred to several committees for consideration, but to date no federal law has been enacted that contains provisions comparable to these state insurance and employment laws.



One federal statute, the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**, provides some protection from discrimination on the basis of genetic information to individuals when they move from one health plan to another. However, it does not put restrictions on the collection of genetic information by insurers, prohibit insurers from requiring an individual to take a genetic test, or limit the disclosure of genetic information by insurers, and therefore it lacks any privacy provisions.

Regulations issued by the U.S. Department of Health and Human Services under HIPAA, often referred to as the HIPAA Privacy Rules, regulate disclosures of individually identifiable health information held by most health care providers, health care clearinghouses, and health plans. Any genetic information that fits the definition of health information as used in these regulations would be protected as well.

The HIPAA regulations do not preempt any state laws that protect health information more stringently than those regulations. Consequently, the more stringent state laws would apply to actions in states that have enacted what have been referred to as genetic exceptionalism statutes. This includes amendments to existing medical information laws that provide additional rules and special protections for genetic information as well as statutes dedicated to protecting genetic information regardless of the context in which it is created, stored, or disclosed.

In regard to genetic information that would fall outside medical record or health information laws (because of who holds the information or how it was created), individuals would need to look to common law for protection of genetic privacy. No court has yet applied any of the common law protections of generalized privacy interests to circumstances involving nonconsensual genetic testing, unauthorized disclosure of genetic test results to third parties, or publication of private genetic information.

See also: **Confidentiality; Constitutional protections; Personally identifiable information; Privacy and inequality; Workplace privacy**

Suggested Reading : Cole, Richard. "Authentic Democracy: Endowing Citizens with a Human Right in Their Genetic Information," *Hofstra Law Review* 33 (2005): 1241–1303; Johnson, Alissa, and Cheye Calvo (eds.). *Genetics Policy Report Privacy*. Denver, CO: National Conference of State Legislatures, 2002; Roche, Patricia, and George Annas. "Protecting Genetic Privacy," *Nature Reviews Genetics* 2 (2001): 392–396; Rothstein, Mark (ed.). *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*. New Haven, CT: Yale University Press, 1997; Smith Alling Lane, P. S. *DNA Database Laws Qualifying Offenses*. www.dnaresource.com. Online, January 2006.

Patricia A. Roche

Global Positioning System (GPS)

The premier satellite-based radio navigation and position-finding system, GPS, was designed and deployed by the U.S. Department of Defense in the late 1970s and has become generally synonymous with such systems, despite the availability and continued development of alternatives such as the Soviet *Glonass* system and the European Union's proposed *Galileo*. GPS now underpins a vast array of defense, commercial, and civil applications, although it was initially conceived to support the American military's demand for worldwide, all-weather, high-precision navigation

and weapons delivery. As a state-controlled, “dual-use” (i.e., military/civil) system of global purview, GPS has raised a number of complex issues in technology regulation, state sovereignty, and the militarization of civil society. Its privacy implications, however, might be less clear, in that GPS satellites are effectively little more than sophisticated radio beacons, allowing receiving devices to compute their three-dimensional positions at a specified time.

It is when GPS is integrated with other technologies that a broad spectrum of privacy concerns results, if privacy can be construed as the ability to conceal or control one’s communications and information about oneself. Technologies that record or transmit location information elsewhere (such as **cellular telephones** or vehicular tracking devices) or that use it to constrain movement (devices that administer progressively stronger electric shocks to children or incarcerated individuals as they stray further into proscribed regions) are pertinent examples. GPS has undeniably changed the field of navigation forever, but in concert with associated technologies, it has yielded a whole new constellation of privacy concerns.

As with any satellite-based positioning system, GPS comprises three segments: a “constellation” of earth-orbiting satellites, a network of ground tracking and control facilities, and a radio receiver, typically operated by an individual user. The satellites are arranged in orbit so that every point on the earth has a direct line-of-sight to at least four of them at all times. Time signals from ultra-precise atomic clocks on board the satellites are encoded and transmitted via radio, along with the satellites’ positions and various corrective information. Individual receivers (bearing lower-precision quartz clocks) compare these time signals with their own, computing the satellite-to-receiver travel time of the signals and thereby the distance. Once the distance and location of four such satellites is known, position in three-dimensional space (e.g., latitude, longitude, and altitude) can be determined using a geometric computation known as *trilateration*.

The privacy implications of GPS precipitate from three distinct developments over its 30-year history. The first centers on the opening up of GPS to civilian users, analogous to the shift by which ARPANET became the **Internet**. Following the 1983 downing of Korean Airlines flight 007 by military aircraft when it strayed into Soviet airspace, President Ronald Reagan announced publicly that GPS signals and technology would be made available internationally for civilian use, thereby helping to keep civil aircraft on course. Regulatory developments over the next fifteen years catalyzed a number of civil-sector uses of GPS—surveying in particular—by ensuring the accessibility of satellite signals, fostering the design of less-expensive receivers, and adopting or publishing GPS standards. Under President Clinton, the May 2000 shutoff of “selective availability”—an intentional blurring of GPS signals for nonmilitary users—improved precision for many by an order-of-magnitude almost overnight, thereby laying the groundwork for a commerce in high-precision (and potentially sensitive) location data.

Improvements in both *timeliness* and *resolution*—that is, the precision with which position can be determined—constituted a second development with direct consequences for privacy. The timeliness with which position can be ascertained depends on a number of factors, such as the number of satellites that can be simultaneously acquired by a given receiver, but for most purposes, position can effectively be updated continuously and instantaneously using GPS. Since its inception,



the resolution of GPS was high compared to other position-finding systems, and that resolution has steadily increased since deployment began. Continuous position-tracking at better than 10-meter resolution is essential for a whole host of applications, such as the navigation of individual vehicles in dense urban areas. While many techniques for tracking position have been devised, most provided only direction or rough location, and/or were limited to city-sized regions or smaller. Instead of exotic equipment that indicates approximate location (perhaps only of subjects within the local metropolitan area), GPS is comprised of commonly available signals and equipment that can provide a current location to within earshot, anywhere on earth.

Finally, a third development key to privacy considerations has been the continued reduction (through electronic microminiaturization) of the physical size of GPS receivers. The capabilities of the suitcase-sized devices of only two decades ago can now be packaged into cellular telephones or wristwatches, with further miniaturization envisioned. In the mid-1990s the proliferation of cellular telephones in the United States caused a dramatic rise in emergency calls, but in many cases the caller was unable to identify his or her precise location. As a result, the FCC ordered cellular providers to build position-finding into their systems, making miniature GPS receivers an attractive add-on to cell phones. The current (and envisioned) enhancement of the cellular phone as a position-finding device has spawned a new information services sector referred to as *location-based services* (LBS), wherein information presented to a cell phone user is modified according to his or her location (GPS-determined or otherwise). Commercial vehicular navigation systems, for example, display a map of the local area without the need for the user to enter his or her current position. GPS-equipped cellular phones themselves could allow urban pedestrians to quickly locate nearby facilities in unfamiliar cities, or act as a medium for localized advertising—while potentially making phone records a record of personal location as well. Receivers small enough to be worn or subcutaneously implanted have engendered further civil applications, including the monitoring of traffic, pets, livestock, criminals, mental patients, or even children. In 2001 the Digital Angel Corporation began offering patented, GPS-based technologies for just such applications.

The profit to be made from this growing array of applications is making “locational information” a valuable commodity to be bought and sold in the same way as telephone numbers or demographic profiles. Location is the principal index of geographic information systems (GIS), the spatially organized databases increasingly used to visualize communities and the environment. Further, recent national and international efforts to develop spatial data infrastructures are indicators of the increasing societal significance being placed on having access to up-to-the-minute location. By both delineating a uniform spatial grid encompassing the globe and by providing a mechanism for instantly determining one’s location on that grid, GPS is a foundational technology that has added location to identity, communication, property, and the other aspects of social life sometimes conceived of as public or private.

Suggested Reading: Caslon Analytics. *Caslon Analytics Privacy Guides: Spatial Privacy*. <http://www.caslon.com.au/privacyguide19.htm>. Online, March 2006.; *GPS World*. <http://www.gpsworld.com>, Online, March 2006; Monmonier, Mark.

Spying with Maps: Surveillance Technology and the Future of Privacy. Chicago, IL: University of Chicago Press, 2002; Pace, Scott, Gerald Frost, Irving Lachow, David Frelinger, Donna Fossum, Donald K. Wassem, and Monica Pinto. *The Global Positioning System: Assessing National Policies*. Arlington, VA: RAND, 1995; Pickles, John (ed.). *Ground Truth: The Social Implications of Geographic Information Systems*. New York, NY: Guilford Press, 1995.

Lane Denicola

Gossip

Gossip is a particular kind of communicative activity that typically involves the sharing of unfortunate, unsavory, or unflattering information about the private affairs of others not present. Gossip has a typical structure in social interaction, and its participants occupy a typical set of social roles. Gossip is usually surreptitiously accomplished in small groups of trusted others in face-to-face interaction, although its content may also be conveyed via phone, **electronic mail**, and letter. Although the discharge of gossip usually focuses on its purveyors, gossip cannot exist without purveyors and audience members; nor can it exist without the persons who are its subject in absentia.

As an organized activity, gossip typically includes a tacit agreement, between purveyors and listeners, that the information shared will be kept private among those included in the conversation, or at least that the purveyor of its contents will be kept confidential among those participating in the conversation. This is often accomplished by using phrases that conceal the source or purveyor of information, such as “I heard . . .” This assumptive procedure also provides purveyors with a convenient disclaimer of responsibility for the truthfulness of the information being shared.

Like stories in general, what matters about the authenticity of gossip’s content is not its truthfulness, but rather the degree to which people regard it to be true, and whether or not it is meaningful to listeners and thus worthy of sharing with others. The nature of gossip as a private conversational activity with unverifiable origins casts doubt on its reliability. As such, gossip does not hold the same ontological status as other kinds of talk, and it is commonly relegated in everyday life to the level of rumor. “Hearsay” is legally disregarded as legitimate testimony in courts of law in the United States because of the shaky ground on which it stands. Depending on the severity of its content, whether what is being shared is purported to be true or can be proven to be true, and whether or not its sources can be identified, the subject likely has little recourse against allegations even to the legal status of libel, slander, or defamation of character. The structure of gossip previously described makes such action prohibitive.

For many years, social researchers overlooked gossip, or perhaps regarded it as trivial and unworthy of scientific investigation. However, in the last three decades, sociologists have begun to recognize and take seriously gossip as an important feature of social life in the subfield of micro-sociology, the study of human behavior in face-to-face interaction. Several sociological studies have discussed the social roles, social organization, social and moral consequences, and social functions of gossip.

The three social roles associated with gossip—the absent subject, the purveyor, and the audience—are all moral actors in the context of gossip. Gossip’s subject matter, the private affairs of others, most obviously bears on the reputation or moral

standing of its absent and unwitting subjects. The subjects of gossip are typically excluded altogether from the information being discussed by others and exhibit no control over its content, meaning, or audience. To the extent that such information becomes known to subjects, the persons whose private affairs are being discussed are likely to perceive gossip as an invasion of privacy. To the extent that the information is perceived as real or true, gossip deprives a person of the ability to participate in the construction of his or her own social reality or to manage impressions of the self. Because gossip incapacitates the subject's ability to control information about the self, it represents the opposite of impression management, one's ability to perform the self, in form and content, and may have further consequences for one's relationships with those "in the know."

The social role of the purveyor includes the ability to exercise control over who is included and who is excluded in the immediate discussion, and what information is relayed and withheld in that encounter. While the consequences of gossip are usually thought to bear most upon the reputation or social status of those being discussed, gossip bears on the moral status of its purveyors as well. What is communicated by purveyors is likely to say as much or more about them as about the subjects being discussed. Through gossip, purveyors perform and reveal themselves, their interests and values, to a chosen audience. Gossip may also bear on its purveyors in another, more salient, way. Given the high cultural value placed on individual privacy, especially in the United States, as well as the expectation for treating others with respect and civility, being perceived to have too great a concern for the personal affairs of others, particularly those details that could cause one public embarrassment, purveyors of such matters might garner a reputation as a "gossiper." Such a reputation potentially casts one as indiscreet, having poor **manners** and "low" concerns, untrustworthy, nosy, or "holier than thou." In potentially soiling the reputations of others through gossip, purveyors risk their own.

Those who occupy the role of audience member are also moral actors. The words typically used to describe this role—audience, listener, or receiver—disguise the agency typically accorded by these terms to this position. In fact, the audience of gossip may exercise a great deal of power in this communicative act. Audience members are not, and are not expected to be, merely listeners. Purveyors usually include them in the conversation because they are trusted. Purveyors are also performing for their audience. Audience members have a range of possible functions in their social role: as confidantes or as betrayers of confidences; as co-constructors of reality, as future purveyors, or as terminators of gossip; and, finally, as adjudicators of purveyors and absent subjects alike. Once included in the conversation, members of the audience are implicated and obliged to assume a stance, rather than to merely listen. The choices audience members make have consequences for their relationships with purveyors and possibly absent subjects, consequences that bear on their own moral standing.

Sociologists have also identified a number of social functions of gossip including, among others, informal social control, social solidarity, information management, and reinforcing the normative order. The most commonly discussed social function of gossip in sociological research is informal social control, a means of responding to deviant behavior and thus maintaining social stability. Because the content of gossip usually conveys something unsavory or unfortunate about the

absent subject, gossiping may lead to the stigmatization and marginalization of absent others by those included in the gossip. All individuals privy to gossip collaboratively negotiate through their interaction what kinds of deviant affairs might merit such talk and, conversely, what values and norms they venerate. Gossiping about absent others, as well as the threat of being gossiped about, is a powerful form of informal social control that functions to regulate human behavior according to the norms of the group. As a response to deviance, the social control function of gossip may also lead to further social functions. The prevalence of gossip in a social group may have deleterious effects, creating suspicion, mistrust, and discord, or “productive” effects such as reinforcing shared group norms and enhancing social solidarity among members.

That gossip has historically connoted the pejorative is evinced by an emerging body of work regarding “good” gossip, just as the term “male nurse” reveals the assumptive gendering of “nurse.” It is not known if gossip’s character is maligned because it concerns the private affairs of others, because of its usual damaging content and consequences for individuals, because of its fictive nature, or perhaps because it is perceived to be predominantly an activity of women. What is recognized is that gossip is a powerful feature of everyday social life and has arrived as a burgeoning subject of social inquiry.

See also: **Privacy, definition of; Secrecy**

Suggested Reading: Bergmann, Jorg R. *Discreet Indiscretions: The Social Organization of Gossip*. New York: Aldine de Gruyter, 1993; Goffman, Erving. *The Presentation of Self in Everyday Life*. Garden City, NJ: Doubleday Anchor, 1959; Goodman, Robert F., and Aaron Ben-Ze’ev. *Good Gossip*. Lawrence, KS: University Press of Kansas, 1994; Robinson, Christine M. *Social Control in a Lesbian Community*. Latham, MD: University Press of America, 2006; Spacks, Patricia Meyer. *Gossip*. New York: Alfred A. Knopf, 1985.

Christine M. Robinson

***Griswold v. Connecticut*, 381 U.S. 479 (1965)**

In *Griswold v. Connecticut*, the Supreme Court struck down as unconstitutional a Connecticut law criminalizing the use of contraceptives as inconsistent with a constitutional right of privacy. In so doing, the Court recognized the existence of such a right, navigated an uneasy tension in its prior cases, and laid what became the foundations for constitutional rights to decisional privacy (including **abortion**) and informational privacy.

Although the U.S. Constitution protects many rights expressly, it does not contain any mention of the word “privacy.” Nevertheless, prior to *Griswold*, the Supreme Court had recognized in a number of cases that the Constitution protected privacy interests of one form or another. Prior to the New Deal era, the Supreme Court had protected the private sphere from government regulation through a number of related doctrines. Thus, in criminal procedure law, it had held in cases such as *Boyd v. United States*, 116 U.S. 616 (1886) that the Fourth and Fifth Amendments to the Constitution created a form of privacy right protecting a person’s private papers from government scrutiny. In *Lochner v. New York*, 198 U.S. 45 (1905) and related cases, it held that the Due Process Clause of the Fourteenth Amendment guaranteed a liberty of contract and state neutrality in economic affairs that



prevented many kinds of state regulation touching private affairs, including workplace safety rules and minimum wage laws. And in *Meyer v. Nebraska*, 262 U.S. 390 (1923) and *Pierce v. Society of Sisters*, 268 U.S. 510 (1925), the Court declared that the Fourteenth Amendment's Due Process Clause denied the states the power to interfere with parents' rights to send their children to private schools and to educate them in languages other than English.

Many of these rules were inconsistent with the needs of the modern regulatory state, and with the notable exception of the *Meyer* and *Pierce* strand of the doctrine, over time they were gradually whittled away by the Supreme Court. Particularly after the Court was comprised of a majority of Justices appointed by President Franklin D. Roosevelt, the Court's constitutional law jurisprudence shifted to allow significantly greater government regulation of economic activity. Interpretations of the Due Process Clause like *Lochner* that appeared to be unmoored from the text of the Constitution became suspect, and the Court increasingly deferred to modern welfare legislation. At the same time, however, as it noted in the famous case of *United States v. Carolene Products*, 304 U.S. 144 (1938), the Court began to show a greater willingness to protect First Amendment and other non-economic civil liberties from government interference. These somewhat divergent impulses—judicial restraint and modern civil libertarianism—would soon come into conflict in contexts relevant to privacy. For example, in *Skinner v. Oklahoma*, 316 U.S. 535 (1942), Justice **William O. Douglas**, writing for the Court, invalidated under equal protection grounds, Oklahoma's law providing for mandatory sterilization of habitual criminals because it violated a fundamental right to procreate. In *Prince v. Massachusetts*, 321 U.S. 158 (1944), the Court held in the context of children engaged in selling religious materials that the modern state's power to regulate on behalf of child welfare trumped both First Amendment rights and parental rights under *Meyer* and *Pierce*. *Griswold v. Connecticut* would again place these two guiding principles of post-New Deal constitutional jurisprudence into direct conflict in the context of privacy.

Griswold was the culmination of a series of challenges by **birth control** advocates to a Connecticut law outlawing contraception. That law, passed in 1879, made it a crime for any person to use or aid any person in using "any drug, medicinal article, or instrument for the purpose of preventing contraception" (*Conn. Gen. Stat.* §§53–32, 54–196). The statute had never been enforced, though Abraham Ullman, Connecticut's long-serving attorney general, had threatened to prosecute any violators. Birth control advocates had twice before attempted to challenge the Connecticut statute without first violating it, but in *Tileston v. Ullman*, 318 U.S. 44 (1943) and *Poe v. Ullman*, 367 U.S. 497 (1961), the Supreme Court rejected these challenges on procedural grounds without reaching the issue of the statute's constitutionality.

In 1961, the Planned Parenthood League of Connecticut and its executive director, Estelle Griswold, tried to challenge the statute again by opening a birth control clinic in New Haven. Their goal was for Griswold to be arrested and force a decision on the constitutionality of the statute. This time they succeeded. Ten days after the clinic opened, Griswold was arrested along with Charles Lee Buxton, a Yale Medical School professor and medical director of the clinic. They were found guilty of violating the statute by giving advice to married couples and fined \$100,

over their objections that the statute violated the Constitution's Fourteenth Amendment guarantee of due process of law. The Connecticut state appellate and supreme courts affirmed Griswold and Buxton's convictions.

The United States Supreme Court heard Griswold and Buxton's appeal and reversed it by a vote of 7-2. The justices recognized that the Constitution includes an unenumerated right of privacy, although they disagreed somewhat about the source and content of that right.

Writing for a majority of the Court, Justice William O. Douglas concluded that state regulation of the use of contraceptives by married couples violated a constitutional right to privacy. However, Douglas had a problem. As a member of the group of justices who had opposed the Court's *Lochner* cases, Douglas was reluctant to merely hold that a broad right of privacy was inherent in basic notions of due process of law. Indeed, to make such an argument would be to have engaged in the same sort of constitutional interpretation that he and others had been so critical of during the New Deal period, in which they had charged that the earlier cases had essentially made up rights and incorporated them into the Constitution by fiat. His solution to the problem was to locate a right of privacy across a broad spectrum of the protections in the Bill of Rights. Thus, he argued that the First Amendment had been interpreted to include not just the rights protected in *Pierce* and *Meyer* (recasting those cases in the process), but also a right protecting against government intrusion into associations of individuals for a common purpose. Furthermore, other provisions of the Bill of Rights had "penumbras, formed by emanations from those guarantees that help give them life and substance" (p. 484.) Thus, the Third Amendment prohibits the quartering of soldiers in private **homes**, the Fourth Amendment gives people security and privacy in their private homes and papers, the Fifth Amendment's self-incrimination clause creates a "**zone of privacy**" that the government could not breach, and the Ninth Amendment recognizes that rights not enumerated by the Constitution might nevertheless be retained by the people. These protections, taken together, he argued, created a broader zone of privacy that while not specifically articulated by any one of these provisions in the Constitution's text, was nevertheless protected by all of them acting together. Because marriage was an association of ancient origins and tremendous social importance, its privacy could not be violated by the state's intrusion into the marital bedroom for signs of contraceptive use. Although Justice Douglas's theory garnered the votes of a majority of five of the nine justices, and thus gained the status of binding law, a number of justices articulated alternative theories justifying the outcome. Justice Arthur Goldberg, along with Chief Justice Earl Warren and Justice William Brennan, joined Douglas's opinion, but they also articulated a broader theory of constitutional privacy grounded in the Ninth Amendment and "so rooted in the traditions and conscience of our people as to be ranked as fundamental." (p. 487). Justice John Harlan, although he rejected Douglas's penumbral theory, agreed with the outcome because the Connecticut law violated basic values "implicit in the concept of ordered liberty" (p. 500) that were protected by the Due Process Clause of the Fourteenth Amendment. Justice Byron White similarly agreed with the outcome, but also rejected Douglas's theory of constitutional privacy. Instead, he argued, the case ought to be resolved by basic principles of due process: the Connecticut law deprived married people of the important liberty of contraceptive use and **family**



planning, and did not directly advance the regulatory interests put forward by the state. Justices Potter Stewart and Hugo Black dissented, noting that while they thought the Connecticut statute was a terrible one (Stewart famously called it “an uncommonly silly law” (p. 527)), the law did not violate any provision of the Constitution and ought to be upheld by the courts. Black and Stewart were both concerned by the fact that the Constitutional text contained no mention of any right of privacy, and that for judges to essentially invent such a right would be for them to substitute their own views of morality for that of legislatures. Black, in particular, was troubled by the legacy of *Lochner*, and by the Court’s reliance on *Meyer* and *Pierce*, which he acknowledged came from that discredited constitutional tradition. More generally, Black feared for the legitimacy of an unelected judiciary that could so easily substitute its own “personal preferences” (p. 526) regarding the correctness of laws. In Black’s view, such an approach to the judicial role would amount to a shocking departure from the constitutional separation of the judiciary from politics and the political branches of government at all levels.

The Court’s opinions in *Griswold* have been read as protecting two distinct varieties of a constitutional right of privacy. On the one hand, *Griswold* can be read as protecting “information privacy”—a right to keep information secret from the government. Two groups of Supreme Court cases have developed this theme further. First, there are two cases that can be read as explicitly recognizing a constitutional right of informational privacy. Thus, in *Whalen v. Roe*, 429 U.S. 589 (1977), the Court intimated that the *Griswold* right to privacy might include an individual right against government disclosure of certain kinds of sensitive information, such as medical information. This suggestion was confirmed in *Nixon v. Administrator of General Services*, 433 U.S. 425 (1977), in which former President Nixon challenged a federal statute nationalizing his presidential papers as violating his right to privacy with respect to personal papers contained in the archive. The Supreme Court agreed with Nixon that he had a *Whalen*-type privacy interest in, for example, presidential documents relating to his family life or personal legal advice, but held that the act’s provisions allowing for archival screening of his papers to separate out the private ones from the public ones sufficiently protected his informational privacy rights, given both the government’s interest in the public papers and the tiny fraction of the total body of papers that were truly private. Further articulation of the constitutional right to informational privacy has been left to lower courts for further development, and although a number of such courts have protected constitutional informational privacy rights, the jurisprudence is neither particularly robust nor consistent.

A second area where information privacy rights have been given constitutional protection is in the Court’s invalidation of notification provisions in state abortion laws. Thus, in cases such as *Hodgson v. Minnesota*, 497 U.S. 417 (1990) and *Planned Parenthood v. Casey*, 505 U.S. 833 (1992), the Court invalidated notification provisions in state abortion laws that would have required women seeking an abortion to first notify their husbands or parents. To this extent, these cases can be read as protecting a constitutional interest in nondisclosure consonant with the *Griswold* conception of informational privacy. Nevertheless, it is fair to say that although the informational reading of *Griswold* is probably a better reading of the

right recognized in Justice Douglas's majority opinion, it has remained largely undeveloped by subsequent cases.

By contrast, an alternative reading of *Griswold* as protecting "decisional privacy"—the right to make reproductive and other intimate decisions without government interference—has received significantly more attention. In *Eisenstadt v. Baird*, 405 U.S. 438 (1972), the Court addressed the contraceptive rights of unmarried persons, and confronted the problem that Justice Douglas's rationale for the **confidentiality** of marital relationships was not as strong outside the marital context. Justice Brennan held for the Court that "if the right of privacy means anything, it is the right of the *individual*, married or single, to be free from unwarranted government intrusion into matters so fundamental as the decision whether to bear or beget a child." In so doing, the Court transformed the constitutional right to privacy from one rooted in the confidentiality of relationships from government scrutiny to an individual liberty interest to make intimate decisions free from government interference. This decisional understanding of the constitutional right to privacy formed the basis for *Roe v. Wade*, 410 U.S. 113 (1973). In *Roe*, the Court found the right to privacy to include a right of abortion and located it in the Due Process Clause of the Fourteenth Amendment, thereby abandoning Justice Douglas's penumbral conception of privacy. Subsequent cases, most notably *Planned Parenthood v. Casey* (1992), have confirmed the basic validity of the Court's ruling that abortion rights are constitutionally protected, although numerous challenges have addressed various aspects of this right, prompted in large part by the enormous importance of the abortion issue to the national political landscape. The right to decisional privacy in fundamental decisions has been extended to other areas of the law with mixed results for claimants, with subsequent cases involving the right to terminate life-sustaining medical care (*Cruzan v. Director, Missouri Dep't of Health*, 497 U.S. 261 (1990)), physician-assisted suicide (*Washington et al. v. Glucksberg et al.*, 521 U.S. 702 (1997)), parental rights to direct their children's upbringing (*Troxel v. Granville*, 530 U.S. 57 (2000)), and the right to private homosexual conduct (*Bowers v. Hardwick*, 478 U.S. 186 (1986); *Lawrence v. Texas*, 539 U.S. 558 (2003)).

Griswold v. Connecticut was arguably the most significant of a number of post-*Lochner* Supreme Court decisions in which the Court was called upon to evaluate the constitutionality of regulations of activities and decisions central to personal identity and self-determination. It thus raised one of the central questions to any society in which judges interpret a written Constitution: how to interpret a written text in light of changed times and changed views of morality. As a general rule, liberals have tended to applaud the Court's willingness in *Griswold* to look beyond a narrow reading of the text of the Constitution to find that the Due Process Clause protects a basic and broad commitment to liberty and individual autonomy. In this regard, they have echoed the arguments of justices Douglas and Goldberg. Conservatives, on the other hand, have tended to argue that *Griswold*'s right to privacy is unmoored by any limiting principle, and that unelected judges interpreting the right to privacy improperly substitute their own elitist morality for the morality of the citizenry acting democratically through its elected representatives. In this regard, conservatives accuse liberals of engaging in the same methodology of constitutional interpretation that was discredited at the end of the *Lochner* era, in an echo of the arguments made by Justices Black and Stewart in dissent.



To this extent, the actual rationale of the decision in *Griswold* has been somewhat obscured by *Roe v. Wade*, as abortion politics have become one of the most important divisions in American politics. This is unfortunate, because the issues raised by *Griswold* are important enough to warrant more separate attention than they have been accorded, both at the level of national politics and academic commentary.

See also: **Constitutional protections; Gender; Women and privacy**

Suggested Reading : Allen, Anita. *Uneasy Access: Privacy for Women in a Free Society*. Totowa, NJ: Rowman and Littlefield, 1988; Allen, Anita. *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability*. Lanham, MD: Rowman and Littlefield, 2003; Allen, Anita, and Erin Mack. "How Privacy Got Its Gender," *Northern Illinois University Law Review* 10 (1990): 441–454; Allen, Anita, and Erin Mack. "Taking Liberties: Privacy, Private Choice and Social Contract Theory," *University of Cincinnati Law Review*, 56 (1987): 461–491; Garrow, David J. *Liberty and Sexuality: The Right to Privacy and the Making of Roe v. Wade*. Berkeley: University of California Press, 1998; Richards, Neil M. "The Information Privacy Law Project," *Georgetown Law Journal* 94 (2006): 1087–1140; Kersch, Ken I. *Constructing Civil Liberties: Discontinuities in the Development of American Constitutional Law*. Cambridge: Cambridge University Press, 2004; White, G. Edward. *The American Judicial Tradition*. Oxford: Oxford University Press, 1988.

Neil M. Richards

H



Harris v. United States, 331 U.S. 145 (1947)

In this case, which involved a search incident to an arrest, the Supreme Court affirmed the admissibility of evidence of one crime that was found by officers during a proper, but warrantless, search for evidence of another unrelated crime. The basis for the Court's ruling was subsequently expanded by the courts as the test required for the **plain view doctrine**.

George Harris was a suspect in the forgery of a \$25,000 check drawn on an Oklahoma oil company that was to be cashed in a New York bank. Two warrants were issued for his arrest, and subsequently five **Federal Bureau of Investigation (FBI)** agents arrested him in the living room of his Oklahoma City apartment. After the arrest, agents spent five hours searching the four-room apartment for evidence of the forgery.

Just before completing the search, one of the agents found a sealed envelope in a bedroom dresser marked "George Harris, personal papers." Inside that envelope was a second sealed envelope in which the officer found 8 draft cards and 11 draft registration certificates. Harris was subsequently convicted of unlawful possession, concealment, and alteration of the Selective Service materials.

Harris attempted, unsuccessfully, to have the evidence found in his dresser suppressed as the result of what his attorney argued was an unreasonable and unconstitutional search. The Court rejected Harris's arguments that officers could not search his apartment, reasoning that searches incident to arrests were authorized to include "the premises under his immediate control." In this case (under now-antiquated Fourth Amendment jurisprudence), the Court held, that included the entire apartment. Opening and then searching the sealed envelopes were authorized because officers were looking for canceled checks and related pieces of paper that easily could have been hidden in the envelopes. The argument that the documents found had nothing to do with the crime then being investigated also failed to convince the Court's majority. "In keeping the draft cards in his custody [Harris] was guilty of a serious and continuing offense against the laws of the United States. A crime was thus being committed in the very presence of the agents conducting the search. Nothing in the decisions of this Court gives support to the suggestion that under such



circumstances the law-enforcement officials must impotently stand aside and refrain from seizing such contraband material.”

The ruling essentially followed earlier findings that generally related to discoveries by police in fields or private yards. In those instances, the courts relied on the premise that citizens had no expectation of privacy for activities conducted in open yards or fields. The *Harris* Court brought concepts from the earlier rulings indoors.

In *Harris*, the FBI agents were properly in the defendant’s **home**, the initial search was deemed valid, and given the nature of the search, the draft cards were discovered in plain view by an agent while he was searching for other papers. Thus, the draft cards were subject to seizure without a warrant. The resulting plain view doctrine thus became an exception to the Fourth Amendment warrant requirement that permits law enforcement officers to seize clearly incriminating evidence or contraband when it is discovered in a place where the officers have a legal right to be.

See also: California v. Ciraolo, 476 U.S. 207 (1986); *Chimel v. California*, 395 U.S. 752 (1969); *Payton v. New York*, 445 U.S. 573 (1980); *United States v. Dunn*, 480 U.S. 294 (1987); *Warden v. Hayden*, 387 U.S. 294 (1967); *Weeks v. United States*, 232 U.S. 383 (1914)

Suggested Reading: Barte, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black’s Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

David J. Brown

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Congress passed Public Law 104-191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), to accomplish multiple purposes. Title II, Subtitle F, Part C covers health care administrative simplification. A major purpose of this part was to encourage development of a modern health information system by establishing standards and requirements for the electronic transmission of certain health information.

The law required the secretary of Health and Human Services to use rulemaking to implement four main objectives. The first objective was the establishment of standards for financial and administrative transactions, as well as the data elements for those transactions, to enable health information to be exchanged electronically. The goals of this objective were to improve the health care system and reduce administrative costs. The secretary published initial rules for eight “standard transactions” (45 C.F.R. Parts 160 and 162) in 2000, with a compliance date in 2002.

A second objective was the establishment of a standard unique health identifier for each individual, employer, health plan, and health care provider. The secretary adopted employer and provider identifier rules in 2002 and 2004. The national health plan identifier was delayed administratively. Controversy about the individual identifier led to later congressional prohibitions against administrative action to adopt an identifier.

A third objective was the establishment of standards for the security of electronic health information. The secretary published final standards in 2003, with a compliance date in 2005. This final rule specifies a series of administrative, technical, and physical security procedures (45 C.F.R. Part 164) for covered entities to use to ensure the **confidentiality** of electronic, protected health information.

The fourth objective was the establishment of national standards to protect the privacy of personal health information. HIPAA directed the secretary to establish a health privacy rule if the Congress was unable to enact a health privacy law within three years of the date of enactment. Congress failed to act by the deadline, and in 2000, the secretary adopted a privacy rule (45 C.F.R. Part 164) with a compliance date in 2003.

The law assigns the secretary the task of enforcing HIPAA standards through administrative sanctions. The law includes criminal penalties for wrongful disclosure of individually identifiable health information. The law did not provide for private rights of action for aggrieved individuals. The Office of Civil Rights at the Health and Human Services Department enforces the privacy rule.

The HIPAA standards generally do not preempt state privacy laws that provide more stringent privacy protections. Thus, the federally established standards provide a floor of privacy and security protections that states can exceed. The privacy and security rules apply to covered entities, which are health care providers that conduct standard transactions in electronic form, health plans, and health-care clearinghouses.

See also: **Disclosures; Health privacy; Personally identifiable information**

Suggested Reading: Institute of Medicine. *Health Data in the Information Age*. Washington, DC: National Academies Press, 1994. <http://www.nap.edu/books/0309049954/html/>. Online, August 2005; National Conference of Commissioners on Uniform State Laws. *Uniform Health-Care Information Act 1985*. <http://www.law.upenn.edu/bll/ulc/fnact99/1980s/uhcia85.htm>. Online, August 2005; National Research Council. Computer Science and Telecommunications Board. *For the Record: Protecting Electronic Health Information*. Washington, DC: National Academies Press, 1997. <http://books.nap.edu/catalog/5595.html>. Online, August 2005; Office of Technology Assessment. *Protecting Privacy in Computerized Medical Information*. Washington, DC: U.S. Government Printing Office, 1993. http://www.wws.princeton.edu/%7Eota/disk1/1993/9342_n.html. Online, August 2005; U.S. Department of Health and Human Services. Office of Civil Rights. <http://www.hhs.gov/ocr/hipaa/>. Online, March 2006; U.S. Department of Health and Human Services. Privacy Protection Study Commission. "Record Keeping in the Medical-Care Relationship." In *Personal Privacy in an Information Society*, pp. 277–317. Washington, DC: U.S. Government Printing Office, 1977. <http://aspe.hhs.gov/datacncl/1977privacy/c7.htm>. Online, August 2005.

Robert Gellman



Health privacy

The privacy of health records has been a concern of physicians and patients since the dawn of medicine. Developments in health care during the twentieth century made health records more complete and more valuable to a wider range of health care and other institutions. These developments have increased tensions between privacy and other societal goals, including providing better quality care, controlling costs, and preventing fraud and abuse. State laws on health privacy, while often numerous, are often disjointed and variable, and may fail to reflect current health care activities. Judicial decisions often recognize the need to balance privacy against other interests. A federal health privacy rule adopted under the authority of the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** established a national floor for privacy protection, forced the health care industry to pay more attention to privacy, and prompted a review of some state laws.

Confidentiality has historically been recognized as an important element of the physician-patient relationship. In the fourth century B.C., the Hippocratic Oath called on physicians to treat as “holy secret” patient information that “should not be published abroad.” Notably, the oath does not prohibit all disclosures. Even at the beginning, health professionals recognized that the obligation to keep patient information private was not absolute.

Later ethical codes for physicians reflected both the importance of confidentiality and the possibility that **disclosure** might be necessary. For example, the first code of ethics of the American Medical Association, adopted in 1847, called on physicians not to disclose information except when “imperatively required to do so.”

Recognition of the importance of health privacy by the law dates back to 1828, when New York state established the first physician-patient **privilege** to protect confidential communications between physician and patient. This privilege is a creature of statute and not of common law. The privilege is testimonial, so it applies only in court or court-related proceedings. While the privilege has spread in some form to all states, it is often limited in scope, unavailable, or simply irrelevant to administrative disclosures that have become a routine part of health care. In some states, for example, the privilege only applies to confidential communications between patient and psychiatrist.

Tensions between privacy and other concerns grew stronger as the twentieth century progressed as a result of developments in the health care system. The growth of these tensions was not always reflected in the rhetoric about the traditional importance of privacy in the health care relationship. Privacy advocates and politicians sometimes failed to recognize the enormous increases in the authorized use and disclosure of patient information for activities far removed from treatment and payment. Neither the public nor health professionals appeared to be fully aware of either the expanded sharing of patient information or the routine maintenance of patient information outside the treatment setting.

Early in the twentieth century, recorded patient health information was rare. Over time, health records maintained by physicians and hospitals grew in size and number. Health records now contain massive amounts of treatment information, as well as information not related to treatment, including information about a patient’s

relatives, finances, education, and employment. The traditional maintenance of tissue samples for research or reference has raised new privacy concerns because of the ability to retrieve **genetic information**.

Third-party payment for health treatment, including payments from both private insurance and government plans, increased demands for the sharing of patient information. Bills for treatment, along with supporting documentation, routinely go to third-party payers. Employer-sponsored health insurance also increased the likelihood that records of workers and their families would be shared with employers. Further, distinctions between treatment activities and payment activities began to blur as pre-approval of treatment by insurers became a common prerequisite for payment.

Pressures to contain health care costs and to provide higher-quality care expanded the routine sharing of individually identifiable health records with new institutions. Disease management programs, often sponsored by employers or insurers, often resulted in more sharing of patient records.

Health fraud investigators, prosecutors, and both public and private sector auditors routinely obtain access to patient records to prevent fraud and abuse. Accreditation of health care facilities and professional licensing activities also have increased demand for the disclosure of health records.

Many public health functions rely in whole or in part on access to identifiable patient records. These functions include vital statistics reporting; communicable disease, birth defects, and occupational injury reporting; public health **surveillance**, investigations, and interventions; adverse event reporting for regulated drugs and devices; occupational disease and workplace surveillance activities; and child abuse, neglect, and domestic violence reporting.

Government activities such as health oversight, health planning functions, civil rights law enforcement; and beneficiary eligibility determinations for public programs often require patient information. Research activities, including systematic investigations to develop or contribute to generalizable knowledge, often rely on access to patient records. The use of institutional review boards to screen research protocols for ethical and privacy concerns became common by the end of the twentieth century. Federal rules governing research involving human subjects apply to federally funded research activities. These rules establish standards for institutional review board membership and activities (Common Rule 45 C.F.R. Part 46).

Law enforcement agencies use health records for functions including routine criminal investigations, health care fraud investigation, gunshot wound reporting, and emergency response. The Secret Service requests patient information in connection with protective activities for the president and other officials. National security agencies also seek health information.

Health information is also of interest to marketers, who routinely traffic in information reflecting the health conditions of individuals. Marketers usually obtain health information from sources outside the treatment process. Private investigators seek health records for use by insurance companies and others. Evidence suggests that the demand has been sufficient to support surreptitious trafficking in patient information.

In 1977, the U.S. Supreme Court considered health privacy issues arising from the use of a state-operated database. In *Whalen v. Roe*, 429 U.S. 589 (1977), the



Court reviewed a state statute that required the reporting of prescriptions for dangerous drugs to the health department. The Court found that the law was a reasonable exercise of the state's broad police powers and that the reporting requirement had not violated any constitutional right of information privacy. However, the Court did acknowledge the threat to privacy implicit in the accumulation of personal information in computerized data banks or other government files.

In *Jaffe v. Redmond*, 518 U.S. 1 (1996), the Court adopted a psychotherapist privilege as a newly recognized privilege in federal court. The privilege applies to confidential communications made to psychiatrists, psychologists, and licensed social workers in the course of psychotherapy. In *United States v. Westinghouse Electric Corp.*, 638 F.2d 570 (3d Cir. 1980), a federal appeals court decided a case involving a federal agency subpoena to an employer for its employees' health records for use in an investigation of a workplace health hazard. The decision listed factors to be considered in deciding whether an intrusion into an individual's privacy is justified. The seven factors were (1) the type of record; (2) the information it did or might contain; (3) the potential for harm in any subsequent nonconsensual disclosure; (4) the injury from disclosure to the relationship in which the record was generated; (5) the adequacy of safeguards to prevent unauthorized disclosure; (6) the degree of need for access; and (7) whether there was an express statutory mandate, articulated public policy, or other recognizable public interest favoring access. The importance of this decision is the identification of specific elements to be considered in weighing a privacy interest.

In *Tarasoff v. Regents of the University of California*, 17 Cal. 3d 424 (1976), the California Supreme Court held a psychiatrist could be liable to a third party for failing to warn about a dangerous patient. State law is not uniform on the duty to warn.

Until 2003, when the federal government required implementation of health privacy rules under the authority of the Health Insurance Portability and Accountability Act (HIPAA), legislative protections for the privacy of health records were largely left to the states. The quality of state health privacy legislation has been highly variable. Older approaches found in many state health privacy laws tend to provide that health records are confidential, but offer little practical guidance about what that means in an era when numerous institutions request or demand access to records. Comprehensive state privacy statutes that reflect institutional and technological developments in the health care system have been relatively rare. Only a few states adopted a model state law proposed by the National Conference of Commissioners on Uniform State Laws in the mid-1980s.

Aside from broad statutes on health privacy, states tend to have dozens of separate and uncoordinated laws addressing different aspects of the collection, maintenance, use, or disclosure of patient information. Laws may cover records by type (e.g., HIV/AIDS, mental health, genetics), by institution (e.g., hospitals, nursing homes, mental health facilities, insurers), by health care provider (e.g., physicians, pharmacists, optometrists), or otherwise (e.g., physician-patient privilege). Privacy standards may vary considerably from law to law in the same state. In some states, a single health record could be subject to privacy requirements under multiple state and federal laws. In particular, many states have special laws addressing privacy and other issues related to HIV/AIDS and to genetic information.

Prior to HIPAA, federal health privacy laws were limited in scope. The **Privacy Act of 1974** (5 U.S.C. §552a) established comprehensive **fair information practices** for most personally identifiable records maintained by federal agencies, including health records. Specific laws and a common set of regulations cover federally funded alcohol and drug abuse treatment records (see, for example, 42 U.S.C. §290dd-2 and 42 C.F.R. Part 2).

The biggest development in health privacy legislation was the enactment of HIPAA. The resulting health privacy rule issued by the U.S. Department of Health and Human Services forced the health care industry to pay active attention to privacy. The rule establishes a minimum national floor of privacy and security protections that reflect fair information practices for access, amendment, openness, accountability, and use and disclosure limitation. Entities covered directly by the rule are health care providers who bill for services using standard (electronic) transactions, health plans, and health care clearinghouses. The rule covers protected health information, which includes individually identifiable health information in the possession of covered entities.

Covered entities must require their contractors who perform a function involving the use or disclosure of protected health information to meet the rule's standards through contracts. However, the HIPAA privacy rule does not apply to secondary users of health records, such as researchers, law enforcement agencies, auditors, and others. The net result is that many users of health information outside immediate health treatment and payment circles are not subject to the HIPAA privacy rule or any other privacy law.

HIPAA does not preempt most state laws that provide more stringent privacy protections. One consequence is that older state privacy laws that were sometimes ignored have become the subject of new attention and compliance. Another consequence is that state legislatures are reexamining their health information laws and revising them to reflect the terminology and policy found in the HIPAA privacy rule. Other federal privacy rules, such as the alcohol and drug abuse confidentiality rules, also remain in effect. Health records maintained by schools subject to the **Family Educational Rights and Privacy Act (FERPA)** (20 U.S.C. §1232g) are not subject to the HIPAA rule.

The HIPAA rule established substantive and procedural restrictions on the use and disclosure of identifiable patient records. The rule allows for the use and disclosure of records for numerous broadly defined categories of activities, including treatment, payment, health care operations, health oversight, public health, judicial activities, law enforcement, research, and others. The rule also allows all uses and disclosures required by law. For most uses and disclosures, patient consent is not required. For the most part, HIPAA allows nearly all governmental and administrative uses and disclosures that became routine during the twentieth century. A minimum necessary rule applies to some uses and disclosures.

Critics have objected to the broad scope of permitted uses and disclosures allowed by the rule, to the weakness of procedural prerequisites for some disclosures, and to the lack of a general requirement for patient consent. The rule also generated objections from communities of record users, such as researchers and public health officials, who claimed that the new rule made their ability to obtain



identifiable records more difficult and created disincentives to disclosures by record keepers.

The HIPAA privacy rule also established a broad range of administrative requirements for covered entities. These requirements include the preparation of a notice of privacy practices, designation of a privacy official, training for workforce members, safeguards for records, maintenance of disclosure history, and formal policies and procedures. Covered entities must also grant patients access to their records and limited rights to seek amendment of records. A separate HIPAA rule establishes detailed standards for the security of electronic protected health information.

Continuing challenges include fully implementing the federal privacy rule, resolving the difficulties that arise when applying different privacy regulations in different states or to different elements of a health record, and adapting privacy policies to an increasingly interstate, interconnected, and digital health information system. In particular, privacy will present new problems in ongoing planning for more widespread use of electronic health records and for a national information network. Existing conflicts between privacy interests and other health objectives are likely to increase, and new conflicts will arise with new implementations of technology. In addition, concerns about the discriminatory use of health information, particularly genetic information, will also be significant issues in the future.

See also: **Personally identifiable information; Public records; Workplace privacy**

Suggested Reading: Institute of Medicine. *Health Data in the Information Age*. Washington, DC: National Academies Press, 1994. <http://www.nap.edu/books/0309049954/html/>. Online, August 2005; National Conference of Commissioners on Uniform State Laws. *Uniform Health-Care Information Act* (1985). <http://www.law.upenn.edu/bll/ulc/fnact99/1980s/uhcia85.htm>. Online, August 2005; National Research Council. Computer Science and Telecommunications Board. *For the Record: Protecting Electronic Health Information*. Washington, DC: National Academies Press, 1997. <http://books.nap.edu/catalog/5595.html>. Online, August 2005; Office of Technology Assessment. *Protecting Privacy in Computerized Medical Information*. Washington, DC: U.S. Government Printing Office, 1993. http://www.wws.princeton.edu/%7Eota/disk1/1993/9342_n.html. Online, August 2005; U.S. Department of Health and Human Services. Privacy Protection Study Commission. "Record Keeping in the Medical-Care Relationship." In *Personal Privacy in an Information Society*. Washington, DC: U.S. Government Printing Office, 1977, pp. 277–317. <http://aspe.hhs.gov/datacncl/1977privacy/c7.htm>. Online, August 2005.

Robert Gellman

Home

Celebration of the home as the place where we realize ourselves as loving, responsible, and satisfied human beings has been a definitive theme in American culture since the founding of the Republic. However, the currently prevailing conception of the home, that is, as a stand-alone private dwelling owned and occupied by a nuclear family, did not assume its central position in American consciousness

until the decades immediately following the Civil War. During this period, urbanization, industrialization, and technological progress converged to fuel the popular conviction that every family ought to possess, or at least strive to possess, a private refuge from the complex pressures of the modern world.

This widespread fixation on the home, now known as the cult of domesticity, also developed in reaction to the burgeoning women's movement, which, in the eyes of its critics, threatened to erase the natural boundaries between public and private life. Tracing the right to privacy back to its roots in the nineteenth century accordingly reveals its anti-feminist heritage. Moreover, sketching the way ideas about privacy evolved over time shows that the area usually conceived as the space in need of protection has not been inhabited by separate individuals, but by a traditional family. Thus, historically, the right to privacy has been deeply entwined with the popular idealization of the conventional family home.

No legislation that was expressly designed to protect the right to privacy passed until after the turn of nineteenth century. However, courts recognized a man's right to suppress public disclosure of his domestic affairs in various rulings on household violence. In *State v. Rhodes*, 61 N.C. 453 (1868), Judge Edwin Godwin Reade held that domestic violence, at least when it did not result in severe or lasting injury, should be ignored by the law because the publicity attending prosecution would undermine the authority that husbands are naturally expected to exert over their wives. In Reade's view, whatever ills might issue from wife-whipping and other types of physical chastisement, paled in comparison with "the evils which would result from raising the curtain, and exposing to public curiosity and criticism, the nursery and the bed chamber."

Similar concerns about shielding the home from public scrutiny animated **Louis Brandeis** and Samuel Warren's famous essay, "The Right to Privacy," which was published in the *Harvard Law Review* in 1890. Citing recent inventions such as instantaneous photography, as well as the overly intrusive practices of the newspaper industry, Brandeis and Warren insisted that new protections had to be devised to safeguard the "sacred precincts of domestic life." In using such phrases, the authors drew from the common understanding of the home as much more than a building or physical space. Thus they observed that it was insufficient merely to protect tangible property; instead, the intangible property associated with the home, such as a man's interactions with his family, personal conversations, and peace of mind, also deserved to be secured from exposure. After all, Brandeis and Warren wondered, how could the common-law adage that "every man's house is his castle" retain any meaning if a man could not guard his home against impertinent prying, just as he had always had the right to defend it against physical trespass?

The conservative views of privacy advocates like Brandeis and Warren drew sharp criticism from contemporary radicals such as Charlotte Perkins Gilman. In *Women and Economics* (1898), Gilman castigated the illogical assumptions made by those who celebrated the privacy of the home. These fantasies, Gilman observed, omitted the frequently resentful servants who witnessed the intimacies of the rich, and they also failed to acknowledge that the overwhelming majority of society lived in cramped common rooms in which family members could not escape from each other. From Gilman's perspective, the pleasant refuge that

appeared under the banner of “Home, Sweet Home” was no more than an illusion, especially for women. While the management of the household turned the home into a “museum” for women who had money enough to hire servants, the endless round of domestic chores reduced it to a “workshop” for those who did not. However, according to Gilman, what made the home most suffocating to women was that wives were entirely dependent on their husbands and thus prevented from exploring any significant aspect of the wider world. The home was, she acknowledged, the birthplace of every worthwhile activity, but it was transformed into a deadening prison for women because they were denied the freedom to engage in any meaningful way in the larger society.

Gilman’s critique of the conventional home foreshadowed the efforts of 1970s feminists to call attention to the darker aspects of domesticity. However, Brandeis and Warren’s conception of the home as an inherently soul-sustaining retreat more or less won the day in the twentieth century, thanks in large part to the advertising industry. Elevating popular preoccupation with domestic life to new heights, advertisements for appliances, furniture, and other must-have merchandise constantly reinforced the nineteenth-century vision of the home as the place where individuals find self-fulfillment. Indeed, if there was one message that middle-class Americans heard more than any other during the past one hundred years, it was that the greatest joys can be had within the properly furnished, smartly equipped, tastefully decorated, fully secured, and well-stocked private home.

Detailed advice on how to live out the American dream in the ideal home was not dispensed exclusively by private industry. The government played an active role, not only in convincing those who could to reject boarding houses and apartments in favor of single-family dwellings, but also in educating homeowners on how to position a house on a lot, decorate specific rooms, and landscape the property to maximize family privacy. For example, in *Better Homes for America*, a typical government pamphlet issued in 1922, President Calvin Coolidge declared, “There are two shrines at which mankind has always worshipped, must always worship: the altar which represents religion, and the hearthstone which represents the home.” In light of this age-old principle, it seemed to Coolidge that Americans had already spent plenty of effort on public works, and that it was time to turn the great energies of the country toward the construction and beautification of private homes, dwellings that were solid and permanent, but modest enough to be affordable to all.

Although Coolidge’s dream of a nation of homeowners has yet to be fully realized, the home-building industry, dominated by huge mail-order companies such as Aladdin, Sears Roebuck & Co., and Montgomery Ward sprang up to meet the rising demand for cheap, single-family houses during the first half of the twentieth century. Aladdin, for instance, offered every man his own ready-made “castle” for under \$500 in 1909, and Sears delivered approximately 100,000 mail-order houses all over the country between 1908 and 1940. In the aftermath of World War II, the government touched off another round of massive development by financing the building of millions of tract houses in suburban areas, setting the stage for suburban sprawl in more recent years. The promise embodied in this frenzy of home building was not simply that middle- and working-class Americans or, more specifically, the majority of white families would own their own homes, but that the bulk

of the population would have a chance to conform to the ideal of the ostensibly normal family, with a male breadwinner at its head and a stay-at-home mother to care for their children. This optimum arrangement represented much more than mere prosperity. In fact, it was a way of life that was worth enormous sacrifice, as exemplified by a widely circulated government poster issued in the 1940s featuring a white family with two obviously loving parents and three wholesome children seated at their kitchen table eating corn. “This is America!” the copy beneath the image reads, “where the family is a sacred institution, where children love, honor and respect their parents, where a man’s home is his castle. This is *your* America. Keep it Free!”

This idealized image of domesticity, which was reinforced by scores of television shows and commercials throughout the 1950s and 1960s, came under heavy fire from the women’s liberation movement of the 1970s. Railing against the popular vision of the home as the place where women naturally find fulfillment, feminists pointed out that living in a man’s castle, having no recourse against sexual coercion, no respite from housework and child care, limited access to education, and little chance to earn an independent income was not conducive to happiness. “The personal is political!” became a popular feminist refrain as increasing numbers of women argued that traditionally private matters such as rape and domestic violence needed to be exposed to the public scrutiny that privacy defenders had tried so hard to avoid. Along these lines, well-known feminists such as Betty Friedan and Gloria Steinem argued that sexual inequality stemmed not only from the active exclusion of women from the higher levels of business, academia, and government, but also from the dependency, boredom, and, in many cases, physical and emotional pain they suffered within the home.

In stark opposition to idealized conceptions of the domestic circle, many 1970s feminists derided the life of the typical housewife as a brainless existence built on sexual submission, vapid consumption, and deep-seated anxiety about meaningless routines. Women’s rights activists declared, first in consciousness-raising groups and then in public demonstrations, that sexual equality would not be achieved until women enjoyed parity on both sides of the **public/private dichotomy**, not only receiving equal pay for equal work, access to higher education, and unfettered opportunity in every profession, but also casting off primary responsibility for childrearing and other domestic cares.

The women’s liberation movement has frequently been blamed for the subsequent disappearance of the stereotypical housewife, that is, a mother who did not work outside the home. However, the deep recession of the mid- to late 1970s, which was characterized by an unprecedented combination of high unemployment and rising inflation, played a much larger role in destroying the ability of single-income families to achieve home ownership. During this period, in a trend that has continued ever since, millions of women moved into the paid workforce, not because feminists urged them to do so, but because most families could no longer expect to survive, let alone own their own homes, by relying on one income.

The notion of the home as a haven from the larger society may be unrealistic, but it has profoundly influenced legal approaches to the right to privacy over the last few decades. For example, in his frequently quoted dissent in *Poe v. Ullman*, 367 U.S. 497 (1961), Justice John Harlan Marshall maintained that the importance

of the home as the center of family life was so profound that the grounds for its protection flowed from a variety of constitutional rights. Drawing from *Poe* and similar cases in *Griswold v. Connecticut*, 381 U.S. 479 (1965), the Supreme Court held that choices made by married couples in respect to family planning are contained within a **zone of privacy** into which the government should not intrude. Echoing Brandeis and Warren's sentimental phrases about the "sanctity of the domestic circle," **William O. Douglas**, who wrote the majority opinion, asserted, "Marriage is a coming together for better or for worse, hopefully enduring, and intimate to the degree of being sacred." According to Douglas, the marriage bond deserves special protections because it transcends other, apparently more mundane concerns: "It is an association that promotes a way of life, not causes; a harmony in living, not political faiths; a bilateral loyalty, not commercial or social projects. Yet it is an association for as noble a purpose as any involved in our prior decisions."

The poetic sentiments expressed in *Griswold* presented feminists with a dilemma: on one hand, the decision advanced the cause of reproductive freedom; on the other, it did so by drawing the usual curtain around the nursery and the bedroom, thereby reasserting the home as a place removed from and, in significant ways, superior to larger social, economic, and political realities. This apolitical or anti-political definition of domestic relations has bedeviled privacy theorists—especially those committed to equal rights for women, gays and lesbians, and other marginalized groups—ever since. Feminists and gay rights advocates have, for the most part, supported the line of Supreme Court cases that built on *Griswold* because these rulings explicitly extended the right to privacy to unmarried persons, women, and homosexuals and, consequently, offered these groups protections that had previously been denied to them. However, feminist scholars have also called attention to the ways in which *Griswold* and similar decisions failed to address the problematic aspects of privacy.

For example, in a series of landmark cases, including *Eisenstadt v. Baird*, 405 U.S. 438 (1972), *Roe v. Wade*, 410 U.S. 113 (1973), *Planned Parenthood v. Casey*, 505 U.S. 833 (1992), and *Lawrence v. Texas*, 539 U.S. 558 (2003), the Court reaffirmed, with important modifications, the right to privacy outlined in *Griswold*, but it did so by casting a similarly gauzy light on the private sphere, evoking the home as a seemingly problem-free zone in which issues of violence, abuse, poverty, and inequality apparently impose no limits on the capacity of individuals to act upon their existential desires. Thus, in *Casey*, in a passage that has since been ridiculed by conservatives such as Justice Antonin Scalia, the Court upheld earlier rulings on the sanctity of the home by observing, "At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life." The problem with these sentiments, from the standpoint of feminist theory, is not that they are false, but that they set up the private sphere as the realm in which we realize ourselves as human beings. However, as Charlotte Perkins Gilman asserted over a century ago, and as feminists have repeated since, self-realization is simply not a private activity, regardless of the extent to which individuals might benefit from the possession of rights to privacy. In short, many feminists argue, even if the right to privacy has shaken off its anti-feminist heritage, it must be acknowledged that democracy, at least as an organized system of government, cannot be practiced in the privacy of people's homes.

See also: **Constitutional protections; Privacy, definition of**

Suggested Reading: Allen, Anita. *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability*. Totowa, NJ: Rowman & Littlefield, 2003; Allen, Anita, and Erin Mack. "How Privacy Got Its Gender," *Northern Illinois University Law Review* 10 (1990): 441–454; Brandeis, Louis, and Samuel Warren. "The Right to Privacy," *Harvard Law Review* 4, no. 5 (December 15, 1980). <http://historyofprivacy.net/RighttoPrivacy.html>. Online March 2006; Friedan, Betty. *The Feminine Mystique*. New York: W. W. Norton, 1963; Gallagher, Susan E. *Be It Ever So Humble: The Making of the American Home: 1869–1930*. <http://faculty.uml.edu/sgallagher/historyhome.htm>. Online, March 2006; Gilman, Charlotte Perkins. *Women and Economics*. Boston: Small, Maynard & Company, 1898. <http://digital.library.upenn.edu/women/writers.html>. Online, March 2006; Kumar, Krishan. "Home: The Promise and Predicament of Private Life at the End of the Twentieth Century." In Jeff Weintraub and Krishan Kumar (eds.). *Public and Private in Thought and Practice: Reflections on a Grand Dichotomy*, pp.204–236. Chicago: University of Chicago Press, 1997; Steinem, Gloria. "Women's Liberation Aims to Free Men, Too," *New York Times*, June 7, 1970. <http://scriptorium.lib.duke.edu/wlm/aims/>. Online, March 2006.

Susan E. Gallagher

Hoover, J. Edgar (1895–1972)

J. Edgar Hoover was born on January 1, 1895, in Washington, D.C., the son of a lowly civil servant employed in the U.S. Coast and Geodetic Survey. Hoover grew up and lived his entire life in the nation's capital. Forgoing a traditional college education, he attended night school at George Washington University Law School (working during the day at the Library of Congress), receiving an LLB in 1916 and an LLM in 1917. Although he graduated shortly after Congress declared war on Germany in World War I, Hoover did not serve in the military but instead, in July 1917, accepted a draft-deferred appointment in the alien registration section of the Department of Justice. In 1918 he was appointed an assistant to the attorney general and in 1919 headed the department's recently created General Intelligence Division, where he compiled dossiers on thousands of radical activists and played a key role in planning and orchestrating the Palmer Raids of January 1920. Promoted to assistant director of the Bureau of Investigation in 1921, Hoover was appointed acting bureau director in May 1924, after Attorney General Harlan Fiske Stone had fired the current director, William Burns, an appointment made permanent in December 1924. Hoover served as bureau director (renamed the **Federal Bureau of Investigation (FBI)** in 1935) until his death on May 2, 1972.

Hoover's appointment as bureau director in May 1924 occurred following a series of highly controversial revelations that bureau agents and the bureau's most recent director had abused power during World War I and the early postwar years. These included bureau monitoring of political and labor union activists and investigating members of Congress who had played key roles in triggering a congressional investigation into the Teapot Dome scandal, a scandal that involved senior officials in the current Harding administration. As director, Hoover instituted a series of reforms to improve the quality of bureau personnel and to preclude future



abuses of power. In the process, he refurbished the bureau's reputation and helped forge a highly professional and respected law enforcement agency. Sensitive to prevailing states' rights fears, and to the adverse publicity and congressional inquiries that had tarnished the early bureau, Hoover acted to project an image of the FBI agent as an apolitical professional. Then, during the 1930s, he purposefully cultivated both the print media and Hollywood to convey the image of the so-called G-man, the efficient professional who always got his man and respected the law and the Constitution.

None of this meant that Hoover had abandoned monitoring radical activists, as exemplified by the central role he played in orchestrating the 1920 Palmer Raids. Nor, given his personal moralistic views, was the judgmental director indifferent to the sexual indiscretions of American citizens. Attuned to the moralistic politics of the 1920s, as captured in the enforcement of the Prohibition Amendment and the rise of religious fundamentalism, Hoover authorized the creation of a discrete "obscene file" in March 1925 to ensure more successful prosecution of purveyors of obscenity and pornography. Creation of this central file ensured a permanent repository of salacious literature and the ability to engage the support of social conservatives. In a companion action, during the late 1930s Hoover himself led highly publicized vice raids in Miami, Florida, to apprehend and prosecute prostitutes and their customers, ostensibly because local police and civic officials protected houses of prostitution.

The combination of Hoover's moralistic and anti-radical sentiments underlay his leadership of the FBI and the attendant practice of collecting and maintaining files recording the illicit sexual and political activities of American citizens and alien residents. He devised sophisticated filing procedures to preclude discovery of FBI practices such as the collection of noncriminal information, the resort to intrusive but illegal investigative techniques, and the purposeful dissemination of derogatory information to the media, members of Congress, and officials in the military and the White House. Hoover thus created an agency that both promoted law enforcement and engaged in political containment. These practices began informally but were refined and expanded during the Cold War years. The FBI director was then able to tap into concerns about ostensible security threats, such as subversion and homosexuality, without any meaningful oversight. The culmination of these practices came in the 1950s, when Hoover launched a Mass Media program (1955) and, then, in 1956 the first of five **Counter Intelligence Programs (COINTELPRO)**, whereby derogatory information about radical activists and suspected subversives was publicly leaked to raise doubts about their loyalty and moral character. In the authorization language of the formal COINTELPRO, the purpose was to "harass, disrupt, and discredit." In 1951, capturing the homophobia of the time, which viewed homosexuals harshly and as vulnerable to blackmail, Hoover also launched a formal Sex Deviate program to purge homosexuals from federal employment and from influential posts in the private sector. The FBI director's interest in illicit sexual activities was not confined to homosexuals, but extended to heterosexual conduct. This has been indirectly confirmed by the massive files that he maintained in his office about the sexual activities of civil rights leader Martin Luther King, Jr., Senator and later President John F. Kennedy, various members of Congress, and First Lady Eleanor Roosevelt. Some information was obtained through illegal wire-

taps and bugs, while other information was gleaned from unverified rumors and malicious **gossip**.

The FBI director was able to finesse any inquiry into his collection of and efforts to act upon such personal information. On the one hand, by creating a secret office file, Hoover could truthfully deny that the FBI maintained derogatory personal information about prominent Americans in its central records system. Hoover also had FBI officials compile summary memoranda (i.e., not files) detailing any information that FBI agents had collected about the “immoral and subversive” activities of members of Congress; these memoranda were also not maintained in the FBI’s central records system but rather in the administrative unit.

During Hoover’s tenure as FBI director, many suspected that he collected personal and political information about political activists, including members of Congress, and used this information to advance his own political objectives. Indeed, during an interview in the late 1970s with Ovid Demaris, Emanuel Celler (the former chair for 22 years and member for 40 years of the House Judiciary Committee) specifically attributed Hoover’s power to the fact that he was the head of an agency that, in turn, had tremendous power, including the power of **surveillance** and the power of information control, over the lives and destinies of everyone in the nation. Hoover had a dossier on every member of the House and every member of the Senate. Despite his powerful congressional position with the attendant ability to subpoena FBI records and testimony, Celler never launched an investigation to confirm his suspicions. Had he done so, Hoover could have truthfully denied that the FBI compiled dossiers on members of Congress, since there were none in the FBI’s central records system. Nor, in truth, given the FBI’s limited resources, could the FBI affect the lives and destinies of everyone in the nation. Yet Hoover did not need to exercise such powers; it sufficed that members of Congress, the public, and the media believed that he could. Similarly, radical activists might not have suspected that they were targets of specific FBI containment efforts. Hoover’s success in immunizing FBI operations from public scrutiny had a chilling effect on public debate while permitting FBI officials to violate privacy rights.

Hoover’s death in May 1972 predated congressional investigations, first in 1973 into the Watergate break-in and then in 1975 into the U.S. intelligence agencies through the **Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities** (known as the Church Committee). These investigations shattered this wall of **secrecy**. Responding to these dramatic revelations, Congress enacted the **Privacy Act of 1974** and authored a series of amendments to the 1966 **Freedom of Information Act** that permitted citizens to obtain access to FBI records, with a resultant documentation of the scope of Hoover’s violation of privacy rights and of the methods he had employed to preclude discovery. Hoover’s iconic status was shattered to the extent that he himself became the victim of a salacious, best-selling biography written by Anthony Summers and published in the 1990s. Without solid evidence, the book portrayed Hoover as a homosexual and transvestite, and alleged that his sexual orientation had caused him to be black-mailed into not prosecuting organized crime.

See also: **Confidentiality; Constitutional protections; House Un-American Activities Committee (HUAC); Internal Security Act of 1950; McCarthyism; National Crime Information Center; Wiretapping**



Suggested Reading: Gentry, Curt. *J. Edgar Hoover: The Man and the Secrets*. New York: W. W. Norton, 1991; Johansson, Warren, and William A. Percy. *Outing: Shattering the Conspiracy of Silence*. San Francisco: Harrington Park Press, 1994; McGhee, Millie L. *Secrets Uncovered: J. Edgar Hoover—Passing for White?* Rancho Cucamonga, CA: Allen-Morris, 2000; Summers, Anthony. *Official and Confidential: The Secret Life of J. Edgar Hoover*. New York: Putnam, 1993; Theoharis, Athan. *The FBI and American Democracy: A Brief Critical History*. Lawrence: University Press of Kansas, 2004.

Athan Theoharis

House Un-American Activities Committee (HUAC)

The House Un-American Activities Committee (HUAC) was formed on May 26, 1938, and abolished in January 1975. The committee was created to investigate disloyalty and “subversive activities.” Initially, HUAC’s investigations were directed primarily at right-wing groups, including a number of pro-fascist organizations and the Ku Klux Klan. However, these investigations were generally short and perfunctory. Under the direction of Chairman Martin Dies, Jr., the committee (informally known as the Dies Committee) quickly adopted an anti-Communist agenda, investigating the infiltration of American institutions by Communists and Soviet sympathizers. Ironically, the committee’s founding co-chair, Samuel Dickstein, would himself be named as a Soviet operative by the VENONA Project, a top-secret effort to decode Soviet communications.

Today, many consider the HUAC hearings to be the political equivalent of witch hunts. However, HUAC played a crucial role in defining Congress’s power to investigate the private associations and activities of American citizens. The committee developed a number of techniques that would later be adopted by Senator Joseph McCarthy’s Government Operations Committee. Sweeping allegations were made. Witnesses were pressured to reveal the names of former and current associates, and those who refused were often charged with contempt. Being questioned as an “unfriendly witness” or being mentioned during HUAC hearings was considered an indication of guilt. Even the mere association with suspect organizations was considered enough to prove one’s disloyalty, setting the standard for guilt by association.

During the prewar years and the early years of World War II, HUAC’s activities were focused on developing legislative policy and investigating the Communist influence within labor unions and government programs. The first legislation proposed by the committee was the Voorhis Act that was signed into law in 1940. The act had two parts. First, it required groups representing foreign governments to be registered with the U.S. attorney general’s office. Second, it required the registration of paramilitary groups and organizations that advocated the forcible overthrow of the U.S. government. The Voorhis Act did not include criminal penalties for membership in these organizations.

The Voorhis Act was quickly followed by Alien and Registration Act of 1940 (generally referred to as the Smith Act), which was far more sweeping. Not only did the Smith Act make it illegal to organize, join, or affiliate oneself with the groups listed in the Voorhis Act, but it also broadened the definition of what was

considered subversive activity. Anything advocating the overthrow of the government, or that presented the overthrow of the government as necessary or desirable, was rendered criminal. Furthermore, those found printing, publishing, teaching, or publicly displaying such material with the intent to overthrow the government could receive a prison sentence of up to 20 years. Although critics argue that the law violates the First Amendment, in cases such as *Yates v. United States* and *Noto v. United States*, the Supreme Court has repeatedly upheld its constitutionality, though it has advocated a more limited interpretation of the act.

Spurred by a number of sit-down strikes by automobile workers, Dies launched investigations into organized labor beginning in 1938. Among the first organizations to be investigated by the committee were the newly formed Congress of Industrial Organizations (CIO) and a number of its local chapters. The result of these investigations was a shift in CIO policy so that unions could be expelled if they were deemed to be “consistently directed toward the achievement of the program purposes of the communist party” (CIO constitution, Article VI). Eleven unions had been expelled from the CIO as “communist dominated” by 1950. Among these unions was the United Electrical, Radio, and Machine Workers Union of America (UE), which represented every General Electric and Westinghouse plant in the United States.

HUAC began hearings in Chicago to investigate the Communist influence within the steel workers union in 1939. Only two years prior, Chicago had been the site of an unprovoked police attack on striking steel workers that had resulted in 10 strikers being killed and another 90 injured. HUAC placed the blame for such acts of violence on Communists, who were undermining union goals. However, HUAC’s claims of Communist influence were so sweeping that they acted more as an ideological attack against organized labor than a practical attempt to excise radical revolutionaries from the union ranks.

During this period, HUAC also held a number of investigations into Communist infiltration of government agencies. One of the earliest hearings involved the Federal Theater Project (FTP), a program started by President Franklin D. Roosevelt during the Great Depression to employ out-of-work theater workers. Among those that were brought before the committee as unfriendly witnesses was Project Director Hallie Flanagan. Committee members implied Flanagan had Communist leanings, citing her support for controversial theatrical productions and her tour of Russian theaters while studying in Europe during the 1920s. It was also during this hearing that one HUAC member embarrassed himself by asking Flanagan if the Elizabethan playwright Christopher Marlowe had been a member of the Communist Party. The HUAC hearings on the FTP would ultimately lead to that program being shut down in 1939.

Perhaps the pinnacle of HUAC investigations into government agencies was the case of Alger Hiss. In 1948, President Truman publicly called HUAC’s attempts to weed out Communists a “red herring.” HUAC used its investigation of Alger Hiss, at the time a high-level State Department employee, to reaffirm its place within American politics. Hiss was convicted of perjury and was perceived to be a Soviet agent, although that would never be proven. The hearings also made HUAC committee member Richard Nixon a major political player on the national scene.



In the late 1940s, HUAC shifted its attention to Hollywood. The committee believed the film industry had a unique capacity to shape public discourse and that it was heavily infiltrated by Communists and Soviet sympathizers. For nearly a decade, HUAC subpoenaed members of the film industry—both as friendly and unfriendly witnesses—and demanded they disclose whether they were members of the Communist Party and name any acquaintances who were Party members. Among the most famous witnesses were a group of filmmakers and screenwriters, dubbed the Hollywood Ten, who refused to answer questions regarding their union and political affiliations. They argued that the committee's questions violated privacy-related constitutional principles, including those regarding the secret ballot and freedom of association. The Hollywood Ten were cited for contempt of court and sentenced to one year in prison. The Supreme Court refused to hear their appeal.

The hearings resulted in the creation of the Hollywood blacklist, an effort spearheaded by such cinematic luminaries as John Wayne and Ronald Reagan. The blacklist denied those believed to be Communists or Communist sympathizers from working in Hollywood or being members of one of the industry's labor guilds. Thousands of producers, directors, actors, screenwriters, and technical workers were blacklisted, including the Hollywood Ten. While some were able to continue their careers in the theater, or continue working using non-blacklisted colleagues as cover, many struggled to piece shattered lives back together. The blacklist remained in place until 1956, when actor/producer Kirk Douglas gave the screenwriting credit for his film *Spartacus* to Dalton Trumbo, one of the Hollywood Ten.

By the 1960s, the committee had shifted its focus from Hollywood to the new wave of social activist movements. Among the groups investigated was the Student Nonviolent Coordinating Committee (SNCC), which pushed for the use of federal intervention in support of the civil rights movement. Representative William Colmer of Mississippi asserted that SNCC was "aiding the Communists to enslave the world" (HR 738, 89th Cong., 2nd Sess.). Portrayals of the group in mainstream media contradicted this claim, showing SNCC's public disdain for Marxist-Leninism, or for any other organized ideology. Instead, SNCC's efforts to involve the federal government in support of civil rights appear to have been the more practical reason for the HUAC investigation. Several HUAC committee members, including William Tuck and Edwin Willis, actively resisted federal intervention, including efforts to enforce *Brown v. Topeka Board of Education*. Members of SNCC who were called before the committee invoked the Fifth Amendment.

Other HUAC investigations during this time focused on public school teachers in San Francisco, anti-war protesters in Berkeley, members of the Progressive Labor Party, and even working mothers in California and Ohio. These investigations were increasingly viewed as publicity stunts by the general public, and were heavily criticized by the media for prying into the private political beliefs and associations of witnesses. The public perception of HUAC was further eroded as witnesses made a mockery of hearings; for example, social activist Abbie Hoffman appeared before the committee wearing a clown suit. The committee was renamed the Internal Security Committee in 1969 in an attempt to reinvent itself. The committee's influence continued to wane, and it was abolished in the beginning of

1975. While often viewed as a dark part of American history, HUAC served as a flashpoint in the debate on privacy, national security, political freedom, and **freedom of association**.

See also: **Constitutional protections; Counter Intelligence Program (COINTELPRO); McCarthyism**

Suggested Reading: Goldstein, Justin Robert. *Political Repression in Modern America from 1870 to 1976*. Chicago: University of Illinois Press, 2001; Navasky, Victor S. *Naming Names*. New York: Hill and Wang, 2003; Schrecker, Ellen. *The Age of McCarthyism: A Brief History with Documents*. Boston: St. Martin's Press, 1994. <http://www.writing.upenn.edu/~afilreis/50s/schrecker-age.html>. Online, March 2006.

Brian L. Zirkle

Hudson v. Palmer, 468 U.S. 517 (1984)

The Supreme Court first addressed whether the Fourth Amendment applies to searches of prison cells in its 1984 decision *Hudson v. Palmer*. Palmer, a prisoner in a Virginia state correctional institution, underwent a “shakedown search” of his cell. Correctional officers regularly conduct shakedowns to look for contraband, especially drugs, homemade alcohol, and “shanks,” or homemade weapons. In Palmer’s case, officers found a ripped pillowcase, which was considered contraband. Although possessing a ripped pillowcase is far less serious than possessing a weapon, officers search for and confiscate such items because prisoners are not permitted to keep more than a certain number of towels and clothing items in their cells at any one time. They are also not permitted to alter state property. These rules are designed to keep inmates from using extra or altered items to facilitate escape attempts or make homemade alcohol and weapons. The rules also help institutions maintain an adequate inventory of clothing, bed sheets, and towels.

Palmer was charged with destroying state property and ordered to reimburse the state. He filed a civil rights lawsuit under 42 U.S.C. §1983, claiming that Officer Hudson had conducted the search in order to harass him, thereby violating his Fourth Amendment right to be free of unreasonable searches. He also alleged Hudson violated the Fourteenth Amendment’s Due Process Clause because he intentionally destroyed the pillowcase during the cell search, thereby depriving Palmer of property he had a right to possess. The trial court granted Hudson’s motion for summary judgment, agreeing with the officer that Palmer had no case. The court of appeals, however, reversed on the issue of whether Palmer’s Fourth Amendment rights had been violated. The appellate court ruled that inmates have a limited right to privacy in their cells and should be protected against searches conducted solely to harass or humiliate them.

In Hudson’s appeal to the Supreme Court, the issue was whether the search of Palmer’s cell violated his Fourth Amendment right to be free from an unreasonable search. In an important decision that has had a significant impact on the rights of prisoners, the Court ruled the Fourth Amendment does not apply to cell searches because prisoners do not have a **reasonable expectation of privacy** in their cells. The Fourth Amendment only protects places and things in which a person has a reasonable expectation of privacy. The Court found that privacy is incompatible



with the need to maintain prison security and **surveillance**. The Court noted, however, that its decision does not give officials the right to destroy inmates' property or use cell searches to harass prisoners.

The *Hudson v. Palmer* case allows officials to conduct cell searches with few restrictions. Officials can conduct a cell search without probable cause, reasonable suspicion, or even a hunch that an inmate possesses contraband. In fact, officials conduct shakedowns on a routine basis and are not required to give prisoners prior notice or seek consent. Cell searches can be quite extensive, with officials opening up and emptying closed containers, shifting mattresses around, and rifling through a prisoner's personal papers, books, and magazines. Officials are not required to conduct a cell search with the prisoner present.

Cell searches are often flashpoints between inmates and officials. A cell is an inmate's **home** and the most personal space he or she has inside a correctional institution. A cell is where an inmate keeps family photos and letters, legal papers, and food purchased from the commissary. A prisoner might have been permitted to have a typewriter, radio, hotplate, or television in the cell, and all of these would be subject to search. A cell search is not always a gentle and orderly event, and an inmate's cell can be left in some mess after it is over. Officers can be rough with an inmate's belongings during the search. Nonetheless, the Supreme Court has made it almost impossible for a prisoner to challenge a cell search. Unless an inmate can establish that the search was intentionally conducted to harass him or her—evidence can be difficult to collect—the search is not restricted by the requirements of the Fourth Amendment.

See also: **Constitutional protections; Prisoners**

Suggested Reading: Branham, Lynn. *The Law of Sentencing, Corrections, and Prisoners' Rights*, 6th ed. St. Paul, MN: West, 2002; Schlanger, Margo. "Inmate Litigation," *Harvard Law Review* 116 (2003): 1555–1706; Smith, Christopher. "Boundary Changes in Criminal Justice Organizations: The Governance of Corrections: Implications of the Changing Interface of Courts and Corrections." In *Criminal Justice 2000*, Gary LaFree (ed.). Washington, DC: National Institute of Justice, 2000.

Barbara Belbot

Human immunodeficiency virus (HIV). *See* **Assisted reproductive technologies; Health privacy; Patient rights; Public health and safety**

Human subjects protections

Human subjects protections in biomedical and social research intersect with privacy issues in three areas: the conflict between informed consent procedures and **confidentiality** assurances; legal issues pertaining to the researcher and the privacy of research data; and the public or private provenance of research data funded by governmental agencies. The first issue concerns the privacy of the research respondent's life, and the second and third concern the privacy of the researcher's data.

Human subjects protections refer to standards and procedures set in place to ensure that unnecessary harm is not inflicted on research subjects (the harms/benefits ratio); that their participation is confidential; and that they are informed of, and consenting to, the research. These protections are in place at every level of research, from

federal funding agencies to university departments and classrooms, and pertain to both funded and unfunded research. Additional protections are added when research subjects are not fully consenting adults: those under 18, pregnant, incarcerated criminals or patients, the elderly, or the developmentally disabled.

Over time, human subjects protections have expanded from biomedical to social science research, and—within the social sciences—from experimental studies to interviews, ethnographic applications, surveys, and even historical research. The origins of public concern with the protection of human subjects can be found in various forms of biomedical experimentation that took place in the twentieth century, most notably those occurring in Hitler's Germany and in the Tuskegee Institute's 1932–1972 syphilis study in the United States. In both these instances, and in many others all around the world, people were subjected to physically harmful—even fatal—biomedical experimentation without their knowledge or consent. Today, if biomedical research might harm research subjects, the subjects must be informed of and consent to such harm; furthermore, any harm to individuals must be counterbalanced by benefits to other individuals or to the community.

In social science research, harm is not physical but may be psychological or social: emotional disturbance as a consequence of the conduct of the research, or violations of privacy that occur as a result of the dissemination of research data or publication. Emotional harm is most likely in two kinds of research situations: interviews on disturbing topics and deceptive research, in which the subject is left feeling duped or stupid. Deceptive research as a problem in human subjects protections came into focus in the early 1970s with the publication of Laud Humphreys's book *Tearoom Trade*. In this book, Humphreys violated his respondents' privacy in two ways: he observed their sexual acts in public restrooms, and he posed as an interviewer on a different topic to get marital and other information from them. Although deceptive research is permissible under some circumstances, today these circumstances are very limited.

Violations of respondents' privacy may lead to emotional harm if any such violation has consequences such as legal action or stigmatization—this is particularly problematic if the research is on sensitive subjects such as sexual behavior, criminal activity, or illegal drug use. Human subjects protections have, however, been extended into areas of research that are not as sensitive, for example ethnographic research on public behavior, on the grounds that all forms of experimentation or observation are violations of privacy.

Ironically, privacy protections may come into conflict with another standard of research protection: the requirement for informed consent. Informed consent procedures involve a considerable amount of written, signed, and stored documentation that, by its very existence, can threaten respondents' privacy and possibly produce negative consequences. Respondents have been known to refuse to participate in research where they have to sign their names to consent documents, seeing the signing of the documents as a violation of their privacy.

The second area in which privacy is at issue in social science research is that of the legal status of research data, especially data derived from interview or field research. Protected by the First Amendment, a journalist may interview anyone she/he chooses to, use the interviewee's name in a subsequent article, and make stigmatizing assessments of the interviewee—so long as these assessments are “the truth.” An ethnographer studying the same setting in the same city is not protected by the First



Amendment and so would have to seek permission and informed consent from the respondent, and give assurances of **confidentiality** (**anonymity** may be promised in survey research, but in interview or field research the respondent is not anonymous). Both the journalist's notes and the ethnographer's field notes may be subpoenaed, but there is no privacy protection in law for the ethnographer's information.

The *Brajuha*, *Scarce*, and *Leo* legal cases in the 1980s and 1990s involved attempts to subpoena sociology graduate students' field notes—concerning, respectively, a restaurant that had burned down, a radical environmental group, and police interrogation rooms. While Leo did turn over his field notes to authorities, thus violating his promises of confidentiality to those contacted and their right to privacy, both Brajuha and Scarce refused. In the *Brajuha* case, the subpoena demands were dropped, but Scarce spent 159 days in jail.

The third issue in the relationship between privacy and research is the public versus private nature of the data gathered by publicly funded research, and thus its availability to researchers other than the principal investigator. Although unfunded research data, such as field notes, may be subpoenaed, other researchers have no legal right to them. In contrast, research that is publicly funded is, in theory, the property of the public rather than of the private citizen or agency that conducted the research. There is a “gentle agreement” in place that the researcher may “own” the data for a year to analyze and write it up, but after that it will be made available upon request. But in practice, and especially with qualitative research that cannot promise absolute anonymity, the issue of informed consent has been used by governmental agencies to restrict other researchers' access to data. Even data gathered with careful informed consent procedures in place have been denied to researchers because they might be parsed for private information about respondents.

The essence of research with human subjects is the tension between the respondents' privacy and the public's right to knowledge; **journalism** is subject to the same tension, but with a different, First Amendment set of resolutions. In the case of research, there is also the question of the researcher's data as public or private with respect to the law, and as public or private property in relation to public funding. Human subjects guidelines have expanded and have been challenged over the past half century, and a continuation of developments and challenges can continue to be expected.

Suggested Reading: American Sociological Association. “Governance: Constitution/Bylaws Changes and Council Policymaking.” www.asanet.org. Online, March 2006; Humphreys, Laud. *Tearoom Trade: Impersonal Sex in Public Places*. Piscataway, NJ: Aldine Transaction, 1975 (1970); National Institutes of Health. *Bioethics Resources on the Web*. www.nih.gov. Online, March 2006; Shamoo, Adil E. *Ethics of the Use of Human Subjects in Research*. Oxford, UK: Garland Science, 2002.

Carol A. B. Warren

I



Identity fraud

There are several varieties of identity fraud, including application fraud and account takeover. Application fraud occurs when a thief obtains new **credit cards** and loans in another person's name. The imposter might also open telephone and electrical utility accounts, rent an apartment, get a mobile phone, or buy a car or home. Victims are not likely to notice application fraud for many months because the thief uses a different address for the monthly account statements. Victims usually find out when they apply for credit cards or a loan and are rejected because they have a low **credit rating**—the result of the imposter's unpaid bills and past-due accounts. This type of fraud is sometimes called new account fraud or true name fraud.

Account takeover occurs when the thief obtains the account number of the victim's existing credit or bank account. The thief might steal the victim's wallet containing credit cards or find credit transaction slips in trash containers. A thief who knows how to hack into a business's **computer** system can obtain credit account numbers over the **Internet**. Dishonest employees have been known to copy the data from the magnetic strip of a customer's credit card onto a handheld device called a skimmer and later download the account number and expiration date to a computer. The thief can use the account information for Internet shopping and can also create counterfeit credit cards with the data. This type of fraud is also known as existing account fraud. It is usually discovered when the victim notices charges on the monthly bill and reports them to the credit card company.

Criminal identity theft occurs when the imposter is arrested for a crime and provides the victim's name to law enforcement. For nonviolent crimes like traffic violations and shoplifting the individual is usually released and told to appear in court later. Then, when the imposter fails to appear for the court hearing, the judge issues a warrant for the arrest of the innocent person. It is often difficult for the victim to prove that he or she is not the person who committed the crime. In the workplace, employment identity theft is perpetrated when the imposter assumes the name and/or **Social Security number** (SSN) of another person. This usually involves undocumented immigrants or individuals who want to hide a criminal record.



Millions of individuals are victims of account takeover and application fraud each year. A 2003 survey by the Federal Trade Commission (FTC) found that over 10 million individuals were victims in the previous year. A follow-up to that survey was published in 2006 by Javelin Strategy and Research and the Better Business Bureau. It found that nearly 9 million individuals in the United States were victims in the prior 12 months. Approximately two-thirds of victims in both surveys experienced account takeover, while one-third were victims of new account fraud. The FTC survey estimates that nearly 5 percent of American adults, or 1 in 20, discovered they were a victim of identity fraud in the past five years.

Over half of all victims do not know how the imposter was able to obtain their personal information in order to impersonate them. But of those who know the identity of the perpetrator (36 percent of the Javelin study's sample), half of the perpetrators were relatives, friends, neighbors, or in-home employees or were otherwise closely associated with the victim. The Javelin survey estimates that the loss to businesses was \$56.6 billion in 2006. The average cost per fraud victim was \$6,383, although federal law protects victims from having to pay the imposter's bills.

Statistics do not adequately describe the impact of identity fraud on its victims. Even though each case is different, the experiences of victims are similar. Victims typically must invest a great deal of time to regain their financial health. Many must take time off from work to make the necessary phone calls, write letters, report to law enforcement, and follow up with the credit-reporting bureaus and credit issuers. Some situations require victims to hire an attorney. Many victims report they do not get effective help from the credit grantors, banks, and credit bureaus. They describe difficulty in reaching the credit-reporting agencies and may be treated disbelievingly by some creditors. Victims must also deal with collection agencies, and many report being treated abusively by debt collectors. Victims may be threatened with lawsuits, garnishing of wages, and having their homes repossessed.

Identity fraud has increased in recent years for several reasons. It is easy for criminals to obtain the information needed to impersonate others in the financial marketplace. Financial companies have adopted the SSN as the key customer identifier. All the imposter needs is an individual's name and SSN in order to fill out an application for credit. Finding the individual's date of birth is not difficult because of free resources on the Internet. The imposter usually fabricates the other data elements on the application form. Identity thieves use a number of ploys to obtain SSNs and other identifying information. They steal wallets, which often contain Social Security cards or other documents with the SSN in them. Thieves also steal mail in search of documents that contain financial account numbers and Social Security numbers. They sift through the trash outside of businesses and residences to find documents containing **personally identifiable information**. Fraudsters also employ phishing to get financial account numbers and SSNs directly from unsuspecting individuals. They obtain the e-mail addresses of millions of individuals and send messages that purport to be from the consumer's bank or credit card company.

The practices of credit issuers also facilitate identity fraud. Many retailers invite their customers to apply for credit on the spot, often offering them a significant discount on the items they have just purchased as an incentive. Within minutes, the

merchant is able to check the applicant's credit score and extend credit to the shopper. Such opportunities do not entail exhaustive authentication procedures, making instant credit one of the more popular strategies for identity thieves.

Another reason identity fraud has skyrocketed is that most law enforcement agencies do not have adequate staff and resources to investigate the crimes and apprehend the criminals. Not only are such investigations highly labor-intensive and time-consuming, but most cases involve multiple jurisdictions. Local law enforcement agencies are traditionally bound to their own city or county, even though a typical identity fraud case can extend to numerous cities, counties, and even states. As a result, identity thieves are rarely apprehended and sentenced. If they are, penalties are minimal and may include only brief prison sentences compared with those for violent crimes.

In recent years Congress and many state legislatures have strengthened the penalties for identity fraud. According to the FTC, in the past decade all of the states have adopted laws that criminalize identity fraud. In 1998 Congress passed the Identity Fraud and Assumption Deterrence Act, which makes it a federal felony to knowingly use the identification of another person with the intention to commit an activity that violates federal or state law. The law also established an identity fraud clearinghouse within the FTC.

The 2003 amendments to the federal **Fair Credit Reporting Act** include several provisions that address victim assistance and credit industry practices. The Fair and Accurate Credit Transactions Act, or FACTA, gives consumers nationwide annual access to their credit reports at no charge. In 2003, California enacted a law requiring that individuals be notified when a data breach has occurred involving sensitive personal information—specifically, SSNs, driver's license numbers, or financial account numbers. In the years since then nearly half of the states have adopted similar legislation. California was also the first state to adopt a law enabling individuals to place a security freeze on their credit reports. Considered by victims' advocates to be the most effective form of protection, a credit freeze prevents credit granters from accessing individuals' credit reports. Creditors typically check the credit reports of applicants before extending credit to the individual. When an individual establishes a security freeze, the creditor is unable to check the credit report and rejects the imposter's application. A dozen states have followed California's lead in enacting security freeze laws.

In 2005 Congress considered nearly a dozen bills addressing identity fraud, data security, and Social Security number restrictions. With names like Identity Theft Protection Act and Personal Data Privacy and Security Act, the bills would extend many of the provisions adopted by state legislatures to the entire nation. While there are obvious benefits to expanding identity fraud protection to consumers nationwide, many privacy advocates are critical of the preemption clauses in those bills because they would in effect strike down state laws that are stronger than legislation enacted by Congress. By the end of the 2005 legislative year, Congress had not adopted any identity theft-related bills, although more activity was expected for 2006.

See also: **Background checks; Banking and financial records**

Suggested Reading: Identity Theft Resource Center. <http://www.idtheftcenter.org>. Online, March 2006; Mari, Frank. *From Victim to Victor: A Step-by-Step Guide for*



Ending the Nightmare of Identity Theft, 2nd ed. Laguna Niguel, CA: Porpoise Press, 2005; Privacy Rights Clearinghouse. *Identity Theft Resources*. <http://www.privacyrights.org>. Online, March 2006; U.S. Federal Trade Commission. *Welcome to the Federal Trade Commission, Your National Resource about Identity Theft*. <http://www.consumer.gov/idtheft>. Online, March 2006.

Beth Givens

Industrial espionage

Industrial espionage refers to the clandestine acquisition of desirable business practices and/or technology by one company from another. By contrast, economic espionage refers to the clandestine acquisition of desirable business or government practices and/or technology by a foreign *government* or a company with the assistance of a foreign government. These definitions assume a clear separation between business and government, which is not always the case. Different countries at different times have been in “learning roles” instead of “innovating roles”; in other words, some nations’ economies are copying or “learning” industry organization and production techniques. The United States was once in a learning role, learning about industry organization from England. A more recent example is the so-called East Asian Tigers (a term referring to Hong Kong, Taiwan, Singapore, and South Korea) learning from industrialized nations to facilitate the emergence of their late industrial period. This example, however, is neither industrial espionage nor economic espionage. Espionage must be a direct instance of a company having some specific item, process, idea, project, or technology actually copied for the benefit of some other company or companies.

The U.S. Congress has become interested in this type of economic interaction and has passed the Economic Espionage Act of 1996 (EEA). This legislation gives the United States the explicit ability to prosecute specific acts of espionage both foreign and domestic. It is meant to provide more tools for the defense of an increasingly globalized information network. It was advocated by both the U.S. government and industry leaders. The legislation defines economic espionage without the distinction mentioned above. Instead, all acts of theft are considered economic espionage. This legislation has already been used to prosecute individuals and groups. The Avery Dennison adhesive technology case is an example. Avery Dennison is a major producer of adhesive products such as stamps and diapers. In 1999, Pin Yen Yang and his daughter were found guilty of paying an Avery Dennison employee, Dr. Ten Hong Lee, to provide them with secret procedures and production methods. Pin Yen Yang was the president of a Taiwanese company that could make direct use of the technology and production techniques.

The EEA is an illustration of a global trend of states to define economic interests as issues of national security. Strangely, this has increased, not decreased, with the end of the Cold War. Intellectual property rights have become more important as the United States has assumed the role of sole superpower; it has become the victim, in some ways, of its own success. Its products (pharmaceuticals, for example) are the main target and model for many other nations and foreign corporations. It is struggling, then, to tighten security on its own copyrights. Direct industrial espionage is one way in which these breaches of copyright are occurring.

Industrial espionage includes attempts to steal any business, financial, economic, scientific, technical, or engineering information. These categories include patterns, plans, designs, compilations, program devices, formulas, prototypes, methods, processes, procedures, programs, or codes, whether tangible or intangible. It does not matter how the information is stored, be it memorized, copied, photographed, or transmitted. The most prosecutable type of industrial espionage is a direct copying of material by an individual or several individuals. Recent prosecutions have involved the hiring of spies in companies or paying off employees of a company for spying activities.

Technology and science have also drastically changed both the perception and implementation of industrial espionage with the advent of the **Internet**. Financial records, prototypes, processes, plans, and so on are increasingly integrated into **computer** networks. As a result, increased pressure to tighten security has been placed on developed economies and corporations. It is likely that keeping up with network security (which includes **surveillance** of those who have access to networks) will continue to increase in importance as the globalized business networks continue to integrate technologically.

See also: **Electronic mail; Electronic surveillance; Secrecy**

Suggested Reading: Barry, Marc, and Adam Penenberg. *Spooked: Espionage in Corporate America*. Cambridge, MA: Perseus, 2000; Nasheri, Hedieh. *Economic Espionage and Industrial Spying*. Cambridge, UK: Cambridge University Press, 2005.

Shaun Parkman

Inevitable discovery

The inevitable discovery doctrine is an exception to evidentiary rules requiring that evidence be suppressed because it was obtained improperly. If the evidence obtained in violation of one's constitutional rights would have eventually been discovered despite the constitutional violation, it will be admitted in court.

The U.S. Supreme Court created the doctrine requiring courts to suppress evidence as the tainted "fruit" of unlawful governmental conduct in its ruling in *Silverthorne Lumber Co. v. United States*, 251 U.S. 385 (1920). In that case, the Court ruled that not only should the illegally obtained evidence be suppressed, but that other incriminating evidence derived from the primary evidence (the "poisonous tree") should be suppressed as well. The *Silverthorne* Court, however, limited its holding, advising that the subsequently discovered evidence does not automatically become "sacred and inaccessible." The Court directed, "If knowledge of [such facts] is gained from an independent source, they may be proved like any others."

In *Wong Sun v. United States*, 371 U.S. 471 (1963), the Court reaffirmed and extended the exclusionary rule to evidence that was the indirect product or "fruit" of unlawful police conduct. Once again, however, it emphasized that illegally obtained evidence need not always be suppressed, stating, "We need not hold that all evidence is 'fruit of the poisonous tree' simply because it would not have come to light but for the illegal actions of the police. Rather, the more apt question in such a case is 'whether, granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that



illegality or instead by means sufficiently distinguishable to be purged of the primary taint.”

While both these cases involved search and seizure violations of the Fourth Amendment, the “fruit of the poisonous tree” doctrine has extended to the violations of the right to attorney guaranteed by the Sixth Amendment, (see, e.g., *United States v. Wade*, 388 U.S. 218 (1967)), as well as to violations of the protections against self-incrimination in the Fifth Amendment (see, e.g., *Murphy v. Waterfront Comm’n of New York Harbor*, 378 U.S. 52, 79 (1964)).

The foundation for the exclusionary rule is that the “drastic and socially costly course” is needed to deter the government from trampling on the constitutional and statutory protections of its citizens. In adopting the rule, the Supreme Court has held that the way to ensure those protections is to exclude evidence even when it means that obviously guilty persons will go unpunished for their crimes. In short, prosecutors are not to be allowed to take advantage of the government’s illegal conduct.

The inevitable discovery doctrine is intended to guarantee that law enforcement and prosecutors are not put in a worse position simply because of some earlier error or misconduct. Thus, the Supreme Court has held that if the government can establish by a preponderance of the evidence that the information or evidence ultimately or inevitably would have been discovered by lawful means, then the exclusion of that evidence will have no deterrent value, and the evidence should be admitted. As the Court noted in *Nix v. Williams*, 467 U.S. 431 (1984), “Exclusion of physical evidence that would inevitably have been discovered adds nothing to either the integrity or fairness of a criminal trial. . . . Fairness can be assured by placing the State and the accused in the same positions they would have been in had the impermissible conduct not taken place.”

Suggested Reading: Black, Henry C. *Black’s Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Dash, Samuel. *The Intruders: Unreasonable Searches and Seizures from King John to John Ashcroft*. New Brunswick, NJ: Rutgers University Press, 2004; Hessler, Stephen E. “Establishing Inevitability without Active Pursuit: Defining the Inevitable Discovery Exception to the Fourth Amendment Exclusionary Rule,” *Michigan Law Review* 99 (2000): 238; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000; Stephens, Otis H. (ed.). *Unreasonable Searches and Seizures, Rights and Liberties Under the Law*. Santa Barbara, CA: ABC-CLIO, 2005.

David J. Brown

Informational privacy. *See* Privacy, definition of

Internal Revenue Service (IRS)

The Internal Revenue Service (IRS) maintains files on every taxpaying American in the United States. The IRS knows not only their names, **Social Security**

numbers, bank account information, and addresses, but also where they work and how much they earn. This type of information is the kind of data that identity thieves, **telemarketers**, researchers, and countless others would like to get their hands on. This information is maintained in government databases and is secured from release to the general public. The **Freedom of Information Act** allows for such data to be shared by other agencies within the government so long as the individual is protected.

This information sharing is no different from a commercial bank sharing certain customer or account information with other divisions within its holding company. Similarly, when financial institutions hire third-party contractors, they must take special steps to maintain the privacy and security of their customers' financial information. The IRS is no different. The American Jobs Creation Act of 2004 created Section 6206 of the IRS Code, allowing the IRS to use private companies as contractors to assist in collecting the estimated \$12 billion in unpaid taxes owed to the U.S. government. This collection agency outsourcing is a cheap and efficient way for the government to collect unpaid taxes, as these contractors would keep only 25 percent of the revenues they collect. However, these contractors would also be privy to the records of the individuals who owe taxes. This is one additional security layer that must be maintained in order to protect information concerning the public.

The Internal Revenue Code, the **Privacy Act of 1974**, and the Freedom of Information Act protect the rights and the privacy of taxpayers. Under the Federal Information Security Management Act, federal government agencies are required to prepare annual reports about their security procedures to the Tax Administration. The Internal Revenue Service also performs evaluations, called Privacy Impact Assessments, on computer systems and software applications to identify any holes in the system that could leak **personally identifiable information** to outside sources.

The Internal Revenue Service and other agencies maintain the privacy of individual taxpayer information and protect this information from release to the public. These organizations, however, have the right to analyze taxpayer data in aggregate for the purpose of decisionmaking. By evaluating an entire population of taxpayer data, the Internal Revenue Service can draw conclusions and create reports on trends and statistical analysis. These reports never reveal any specific information pertaining to an individual taxpayer and thus maintain an individual's privacy. Only government employees who are held to the same data security standards used to protect individual data would perform these analyses.

The Internal Revenue Service may disclose individual taxpayer data from their data systems only with the written consent of the taxpayer in question. The exceptions to this rule are many; they focus mainly on providing such data to government agencies outside the scope of the Internal Revenue Service. The **United States Census Bureau**, for example, may access individual data strictly for the purpose of planning and performing statistical analysis with data from other agencies as allowed by Title 13. Individual taxpayer data may be provided to an individual as long as adequate written assurance is provided that these records will not be released and will be used strictly for statistical purposes with results that do not lead back to any single individual. If such a release of individually identifiable data



should occur, then the person who had received the data from the Internal Revenue Service would be subject to fines and possible imprisonment. Data on an individual may also be provided, without consent, to law enforcement agencies for prosecuting criminal and civil activities so long as the director of the law enforcement agency makes assurances that the data will not be released to the general public.

Any instance in which the Internal Revenue Service releases individual data is logged in a central database by the IRS along with the date, nature, and purpose of **disclosure** to any person or agency for each record. These transcriptions are maintained for a period of not less than five years. This database is designed to assist in the determination of whether individual information has been released and who would be held responsible in the event of a leak.

Once an individual prepares his or her tax return and sends it to the local IRS processing center, there is the expectation that this information remains private. However, the U.S. government is able to use the information provided on the tax return in many ways. Most commonly, the data are aggregated to assist U.S. government agencies in making better decisions in all areas of the government.

See also: **Banking and financial records; Bank Secrecy Act**

Suggested Reading: General Accounting Office Reports & Testimony. *Taxpayer Information: Options Exist to Enable Data Sharing Between IRS and USCIS but Each Presents Challenges*. Farmington Hills, MI: Thomson Gale, 2006; United States Department of the Treasury. Internal Revenue Service. www.irs.gov. Online, December 2005.

Christine Berry Lloyd

Internal Security Act of 1950

The Internal Security Act was passed in 1950 during the height of anti-Communist hysteria in the United States. The act was aimed at furthering a conservative anti-Communist agenda that sought to eliminate Communist influence in American politics and society through coercion. The act is widely regarded by scholars as one of the most egregious attacks on the freedoms of speech and association in American history. Not only was it an attempt to criminalize a particular ideology, but also an assault on private associations that involved no actual criminal activity. The act remained on the books until 1990, and many of its provisions were reinstated with the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)**.

The Internal Security Act made it illegal to pursue a Communist or totalitarian political agenda and required all Communist organizations to register with the U.S. Attorney General. Any organizations that failed to register could be brought before the Subversive Activities Control Board (SACB) and forced to register as Communist. Registered organizations were required to label their publications and broadcasts as originating from a Communist organization. Furthermore, members of registered organizations were denied employment in the government or in private firms with federal defense contracts and were prohibited from applying for or using passports.

The act also contained a number of provisions dealing with immigration and naturalization. Aliens who were at any time members of or affiliated with a Communist or totalitarian party were denied entry to the United States. Those already in the United States could be deported without a hearing. Naturalized citizens could have their citizenship revoked if they joined a registered Communist organization within five years of becoming a citizen. Additionally, aliens who were members of newly registered Communist organizations could be denied naturalization unless they were able to prove that they had left the organization within three months of its being registered.

Finally, judicial standards for search and seizure, the use of informants, **wire-tapping**, and other forms of **surveillance** were relaxed. The act also allowed the president to declare an “internal security emergency,” during which time the Attorney General was empowered to detain anyone who “probably would engage in, or conspire to engage in, acts of espionage or sabotage.” There were provisions for administrative hearings, but not court trials. In this way, Communist organizations remained formally legal, but mechanisms were institutionalized that allowed the indefinite detention of their members without any criminal act being committed and with limited judicial oversight.

Anticipating that the law would lead to a wave of arrests (the **Federal Bureau of Investigations (FBI)** had compiled a list of 26,000 individuals it considered a threat), Congress earmarked \$775,000 to establish six detention camps in Arizona, Florida, Pennsylvania, Oklahoma, and California. However, although several thousand people were arrested during the 1950s, their numbers never reached the expected level. The 1950 version of the act was actually more restrained than the version initially passed in the House in 1948. This initial version held no provisions for judicial oversight, suspended the writ of habeas corpus, and barred the legal rules of evidence. Furthermore, the 1950 version was passed over the veto of President Truman, who believed the law to be a significant move toward totalitarianism. As a result, an internal security emergency was never declared, and so the provisions that required it were never implemented.

See also: **Counter Intelligence Program (COINTELPRO); Freedom of association; Hoover, J. Edgar; House Un-American Activities Committee (HUAC); McCarthyism**

Suggested Reading: Goldstein, R.J. *Political Repression in Modern America, from 1870 to 1976*. Chicago: University of Illinois Press, 2001.

Brian L. Zirkle

Internet

Commissioned in 1969 by the U.S. Department of Defense as the Advanced Research Projects Agency Network (ARPANET), the Internet was designed to serve as a decentralized military communication system that would continue working even if parts of it suffered a military attack. Technically, therefore, the Internet is a decentralized worldwide system of **computer** networks that allows for the exchange of data among networked computers through a technology called packet switching and through standardized protocols that enable this exchange. Through packet switching, messages (in the form of e-mails, audio,

video, or other file formats) are broken down into small packets of digital information, each with address and reassembly instructions, to be sent via the most efficient routes to their destination, where they are reassembled. By breaking messages down into smaller packets that can travel independently, packet switching technology takes optimal advantage of bandwidth and enables data exchange among millions of networked computers with unprecedented speed, reach, and interactivity.

Because of these qualities, the Internet has in many countries and communities become the primary means by which individuals, communities, governments, civil society organizations, businesses, and other entities communicate and interact. Between the early 1990s, when the Internet first became available for public and commercial use, and 2006, it has grown to encompass almost 1 billion users. These users take advantage of a multitude of communication technologies that constitute the Internet, such as the World Wide Web, **electronic mail**, Instant Messaging, and Usenet groups, to engage in a wide range of activities. All of these online activities involve interactions among individuals, corporations, civil society organizations, businesses, and other entities, during which personal data about individuals can be tracked, collected, archived, shared, copied, manipulated, transferred, or exposed—often without the individual's knowledge. For example, different technologies can track website users' visits, as well as visits to previous and subsequent websites; what they read; how much time they spend on a given article; what they buy, and where and when they buy it; what ads they view and for how long; what personal data, including financial data, they enter into web forms; what software they are using; and what e-mails they read, including when and where (in what city) they read them and to whom they forward them. Online newspapers, for example, have records of the political or other interests of their readers, and online bookstores have records of what books their customers have viewed or purchased (on any topic, including health topics, finances, etc.).

The Internet privacy landscape has become so confusing and increasingly sophisticated that some have decided it is hardly possible to continue to expect any form of data privacy. Others agree that the Internet could indeed become the ultimate data **surveillance** technology, but add that the technology does not itself allow the exploitation of personal data; rather, the Internet technologies as well as the public policies that regulate their design and use reflect the interests of different stakeholders in access to personal information or in its protection. The ways in which these interests are negotiated in the context of the Internet have significant implications for a person's right to self-determination; personal safety (especially for victims of crimes, e.g., of domestic violence); medical and financial privacy; risk of suffering **identity fraud**; opportunities for free political deliberation, dissent, and activism; and access to employment opportunities.

This entry provides an overview of the nature and trends in Internet privacy and focuses on three questions. First, how has the Internet reshaped the privacy landscape; second, how does Internet privacy affect different stakeholders, and what new organizations and entities have emerged to advance the divergent interests of these stakeholders; and third, what main technical tools, concepts, and practices have emerged to track and access or protect personal data?

I. How the Internet Has Reshaped the Privacy Landscape.

The Internet is redefining the privacy landscape through both its technical design and the social uses of this design. First, the Internet allows for massive access to and instantaneous surveillance of millions of messages. It thus allows for new ways of scanning and intercepting large amounts of data or packets as opposed to a simple connection between two points of a traditional phone line or a printed letter.

Second, compared with paper-based data records, privacy on the Internet has changed through the proliferation and transferability of personal data as the technology allows personal data to be processed and manipulated in ways previously unimagined. Data can now easily be shared, copied, searched, mined, compiled, compared, matched, combined, or transferred worldwide at the click of a mouse, leading to a proliferation of personal data and the development of what some privacy researchers have termed a “digital persona”—a collection of an individual’s data available in digital form.

Third, the Internet has changed privacy as a result of the stickiness of digital data. Not only has **personally identifiable information** proliferated on the Internet, but once there, it tends to be difficult to remove. For example, data may reside on servers to which individuals have no access, remain cached (stored for easy retrieval) in search engines, or have been copied and sent on to other sites or discussion forums. Hence, the data remain in the system, creating a permanent searchable record, so that the extent to which individuals can control their data is decidedly reduced.

Fourth, privacy on the Internet is characterized by a lack of transparency in data collection practices. Given the particular interests of businesses in collecting personal data from Internet users for marketing, advertising, and other commercial purposes, as well as the interests of thieves in obtaining personal financial data, technologies designed to collect personal data from Internet users have proliferated; and for the most part, such technologies have been designed to make data collection unnoticeable. Fifth, because of the variety of opportunities for online personal data collection, methods for data compilation, and uses for the data, the Internet raises the stakes of privacy. More data are at stake more frequently for more uses—many of them unauthorized by the individual.

In essence, privacy issues are different for the Internet compared with previous paper-based data storage and communication systems both quantitatively and qualitatively, because personal data proliferate, can be manipulated for an unprecedented array of uses, are more difficult for individuals to control, can be collected more easily without a person’s awareness, and, for all these reasons, entail more severe consequences for individuals.

II. The Stakes in Internet Privacy.

Individuals have a great interest in controlling access to their personal data because their data can be collected without their awareness, can be copied and transferred easily to anyone, and can be mixed and matched with any other data available about them. One of these consequences is identity fraud or theft, a class of crime in which a person’s personal data (e.g., ID numbers, address, or financial information) is used by someone else who assumes the identity of that person in

order to obtain credit or money or to commit a crime in that person's name. For the victims of identity theft, reestablishing their credit record or clearing a criminal record in their name can be both time-consuming and costly. With identity fraud now the fastest-growing crime in many countries, the costs associated with it have skyrocketed to billions of dollars, not to mention the emotional distress victims may experience.

In addition, individuals have a great stake in protecting their personal information from access by governments or other individuals, especially if they are engaged in social, political, or environmental activism and use the Internet to express dissenting views, to organize public deliberations with fellow citizens, or to fight for social justice. Perhaps even more important, citizens who believe that their personal information or whereabouts can be easily tracked and monitored may abstain from expressing dissenting views or engaging in civic activism. As a result, a lack of data privacy may inhibit free speech and open democratic deliberation.

The extent to which personal data about individuals is available can also have important implications for the interaction of individuals with businesses as customers or as employees. As customers, for example, individuals may find that their creditworthiness for important purchases such as homes or cars depends on the amount and type of information a business has about them. Moreover, personal data collected by businesses, such as airlines, are also used increasingly by governments. As employees, individuals may find that their opportunities for employment or promotion increasingly depend on the amount and type of information businesses are able to collect from various sources as well as by monitoring them at work.

To advance the privacy rights of individuals, a number of nonprofit organizations and **privacy advocacy organizations** have emerged that track privacy trends and legislation, educate citizens about privacy, lobby governments, testify in legislative hearings, and contest legislative proposals that may infringe on individual privacy rights.

Conversely, businesses have strong interests in personal data for a number of reasons. On the one hand, the success of Internet commerce depends on the level of control customers have over their personal data. In fact, some studies have shown that customers shy away from Internet commerce or abandon their online shopping carts if they are unsure about their privacy, resulting in billions of dollars of lost business. On the other hand, businesses depend on personal data about customers to rate their creditworthiness, to target marketing and advertising strategies, or—in the case of the software and entertainment industries—to track customer use of software and digital files (e.g., music files, CDs, and DVDs). In addition, businesses also depend on personal data from employees to make hiring and promotion decisions (e.g., by using **credit ratings**, medical data, and criminal records or by monitoring web surfing, e-mail use, keystrokes, or desktops of employees).

This increased interest in and need for personal data on the Internet have given rise to entire industries devoted to the collection, sale, or protection of personal data. For some businesses, collecting or selling personal data has become the main source of revenue. For example, online marketing and advertising businesses collect information about web browsing and purchasing patterns of customers in order

to compile and sell customer profiles and to deliver targeted advertising to these customers. Similarly, large commercial **data brokers** have emerged to collect and combine all available personal data about individuals to provide employment and background checks for businesses, including insurance and marketing companies, as well as for government law enforcement agencies. For these industries, unconstrained access to and use of personal data is an important source of profit. However, as businesses, these data collection entities are not accountable to the public, so individuals do not know what information is being collected about them or how it is being used.

Other industries that have great stakes in accessing people's personal information, specifically in tracking their use of digital files, are the software industry and the content or media industry (e.g., film and music producers and publishers). Because software, music files, movies, books, and other content in digital format can be easily copied and shared, these industries are concerned about copyright infringement and, therefore, have a great interest in tracking how their customers use digital media and content files. To address this need, a technology industry has emerged around digital rights management. Digital rights management (DRM), the controls and constraints copyright holders place on the use of their digital files, has a number of privacy implications. Some DRM systems, for example, require users to identify themselves with a username and password to gain access to files. As a result, the systems are able to track the files that a particular individual watches or reads. Other DRM systems use the default of assigning a randomly generated "Globally Unique Identifier" (GUID) to a computer, which can then be used to keep track of the downloading and playing of media files on that particular computer—a technology that is used, for example, by the Microsoft Media Player software.

However, some DRM software can leave Internet users particularly vulnerable to privacy invasion. The widely publicized case of Sony's digital rights management software on its music CDs demonstrates this well. The company had installed XCP (Extended Copy Protection) software on a number of its recent CDs to prevent its customers from making more than three backup copies of a particular CD. The software installed itself in the operating system of the customer's computer and consistently monitored all processes, putting great stress on the customer's hard drive. Moreover, to hide its existence and its monitoring activities, the XCP software used rootkits, a technology designed to hide files, software codes, and running processes from systems and diagnostic and anti-spyware software. This technology allowed Internet malware, software intended to control or harm a person's computer, to remain hidden from users' view as well, increasing users' vulnerability to such malware. The XCP software also came without uninstall features. Those customers who were able to find the XCP software and tried to uninstall it risked damaging their operating system and CD-ROM drives. When Sony finally supplied an uninstaller, one of its components remained active, which left customers even more vulnerable, allowing any website the customer would visit to potentially take over the customer's computer.

Obviously, businesses have a great stake in access to individuals' personal information and tend to favor policies that allow self-regulation of privacy practices in engaging with customers. Moreover, regulations requiring provisions for customers

to access, correct, or erase their personal information in business databases could be costly. To advance these interests in self-regulation, businesses have formed lobbying associations such as the Privacy Alliance to influence legislators in the United States and Europe. In addition, they have developed voluntary “privacy seal” programs, such as TRUSTe and BBBOnline, to implement self-regulation initiatives. The TRUSTe program, one of the most popular self-regulation initiatives, provides oversight and a resolution process in addition to guidelines for privacy policy development. For example, the program allows users to notify TRUSTe of any apparent misuses of the TRUSTe mark and offers to investigate complaints. Yet TRUSTe is funded by some of the corporations it serves, resulting in a conflict of interest if the program were to investigate one of its sponsors. BBBOnline is another industry-sponsored self-regulation initiative that is similar to TRUSTe but adds the customer recourse options of the Better Business Bureau. In addition, the program features monitoring services, consumer dispute resolution, and a compliance seal. Consequences for noncompliance include seal withdrawal, bad publicity, and referral to government enforcement agencies. However, the program does not provide legal redress mechanisms.

Governments likewise have a great stake in the personal information of individuals. For example, they use this information to fulfill their duties such as providing law enforcement services, regulating traffic, and providing social services, but they can also use them to monitor political activists, dissidents, or government protesters. In addition, governments create legislation to mediate the interests of individuals and businesses in accessing and protecting personal data.

To pursue their missions, governments have used both technologies and public policies to respond to the changing data privacy landscape on the Internet. One of the most famous examples of technology development for access to personal information for law enforcement is the **Carnivore** software developed by the **Federal Bureau of Investigation (FBI)**. Together with other software packages in the FBI’s Dragonware software suite, Carnivore was able to sniff out or identify, reassemble, and analyze data packets from individuals based on certain information (e.g., the individual’s computer Internet Protocol (IP) address or a certain set of keywords) in order to search through the data of suspects. Carnivore has now been replaced with commercially available packet sniffers.

Another well-known technological proposal to provide easy access to the personal data of individuals was the so-called **Clipper chip** proposed by the Clinton administration. This encryption initiative was designed to set a standard for the encoding of voice transmission, and a similar chip called Capstone was envisioned as a standard for the encoding of Internet data. In both cases, the government envisioned holding the keys to the encryption code in order to facilitate access to the encrypted data of individuals once legal authorization had been granted. The initiative was met with protest nationally as well as internationally, and has since been abandoned.

Combined with technological approaches, governments have also developed legislation to regulate the extent and the circumstances under which the personal data of individuals can be accessed by government agencies to pursue their objectives in the changed Internet privacy landscape. For example, the **Electronic Communication Privacy Act of 1986** regulates government access to electronic

communication in transit and in storage, requiring government agencies to obtain warrants or court orders to intercept or access electronic communications of individuals. Other laws have expanded regulations to cover access to personal data in the Internet context as well. To ensure the ability of law enforcement to wiretap phone calls over the Internet, for example, the Federal Communications Commission ordered broadband and Internet telephony (VoIP) providers to make their systems wiretap friendly. In this way, the Commission extended the 1994 **Communications Assistance for Law Enforcement Act (CALEA)** to VoIP as well, although CALEA was originally designed to require public switched telephone network service providers to make technological accommodations to facilitate **wiretapping** by law enforcement.

More recently, the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)** has also expanded law enforcement access to personal Internet data. For example, the act increased the range of data types (e.g., session times and duration) about individuals the government can request from Internet service providers (ISPs). The act also redefines wiretapping to include not only dialed phone numbers but also the addresses of websites and e-mail messages. In addition, the act authorizes roving wiretapping (intercepting and accessing data trails that an individual leaves regardless of his or her location) and requires the cooperation of public organizations such as libraries with such wiretapping. For example, it requires that librarians hand over Internet sign-up records such as URLs and e-mail data, as well as session data such as keywords typed into search engines.

In addition to creating legislation to support their missions in the changed Internet privacy landscape, governments also create legislation to negotiate the interests of all stakeholders. For this purpose, governments have taken different approaches depending on their legal traditions and on the role privacy has played in the legal system. For example, the European Union, which includes personal privacy as a fundamental human right in its Charter of Fundamental Rights of the European Union, has favored a comprehensive approach to electronic data protection. Accordingly, the 1995 **European Data Protection Directive** guarantees the right of individuals to control their personal information.

In the United States, several thousand data privacy laws are proposed every year at the federal and state levels and several hundred are implemented. For example, the **Children's Online Privacy Protection Act of 1998 (COPPA)** applies specifically to children under the age of 13, requiring commercial websites to obtain explicit parental consent before collecting personal information from children. Some legislation is targeted at particular practices or technologies such as restricting the secret installation of unwanted software on a person's computer or requiring businesses to notify individuals if their data have been exposed as a result of a security breach.

III. Technologies and Practices Designed to Capture and Access Internet Users' Information.

When people use the Internet, personal information about them is captured and accessed in a number of ways. First, the general Internet activity of users is logged and captured on their computers, on the websites they visit, and on their ISP's servers. Second, as they use specialized web services, such as search engines, e-commerce

websites, Internet telephone services, or file-sharing services, users leave trails of personal information that can be captured and used for various purposes. Third, Internet users encounter increasingly sophisticated technologies designed for the sole purpose of accessing and monitoring their personal information and Internet activities.

Trails of Personal Data Captured from General Internet Use. When individuals use the Internet, the trails of information they leave are captured not only by their computers, the websites they visit, and their ISPs, but also by website registration protocols in the form of the **WHOIS database**.

Browsers such as Internet Explorer, Netscape, and Mozilla Firefox capture Internet users' web surfing patterns in a number of ways. Browsers capture a history of the sites a user visits, creating a record indicating when each site was visited. In addition, browsers store the addresses of previously visited websites for a set period of time in the drop-down address bar. Moreover, computers store websites and images in a cache, a storage area for copies of Internet files, so that they load faster and do not have to be retrieved again and again. The computer hard drive also stores temporary Internet files, usernames, passwords, and other information. All of this information can be easily accessed by anyone who gains access to the user's computer.

Clickstream data, sometimes called clickpath data, is a logged record of what a person does while visiting a website. A clickstream can contain all the pages users visit, the time users spend on a given page, the date and time of their visit, the order in which they view the pages of a website, the search terms they enter, the site they came from, the site they depart to, the addresses of their received and sent e-mails and user's server address, screen resolution, browser preferences, operating systems, and downloads. Clickstreams can be traced by ISPs and by websites. Often used to determine how effective or attractive particular website features are to visitors, clickstream data are of great interest to marketers and advertisers. An entire industry has sprung up to produce software that analyzes visitor clickstreams and produces live graphic representations of user activities on the website.

Internet service providers are companies that provide individuals, organizations, or businesses with Internet access, including e-mail and web hosting. Accordingly, ISP log files can contain a record of all of this activity of an Internet user (e.g., what e-mails users wrote to whom and when, what websites or files they downloaded and when, which chat rooms they visited, or with whom they engaged in Instant Messaging (IM) conversations). If requested by law enforcement, ISP records in the United States must be stored for up to 90 days according to the Electronic Communication Transactional Records Act of 1996. However, the debate continues over whether ISPs should be required to keep these logs for a certain amount of time and, if so, for how long. Recently, the USA PATRIOT Act has increased the range of data types to be handed over to law enforcement officials.

Internet users who wish to have their own website with their own domain name, such as their family or company name, must request and register the domain name with a Domain Name Registrar, a company that is authorized by ICANN (the Internet Corporation for Assigned Names and Numbers), the nonprofit organization charged by the U.S. government with managing the Internet domain name system and other technical processes. A domain name is an easier-to-remember textual

representation of an Internet Protocol (IP) address, which is a somewhat complicated string of numbers (e.g., 17.254.3.183) assigned to every computer on the Internet as a unique ID—somewhat like a telephone number. The Domain Name Registrar makes sure the domain name is unique and enters it with the matching IP address into a central registry so that other users can find the website or send e-mail to the user.

In addition, current ICANN procedures stipulate that domain name registration requires accurate personal contact information from the website domain owner, which, along with the technical information, is to be entered into a publicly available WHOIS database currently overseen by Network Solutions, Inc. Although originally intended to help network administrators look up technical details and contact information for websites to solve technical problems, the WHOIS database presents privacy problems for website owners because anyone can find out their personal contact information. For example, if a family maintains a website with the photos of children, a pedophile would need only to query the WHOIS database to find out where the family lives. Similarly, if a political dissident group maintains a website, the government could access the WHOIS database to retrieve the contact information concerning the person who registered the site. Public display is the default setting; sometimes, for an additional fee, however, registrars will list alternative proxy contact information to keep the user's personal contact information out of public view. However, there is considerable debate over whether individuals should have the right to register domain names without having their personal contact information publicly available in the WHOIS database. In February 2005 the National Telecommunication and Information Administration, for example, prohibited private registrations for domains employing the .us suffix.

Trails of Personal Data Captured by Using Specialized Internet Services. When using various specialized Internet services such as search engines, online shopping websites, VoIP, or file-sharing networks such as **Peer-to-Peer (P2P) technologies**, individuals leave a trail of personal data that can make them vulnerable to privacy invasions.

Search services can present privacy problems because search terms can be logged together with the computer's IP address in web logs. Moreover, if search engines use **authentication** (i.e., ask users to log in with their username and password), they can create a profile of a user's search history. The most widely used search engine, Google, for example, offers a personalized search service that allows users to log in and keep track of their searches. While the search engine allows users to delete items from their search history, these items are usually erased only from the web, not from Google's internal systems. Like other data, all of the search data can be subpoenaed by governments, as the recent case of the Bush administration's subpoena of search data from Microsoft Network (MSN), Yahoo!, America Online, and Google shows. In an effort to achieve its law enforcement objectives in the area of Internet pornography, the administration requested data about the searches of millions of search engine users.

Moreover, search engines offer a broad array of services that allow them to integrate user information from multiple activities. Google offers a wide range of such converging services, all of which have increasingly complex privacy implications. For instance, in addition to its personalized search service, Google's Gmail e-mail

service allows for unlimited storage of e-mail messages—more data that can be scanned for a profile, which can then be matched with billing information from Google's planned payment services. In addition to the increasing convergence of services (and hence user data) in the hands of one entity, geographic search services of satellite images tied to the **Global Positioning System (GPS)**, such as Google's new Google Earth search, have raised privacy concerns about the ability of such a function to facilitate stalking and tracing an individual's whereabouts, especially once resolution improves.

Similarly, on e-commerce websites such as the online bookstore Amazon.com, users are profiled based on their purchasing habits, product reviews, wish lists, and gift shopping. Recently, the company announced a new profiling technology designed to create databases of gift recipients, guessing their personal information (gender, age, interests, etc.) based on the gifts being sent to them. In this way, the company is creating user profiles even of those who never use the site, but who simply happen to be the recipient of a gift sent by an online shopper. As a result, these individuals may not even know that someone is creating a profile of their personal information, let alone be able to correct the information in the profiling system.

Using microphones and headsets, users can telephone each other directly via their computers, or they can connect from their computers with analog telephone users. Most VoIP systems route phone calls through a central server so that they can be easily tapped or rerouted to law enforcement officers requesting access to them. To ensure the capability of wiretapping VoIP phone calls, the Federal Communications Commission in the United States recently ordered broadband and VoIP providers to accommodate wiretaps.

Peer-to-Peer (P2P) technologies and software such as KaZaA, Gnutella, or Grokster allows computers to both share files from their hard drives and access files on the hard drives of other computers, or peers, in a network using the same P2P software and hence having the same file-sharing capability. In other words, computers with the same P2P software can choose to connect with any other computer in the same network. However, P2P software requires active security management that many users are not aware of. As a result, users may—without their knowledge—be sharing files or allowing others to access their computer functions. In addition, P2P software has often been infected with spyware without any warning notifying users that they are downloading unwanted software along with the P2P software.

P2P networks are also increasingly being used for VoIP services such as the popular Skype program, which also allows for instant messaging (IM), searching, and file sharing. P2P-based VoIP systems allow users to network each other's computers to obtain free VoIP, which raises its own set of privacy issues. Although Skype, unlike regular telephone services or server-based VoIP, is encrypted, it is currently not clear how secure that encryption is. Also, while Skype does not record voice conversations, it keeps histories of IM exchanges, which could be read by spyware programs or other intruders. And although Skype uses P2P networks to transmit phone calls, a central server-based system is used for authentication, so users could easily be tracked by law enforcement officials or by others interested in analyzing network traffic and finding out who is calling whom.

Technologies and Practices Designed to Access Data from Internet Users. In addition to web services capturing and compiling personal information about users, other technologies and practices are designed for the sole purpose of accessing or monitoring Internet users' personal information—usually without their knowledge or consent.

Cookies are small text files of information sent from a web server (a networked computer that stores information that users from other computers can request through their web browsers, e-mail software, and other software programs) to an Internet user's computer while the user is visiting a website. For the most part, these text files contain a unique ID assigned to a user by a website. The ID can be linked to the activities the user engages in while visiting the website, and these activities can then be logged in a database linked to the cookie ID. The cookie file is stored on the user's computer and can be accessed by the server every time the user requests information (e.g., clicks a link on the website). Some cookies are stored permanently on the user's computer (until the user deletes the cookie or it reaches its set expiration date) while others, called session or transient cookies, are set to be erased once the browser is closed. Cookies are usually designed to keep track of what a user does on a website, to store and remember information entered (e.g., a username and password, products purchased, **credit card** information), to customize advertising to user preferences, to keep track of purchases in an online shopping cart, and to monitor how many times an ad has been viewed. Although Internet users can adjust their browser settings to refuse cookies, they would be excluding themselves from most services, since most websites use cookies.

Usually only the website that sent the cookie can read it. However, some websites, especially those of marketing and advertising companies, which provide ad placement services to other websites, place cookies that can be used to track users' activities across many websites. These so-called third-party or tracking cookies usually serve to ensure that ads are targeted at the interests of the website visitor; for example, a user who has clicked on baby toys will likely get ads for other baby products. However, these third-party cookies have also been used to create profiles of user surfing habits and interests. For example, Doubleclick, the most prominent Internet marketing company, can track every website a person visits, every article he or she reads, every purchase he or she makes, and so on. The company could also link an Internet user's entire purchase history and other data to a person's contact information and then sell such a database. This was the plan of Doubleclick when it merged with Abacus, a mail-order management company, in order to create comprehensive customer profiles—a plan it had to abandon after a loud public outcry and a class-action suit.

Web bugs (also called one-pixel gifs, web beacons, tracking bugs, or transparent gifs) are small invisible images—usually only 1×1 pixel and kept in the color of the web page or e-mail background—that are often used in combination with cookies to track who has visited a web page or read an e-mail message (only e-mail messages in html format), how much time they spent on it, and how often they have read the page. They are, for example, frequently used by spammers to determine whether their **spam** e-mail has been read and whether the e-mail address is active. When a website with a web bug is called up or a message with a web bug is read, the browser or the e-mail system automatically requests the web bug image from

the server, thus letting the sender know that the page or e-mail message is being read.

Web bugs have also been used by companies (e.g., Rampellsoft) to develop a service for e-mail users who would like to know, without the addressee's knowledge, whether or not, when, and where their e-mail was read. To spy on the addressee's response to their e-mail, senders add ".didtheyreadit.com" to the recipient's e-mail address to route it through the DidTheyReadIt server, which then attaches a web bug and maintains a connection with the recipient's mail server to track how long the e-mail message remains open on the recipient's server. It can monitor how often the recipients (including those to whom the e-mail was forwarded) open the e-mail, how long they keep it open, and what IP address they are using, which can also be traced to a geographic location such as a city.

Packet sniffers are programs designed to monitor the traffic on a computer network. These programs look at, or sniff, each packet of information on the network and are able to monitor who reads and sends what e-mail to whom with what content, or who downloads what web pages with what content. They can be set to look for specific words or other data or to simply monitor all data flow. They are frequently used to monitor employee communication in the workplace. The best-known packet sniffer is Carnivore (discussed previously).

Spyware is a type of malware—a piece of software (including viruses, worms, etc.) designed to take control of another person's computer, to inflict damage on a person's computer, or to execute other tasks without the consent or awareness of the victim. For example, some types of spyware act as **keystroke loggers** on a user's computer, lock the computer, restart it, read files on the computer, or turn on the computer's microphone and transmit the user's voice over the Internet.

Spyware is designed to observe Internet users' activity without their knowledge and to obtain their personal data. Users usually install the software unknowingly when opening e-mail attachments, sharing files in P2P technologies and networks, or downloading so-called free software such as screen savers, **cellular telephone** ring tones, and browser upgrades from the Internet. They can also become the victim of browser attacks when they accidentally come across the website of a spyware distributor and thereby have the spyware forced on them. They can also contract the spyware from viruses or worms.

Spyware can monitor a user's e-mail, web browsing habits, and keystrokes (and hence record passwords, credit card information, or any other personal data entered into web forms). The software can also reroute payment information to a fraudulent website, tamper with firewalls or anti-virus protection software, serve pop-up ads, redirect dial-up access to an expensive long-distance service, alter home page settings, or change search engine results. These types of software are usually designed for commercial gain in some form—for example, to steal financial and other personal data for identity theft or to collect personally identifiable information about users' shopping habits, preferences, or web browsing patterns for marketing and advertising purposes. In addition, spyware programs take up processing power, slow down the user's computer, and are the primary basis for requests for technical support.

Spyware can be particularly difficult to detect because it is designed to conceal its existence and activities often in the form of rootkits—technologies designed to

hide files, software codes, and running processes from systems and diagnostic and anti-spyware software. At the same time, spyware is designed to make it difficult to uninstall, with such attempts sometimes resulting in damage to the computer system. Given the pernicious and covert nature of spyware, it is perhaps not surprising that, according to a 2004 survey by America Online and the National Cyber-Security Alliance, more than 80 percent of survey respondents were found to have spyware on their computers, with almost 90 percent of these respondents being unaware of it.

Phishing is the crime of sending fraudulent e-mails, presumably in the name of banks or e-commerce websites such as eBay or PayPal, to trick e-mail recipients into entering their personal information (including passwords, user names, address information, and credit card numbers) to a fraudulent website. Both the e-mail and website are usually designed to appear authentic, which makes it difficult for victims to detect the fraud. In addition to using e-mails, phishers attempt to collect personal data on other websites, for example, by fraudulently misrepresenting themselves as potential employers to job seekers on career websites. Phishers either sell the stolen personal data in online markets or use it directly to obtain credit, make purchases, or pursue criminal activities in the victim's name.

Pharming is the deceptive practice of redirecting Internet users to fraudulent websites without their knowledge to trick them into entering their personal information into the fraudulent site. To redirect users without their knowledge, hackers e-mail a virus to victims to alter the Domain Name System (DNS) entries, the list of names that are matched to specific IP addresses (e.g., "apple.com" for "17.254.3.183"), for previously accessed websites stored on the victim's computer. Hackers may also attack the entire DNS server and alter its list of domain names, in which case all users who believe themselves to be going to eBay, for example, actually end up at a fraudulent website.

IV. Technology to Protect User Information or to Make Data Collection More Transparent.

Just as a whole industry has developed to monitor and track people and to collect their personal information, another industry has developed to provide solutions to privacy invasion, so-called privacy-enhancing technologies (PET). For example, in addition to common firewall systems—usually hardware and/or software designed to prevent unauthorized access to a computer—some companies offer anti-spyware programs (e.g., Microsoft Windows Defender), which search the computer for hidden spyware and alert users to unauthorized software downloads. Others offer software to identify web bugs or to manage cookies—so-called cookie busters. Yet others provide services for protecting users' **anonymity** while browsing and e-mailing, or for encryption (e.g., software provided by the company **Pretty Good Privacy (PGP)**, a technology that translates data into an unreadable format using a secret code or format accessible only to the intended recipient).

In addition, the World Wide Web Consortium (W3C), an international nonprofit consortium devoted to the development of technology standards for the World Wide Web, has developed a standard called Platform for Privacy Preferences (P3P) that provides Internet users with more transparency and control regarding the data collection processes of websites. Using P3P-enabled browsers, users can compare their privacy preferences with those of the websites they are visiting and forgo visiting websites whose privacy standards do not meet their expectations. However, P3P does



not enable users to influence the privacy practices of the website for their visit or to access, correct, or erase their data; nor does it provide recourse for users who feel that their privacy has been violated.

As a packet-switching technology that brings together almost a billion people into a shared communication network, the Internet offers new opportunities for interaction, including new opportunities for sharing and accessing personal data in unprecedented numbers and ways. These opportunities redefine the emerging Internet privacy landscape by allowing for massive access to increasingly proliferating and easily transferable data that can be difficult for users to retract and control and that are often collected without their awareness. At the same time, the Internet raises the stakes in data privacy. More data can be collected in more ways for more uses than ever before, affecting individuals' access to employment opportunities, health services, and freedom of political dissent and deliberation, in addition to opportunities for governments and businesses to pursue their missions. It is the negotiation of these stakes through policies and technologies that ultimately shapes the emerging and constantly changing Internet privacy landscape.

Suggested Reading: Agre, Phil, and Marc Rotenberg (eds.). *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT Press, 1998; Federal Trade Commission. *Privacy Initiatives*. <http://www.ftc.gov/privacy>. Online, January 2006; Gellman, Robert. *Privacy, Consumers, and Costs*. <http://www.epic.org/reports/dmf-privacy.html>. Online, January 2006; George, Joey F. (ed.). *Computers in Society: Privacy, Ethics and the Internet*. Upper Saddle River, NJ: Pearson Prentice Hall, 2004; Gurak, Laura. *Cyberliteracy: Navigating the Internet with Awareness*. New Haven, CT: Yale University Press, 2001; Gurak, Laura. *Persuasion and Privacy in Cyberspace: The Online Protests over Lotus Marketplace and the Clipper Chip*. New Haven, CT: Yale University Press, 1997; Internet Education Foundation. <http://www.neted.org>. Online, January 2006; Klang, Mathias, and Andrew Murray. *Human Rights in the Digital Age*. London: Glasshouse Press, 2005; Lessig, Lawrence. "On the Internet and the Benign Invasions of *Nineteen Eighty-Four*." In A. Gleason, J. Goldsmith, and M. Nussbaum (eds.), *On Nineteen Eighty-Four: Orwell and Our Future*, pp.183–212. Princeton, NJ: Princeton University Press, 2005; O'Harrow, Robert. *No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society*. Boston: Free Press, 2005; Pew Internet and American Life Project. *Spyware: The Threat of Unwanted Software Programs Is Changing the Way People Use the Internet*. http://www.pewInternet.org/PPF/r/160/report_display.asp. Online, January 2006; Pew Internet and American Life Project. *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*. www.pewInternet.org/reports/toc.asp?report=19. Online, July 2002; Solove, Daniel J. *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University, 2004; Solove, Daniel J., and Marc Rotenberg. *Information Privacy Law*. New York: Aspen, 2003; World Wide Web Consortium. (2002). *Platform for Privacy Preferences (P3P) Project*. www.w3.org/p3p. Online, August 2002.

Doreen Starke-Meyerring and Laura Gurak

Internet Protocol (IP) address. *See Internet*

J



Journalism

Privacy in the United States means many things, although it was perhaps best summed up by Judge Thomas Cooley as the “**right to be let alone.**” **Privacy torts**—areas of law enabling individuals to sue for monetary damages because of intrusions or communications harmful to privacy—originated in part from perceptions of journalistic misbehavior, making it possible for individuals to sue journalists, advertisers, and others for “invasion of privacy.”

In 1890 two Boston law partners—Samuel D. Warren and future Supreme Court justice Louis D. Brandeis—published the *Harvard Law Review* article “The Right to Privacy.” The article did not advocate a constitutional right, but rather argued that a new, independent legal action for invasion of privacy could be found by taking pieces of existing tort law, including **trespass** to property and defamation. Warren and Brandeis wrote in a famous passage, “The press is overstepping in every direction the obvious bounds of propriety and decency.” They asserted that **gossip** was a trade pursued with “industry as well as effrontery. . . . Modern enterprise and invention have, through invasions upon privacy, subjected . . . [modern man] to mental pain and distress far greater than could be inflicted by mere bodily injury.”

In 1890 a brash invasion of privacy led to a famous early lawsuit. Abigail Roberson sued the Rochester Folding Box Co. for \$15,000 after she found a picture of her face decorating a box of Franklin Mills flour along with the slogan “The Flour of the Family.” New York’s highest court ruled that Roberson could not collect damages because there was no law protecting privacy, adding that the legislature could create one. New York’s legislature responded to the public dismay and to newspaper editorials denouncing the *Roberson* decision by passing a statute in 1903 that made it a tort and a misdemeanor to use someone’s name or likeness without the person’s permission for “trade purposes.” Other states did not wait for legislative action. In 1905 the Georgia Supreme Court ruled in a case involving an unauthorized testimonial in an advertisement for life insurance that there is a legal interest preventing the use of pictures of individuals without their consent.

Privacy in the twentieth and early twenty-first centuries has been a continuing concern and political issue. Since 1905 legal definitions of privacy torts expanded

haphazardly, sometimes by legislative enactment and often by judicial or “common law” adoption of the concept. In 1960 Dean William L. Prosser of the University of California School of Law, America’s foremost torts scholar, wrote a remarkably influential *California Law Review* article, “Privacy,” defining four somewhat overlapping areas of law in a manner readily accepted by both state and federal courts: intrusion, false light, appropriation, and publication of private matters.

Intrusion on a person’s physical solitude includes trespass, eavesdropping, and **wiretapping** or other interception of electronic communication. Prosser included window peeping in his definition, but his view from 1960 could not foresee all of the problems that would come to be associated with the use of increasingly sophisticated electronic devices, including “bazooka microphones,” miniature cameras, **computers, cellular telephones**, and the **Internet**. This Prosser category, by the late twentieth century, had assumed a journalism-specific label, “newsgathering torts.”

The key intrusion precedent involves a *Life* magazine reporter and a photographer who made an unethical deal with authorities to entrap an unlicensed medical practitioner. The *Life* staffers got into the practitioner’s home under false pretenses, with the woman reporter claiming that she had a lump in her breast. The reporter had a transmitter in her purse, which broadcast her conversations with the practitioner, a plumber named A. A. Dietemann, to a nearby automobile, where representatives of the district attorney’s office and of the California State Department of Health listened and made a tape recording. *Life* published an illustrated article, and the information gathered by the reporter and photographer was used to convict Dietemann of the unlicensed practice of medicine. Dietemann then sued the magazine for invasion of privacy.

Life attorneys argued that electronic devices and hidden cameras are indispensable tools of investigative reporting. Writing for the U.S. Court of Appeals, Ninth Circuit, in *Dietemann v. Time, Inc.* (1971), Judge Shirley Hufstедler upheld a small jury award of \$1000 against the magazine for invasion of privacy. The award was small, but the message was clear: “investigative reporting is an ancient art,” existing long before electronic devices and miniature cameras. The First Amendment, Hufstедler declared, provides journalists with no immunity from torts or crimes committed in the gathering of news.

That principle applies to journalists and others who invade privacy by means of old-fashioned eavesdropping, or who use high-tech means to intercept cell phone messages, voicemails, or **electronic mail** messages via the Internet. Photographers and videographers are permitted to capture images in public spaces; they are not permitted, however, to intrude into private spaces or to use sophisticated telephoto lenses or microphones that can pick up conversations at a distance far beyond the range of human hearing. The egregiously aggressive shadowing of celebrities by “**paparazzi**” photographers, even on public thoroughfares, can be banned by judicial order. There are no trustworthy legal defenses if the tort of intrusion occurs. In this and other privacy torts, if a jury is convinced that a plaintiff’s legitimate “expectation of privacy” has been violated, a verdict against the media is likely.

False light (fictionalization) was defined by Prosser as placing someone in a false but not necessarily defamatory light in the public eye. This is the privacy tort closest to defamation of a person’s reputation, and it is the only area of inva-

sion of privacy law where proof of truth is a viable defense. The key precedent here involved a woman, Margaret Mae Cantrell, who was included in a reporter's story even though he had not spoken with her. The reporter gave the impression that he had talked to her about her life six months after her husband had been killed (along with 43 others) when a bridge collapsed. The story for the Cleveland *Plain Dealer* said that the reporter saw the woman "wearing the same mask of non-expression" that she had worn at her husband's funeral. The Supreme Court of the United States agreed that this constituted an actionable knowing and reckless falsehood.

Media employees' deceptiveness with sources is related to the false light tort. For example, the producers of NBC-TV's *Dateline* news magazine convinced a truck driver and his employer that the program was going to focus positive attention on the trucking industry. Instead, the program declared that American highways are a trucker's killing field. A U.S. Court of Appeals allowed the case to go to trial for negligent representation and false light.

The false light tort's similarity to defamation is illustrated by a lawsuit against *Life* magazine by the James J. Hill family. The Hill family had been held hostage for a day by three escaped convicts, who terrorized but did not harm the family. A best-selling novel based on a highly similar situation, *The Desperate Hours*, was made into a play, and a *Life* photo-essay headlined "True Crime Inspires Tense Play" depicted actors from the play in their roles as the son and one of the convicts. The Supreme Court found that individuals who bring false-light lawsuits involving newsworthy accounts must meet the libel standard of proof set in *New York Times v. Sullivan* (1964); that is, the plaintiffs claiming "false light" in a situation of public interest must prove "actual malice"—publication with knowing falsity or with reckless disregard for the truth. As Justice William J. Brennan, Jr., wrote for a divided Court in *Time, Inc. v. Hill*, 385 U.S. 374 (1967), "Material and substantial falsification is the test."

That ruling, however, might not withstand courts' twenty-first-century impatience with broad claims of First Amendment rights for news media. Also, there is concern over the false-light tort because it overlaps reputational interests protected by defamation law. As of 2005 all but 10 states recognized false light. In 1994 a convict's whimsical lawsuit gave the Texas Supreme Court the opportunity to renounce the tort. Clyde Cain sued Hearst Corporation's *Houston Chronicle* for reporting that Cain might have killed eight people. Cain sued because he had killed only three. This led the highest civil court in Texas, by a 5-4 vote in 1994, to abandon the false-light tort because it duplicates the tort of defamation "while lacking many of its procedural limitations."

Celebrities have property rights in their likenesses or images. Successful suits have been brought by baseball players for unauthorized use of their likenesses on baseball "trading cards" or for videotaping, without permission, entertainment performances (including being shot from a cannon, in the case of *Zacchini v. Scripps-Howard Broadcasting* (1977)). Entertainers provide fertile grounds for parodies, but courts have not been uniformly protective of heavy-handed social commentary or humor. A jury awarded \$403,000 to TV celebrity Vanna White of the *Wheel of Fortune* game show, finding that a Samsung Electronics advertisement featured a robot too closely resembling White.

“Sound-alike” ads also cause problems. When entertainer Bette Midler—“the Divine Miss M”—refused to perform a song from her repertoire for a Ford Motor Company advertisement, Ford’s advertising agency (Young & Rubicam) hired a singer to mimic the star’s voice. Ms. Midler won \$400,000.

The general rule in privacy lawsuits, as in libel law, holds that “the dead can’t sue.” However, the estates of deceased celebrities, including Elvis Presley, mystery author Agatha Christie, rock star Janis Joplin, and Rev. Martin Luther King, Jr., have on occasion successfully asserted “descendibility.” That means that a celebrity’s estate can at times control and profit from the commercial exploitation of aspects of the famous dead person’s appearance or performances.

Prosser defined this tort as the revelation of private information violating ordinary decencies, for which truth is no defense for the publisher. Newsworthiness, however, can be a potent defense, as Oliver Sipple learned from his effort to sue the *San Francisco Chronicle*. In 1975 decorated U.S. Marine veteran Sipple became a national hero and made international news while watching a parade featuring President Gerald Ford. When Sarah Jane Moore pointed a pistol at the president, Sipple grabbed her arm, defeating her assassination attempt. A *Chronicle* columnist wrote that San Francisco’s gay community was proud of Sipple’s courage. Sipple argued that publication of his sexual orientation invaded his privacy, suing the *Chronicle* and the Los Angeles *Times* for damages totaling \$15 million. His lawsuit failed when a California appellate court found that Sipple was such a newsworthy subject of public interest that he could not pursue his claim of invasion of privacy.

If private facts about a person become part of an official public document, **disclosure** of those facts will not support a lawsuit against the news media. Even disclosure of a rape victim’s identity—the kind of revelation that reputable media organizations generally avoid on ethical grounds—is not actionable if the information is gained from an official public record, the U.S. Supreme Court held in *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975), a ruling later broadened in *Florida Star v. B. J. F.* (1989). Although private-facts lawsuits are difficult to win against news media, growing judicial impatience with intrusive news media procedures and public concerns over the evaporation of privacy may well make both judges and juries more supportive of privacy lawsuits. In the 1980s, the *Oakland* (California) *Tribune* published a truthful but tasteless gossip column revealing that Toni Diaz, the first woman student body president at the College of Alameda, was born Antonio Diaz and had undergone a sex change operation. After the case languished for years in the California courts, an appellate judge ruled that the question of newsworthiness in this matter should have been submitted to a jury. The newspaper ended the lawsuit with a six-figure out-of-court settlement to Ms. Diaz.

In the search for new weapons to use against the media, “intentional infliction of mental injury,” sometimes styled “negligent infliction,” appeared to be a powerful legal concept in the mid-1980s. The ancient law of libel has developed hard-to-overcome defenses, as have the far newer privacy torts. Larry Flynt’s *Hustler* magazine published a scurrilous parody advertisement, clearly marked “ad parody—not to be taken seriously,” asserting that Rev. Jerry Falwell’s first sexual experience took place in an outhouse with his mother when both were drunk. Falwell sued for intentional infliction of mental injury. He also added the more traditional tort areas of defamation and invasion of privacy to his petition.

The jury in the Falwell case decided that the parody ad was not libelous because no one would believe it. The jury likewise found that the parody was not an invasion of privacy, but concluded that Rev. Falwell should be awarded \$200,000 for intentional infliction of mental injury, an outcome upheld by the Fourth Circuit U.S. Court of Appeals.

The U.S. Supreme Court, however, found that First Amendment values protected even this repugnantly offensive parody advertisement involving a public figure. Writing for a unanimous Court in *Hustler v. Falwell* (1988), Chief Justice William H. Rehnquist concluded that any system of civil damages that might be used to teach Flynt a lesson also would endanger the long American tradition of political cartoons or speech critical of public officials or public figures. This decision discouraged attempts using emotional distress lawsuits against the media to leap over established defenses in libel and privacy law.

See also: Associated Press v. Walker, 388 U.S. 130 (1967); *Bauer v. Kincaid*, 759 F. Supp. 575 (1991); Clinton-Lewinsky scandal; Confessional culture; Confidentiality; Constitutional protections; Freedom of Information Act; Gossip; Public/private dichotomy; Privacy and inequality; Privilege; *Red & Black Publishing Co. v. Board of Regents*, 262 Ga. 848 (1993); Secrecy; *United States v. Caldwell*, 408 U.S. 665 (1972)

Suggested Reading: Folkerts, Jean, and Dwight Teeter. *Voices of a Nation: A History of Mass Media in the United States*. Boston: Allyn & Bacon, 2004; Husselbee, L. Paul. "Respecting Privacy in an Information Society: A Journalist's Dilemma," *Journal of Mass Media Ethics* 9 (1994): 145–156; Kieran, Matthew, David Morrison, and Michael Svennevig. "Privacy, the Public, and Journalism: Towards an Analytic Framework," *Journalism* 1 (2000): 145–169; Lamay, Craig L. (ed.). *Journalism and the Debate over Privacy*. Mahwah, NJ: Lawrence Erlbaum Associates, 2003; O'Harrow, Robert, Jr. "The Press and the Public: At Odds Over Privacy?" *Columbia Journalism Review* 39 (2001): 6–10; Voakes, Paul S. "What Were You Thinking? A Survey of Journalists Who Were Sued for Invasion of Privacy," *Journalism and Mass Communication Quarterly* 75 (1998): 378–393.

Dwight L. Teeter, Jr.

K



***Katz v. United States*, 389 U.S. 347 (1967)**

The 1967 Supreme Court decision in *Katz v. United States* revolutionized the interpretation of the Fourth Amendment regarding the extent to which a constitutional right to privacy applies against government interference. The ruling established a new paradigm for evaluating the balance between searches and privacy by establishing that the Constitution protects people, not places. The decision demonstrated the Court's progress in understanding law and technology, and established a **zone of privacy** even in accessible areas existing within the public realm.

In *Katz*, law enforcement agents obtained evidence of an illicit gambling operation by attaching an electronic listening and recording device to the exterior of a public phone booth used by a bookie. Rejecting previous twentieth-century Fourth Amendment jurisprudence geared toward the protection of property and the rule that a **trespass** to a traditional zone of privacy such as the home or the person was necessary for a violation of the **reasonable expectation of privacy**, the Court took the revolutionary position that a search may occur even in the absence of a physical penetration of a place. Property rights gave way to the expectation of privacy. The determining question was not whether the telephone booth was a constitutionally protected area, but whether Katz, the bookie, acted in a manner exhibiting the desire to maintain the privacy of his conversation. Thus, although the government's activities in *Katz* involved no physical intrusion, they were found to have violated the privacy on which Katz justifiably relied, thereby constituting a search and seizure within the meaning of the Fourth Amendment.

The technologically savvy Court held that the fact that the electronic **wiretapping** device employed to intercept Katz's conversation did not penetrate the wall of the phone booth had no constitutional significance. The existence of a recognizable privacy interest turns on whether a person has a subjectively reasonable expectation of privacy in the place or thing searched or seized, and whether society is willing to recognize it as objectively reasonable. The Court articulated that Katz had such a subjectively reasonable expectation of privacy in the content of his conversation within a public yet temporarily enclosed phone booth, and his expectation was one



that society was prepared to recognize as reasonable. By entering the phone booth and closing the door, Katz sought to exclude his words (not his physical being) from others. These actions allowed him to reasonably presume that the government's conduct in recording his conversation violated his justifiable expectation that the content of his conversation would not be broadcast to the world, even absent physical intrusion into the phone booth. This decision extended the scope of the Fourth Amendment beyond the persons, houses, papers, and effects cataloged therein and guaranteed a previously unrecognized privacy right. **The right to be let alone** by others was officially recognized under the Constitution.

Although the *Katz* decision was a tremendous victory for privacy advocates, its impact is somewhat limited. A person's entitlement to protection is not absolute or unrestricted. Protection requires both an actual, subjective expectation of privacy and an objective, reasonable expectation of privacy that society as a whole would be willing to accept.

The *Katz* holding revolved around the collection of private information without notice through a technological invasion. Thus, its scope is largely limited to content versus non-content material. Non-content materials are not subject to the same extension to the zone of privacy protections. For example, **pen register** devices, which capture addressing materials rather than content, are outside the scope of the Fourth Amendment (*United States v. NY Telephone* (1977)). Monitoring or tracking devices that collect location data also may not be included within the zone of privacy protection. Cell-site data fall between content and non-content material. Privacy advocates consider it content material because it is not specifically included in the provisions listing information accessible by subpoena under the Stored Communications Act (SCA). Law enforcement personnel argue that cell-site information provides merely location or tracking material and therefore is clearly non-content information. Their argument is bolstered by the fact that this information is typically collected by the **cellular telephone** companies for billing and routing purposes. The companies do not collect content information as part of their regular business practice.

Furthermore, the *Katz* decision did not extend Fourth Amendment protection to the government's recovery of private information from third parties (*Couch v. United States* (1973)). The Fourth Amendment has never protected a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it (*Hoffa v. United States* (1966)). The mandate that the Fourth Amendment protects people and not places did not extend coverage to that level. Account information held by banks (*United States v. Miller* (1976)), telephone companies (*Smith v. Maryland* (1979)), and Western Union (*In re Grand Jury Proceedings* (1987)) has been declared unprotected material because the customer voluntarily conveyed the information to a company and "exposed" the information to its equipment in the ordinary course of business. In so doing, the customer assumed the risk that the company would reveal the information to police or others.

Likewise, the *Katz* decision has not extended absolute protection to the collection of private information without notice in public areas where privacy is believed to be protected. The government's intrusion onto an open field (*Oliver v. United States* (1984)) without a warrant is not proscribed by the Fourth Amendment even if the open field is private property (*California v. Ciraolo*, 476 U.S. 207 (1986)). Information that is exposed knowingly in an enclosed backyard to the naked eye

over great distances by aerial **surveillance** is not protected (*Dow Chemical Co. v. United States* (1986)). The rule is that if **curtilage** (the zone of privacy that one expects to be present around a dwelling or industry site) is open to view, police may observe it from a public area. However, if technology is used that discloses intimate associations, objects, or activities, that conduct may constitute a search implicating Fourth Amendment protection.

The issue concerning the use of enhancement technology has been temporarily resolved by the Supreme Court decision in *United States v. Kyllo*, 533 U.S. 27 (2001). In *Kyllo*, the government used a **thermal sensor** or imaging device on a private residence to detect activity and movement via heat patterns to establish probable cause that the home contained a hydroponic marijuana growing operation. Applying the *Katz* two-pronged test, the Court concluded that *Kyllo* did have a subjective expectation of privacy in the heat emissions within his home since the thermal imaging technology had the potential to reveal more than the contraband growing operation. Protected information, such as when the lady of the house was bathing, could also be revealed. Furthermore, the subjective privacy expectation was objectively reasonable and one that society would be willing to recognize. Hence, the interior of house was off limits to any technology, no matter how unobtrusive the technology, provided that the technology was not in general use. This conclusion was reached partly on the basis that the technology of thermal imagers cannot penetrate walls and partly because the devices are not commonly available to the general public. This decision offers minimal and temporary protection to privacy advocates since technology rarely remains static and eventually migrates into the general public domain.

Per the *Katz* decision and its progeny, the element of property rights is but one factor in determining whether expectations of privacy are legitimate. It is more meaningful and appropriate to examine the actual interests involved, an individual's liberty balanced against the government's need for effective law enforcement. The *Katz* decision is an attempt, in a technologically advanced society, to reaffirm the bedrock constitutional provision that searches conducted outside the judicial process, without prior approval by a judge, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.

See also: *Bartnicki v. Vopper*, U.S. 514 (2001); **Constitutional protections**; *Olmstead v. United States*, 277 U.S. 438 (1928)

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Hall, Kermit L. *Conscience, Expression and Privacy: The Supreme Court in American Society*. New York: Garland, 2000; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; Turkington, Richard C., and Anita L. Allen. *Privacy Law: Cases and Materials*. St. Paul, MN: West, 2002.

Jill Joline Myers



Keystroke loggers

A keystroke logger, or key logger, is a small device that monitors each keystroke by a user on a keyboard. The **Federal Bureau of Investigation (FBI)** refers to the device as a “Magic Lantern.” The key logger program records each of the user’s keystrokes and uploads the information over the **Internet** periodically to the person who installed the program. A key logger program can be installed by someone who wants to monitor activity on a particular **computer**, such as by parents who want to monitor their children’s activities on the Internet. It can also be downloaded unwittingly as virus spyware through a remote Trojan horse.

Privacy advocates are primarily concerned about the ease of installation of the device and its capability to circumvent encryption by reading the keystroke logs. The device may be installed by a person opening an **electronic mail** attachment or by landing in the recipient user’s e-mail box. The second major concern relates to its ability to capture content, free of judicial oversight, by recording the secret keys that a person uses to encrypt messages or computer files. The equipment may be installed under the authority of a traditional **search warrant** as opposed to a **wire-tapping** order because the key logger device does not capture or intercept the communication as it is being transmitted over a telephone or cable line while the modem is in operation.

Since the program is practically impossible to detect, there is no way to protect information from being disclosed without authorization and potentially leaked or used in an illicit manner. On the positive side, key loggers are user specific, as opposed to black box programs, which monitor regional communication activities. Furthermore, key loggers reveal a target’s key and key-related information so that access to indecipherable documents can be secured. Timely attainment of information of this sort is crucial to law enforcement in investigating and preventing serious terrorist plots or criminal acts.

See also: **Carnivore; Cryptography**

Suggested Reading: CBS News. *FBI’s Secret Cyber-Monitor*. <http://www.cbsnews.com/stories/2001/11/21/tech/main318869.shtml>. Online, March 2006; Electronic Privacy Information Center. <http://www.epic.org>. Online, March 2006; Nabbali, T., and Mark Perry. “Going for the Throat: Carnivore in an Echelon World. Part 1,” *Computer Law and Security Report* 6 (2003): 456–467; Search Security.com. *Definitions*. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci962518,00.html. Online, March 2006.

Jill Joline Myers

L



Landlord and tenant

In terms of privacy, the relationship between landlord and tenant in the United States is an unbalanced one. In general, laws in all 50 states protect the business interests of the landlord (i.e., the right to find a desirable tenant and to protect his or her property) rather than the right to privacy of the tenant. Renting provides a challenge to privacy, as these owners' right to protect the rental property often requires that tenants give up their **right to be let alone** in their residence or business. Most states provide some protection from unnecessary landlord intrusions; however, in order to rent, tenants give up their privacy to **credit ratings** and reports as well as **background checks**, which often give landlords access to both personal and financial information about prospective tenants.

Tenants are granted several rights that relate to privacy in rental properties. First, landlords do not have the right to **trespass**. Landlords in all states are allowed to enter their properties without their tenants' permission only in case of emergencies that threaten life or property, to make repairs or improvements, and to show property to prospective tenants or buyers. Second, landlords are not allowed to invade tenants' privacy through harassment, **voyeurism**, or **surveillance**. Finally, in all but three states, tenants have the right to the "covenant of enjoyment" requiring landlords to provide a safe and clean living environment.

Some states have taken additional steps to protect tenants' right to privacy by requiring landlords to give prior reasonable notice before entering for non-emergency reasons. Unfortunately, this protection varies considerably from state to state, and over half of all states do not have a statute or do not provide notice guidelines in their statutes. States that do require landlords to give reasonable notice require landlords to give notice 12 to 48 hours prior to entry. Most states also allow courts to decide whether or not landlords gave reasonable notice depending on the circumstances. States do not necessarily require landlords to give written notice and do not always specify the time of day when landlords may enter the property. Delaware specifies that entry must occur between 8 a.m. and 9 p.m., and California requires entry during normal business hours.



Although tenants have the right to disallow their landlords from entering their residences, especially if the latter do not follow state laws, these rights are very limited. All states grant landlords the right to access, especially if they give reasonable prior notice, and grant landlords the right to evict and/or end the tenancy if tenants refuse to let landlords into their residences. Tenants who do not have long-term leases or who do not live in states that require landlords to provide cause for ending tenancy are even more at risk if they do not cooperate with their landlords. Landlords in these cases can terminate residency agreements without cause.

Landlords are not the only individuals who may have a legal right to invade a tenant's residence. Local and state **public health and safety** inspectors may also enter a tenant's residence if they have a warrant or get cooperation from the landlord. Landlords in states with reasonable notice are still required to provide prior notice before letting the inspectors into the residences. Local and state police officials may also appeal to landlords to gain entry into rental units, but must also produce a warrant or show probable cause of criminal activity. Landlords who allow other people in without proper notice or tenant consent are legally liable if there is damage to or loss of property. In general, tenants' rights are better protected when the right of entry and reasonable notice is specified in the lease.

In addition to routine maintenance and inspections, landlords in most states have the right to enter residences if they suspect a resident of unlawful behavior. In particular, landlords are held responsible for protecting their other tenants and their neighborhood from drug dealing or other dangerous activities. Moreover, landlords not only are allowed to violate tenants' privacy if they believe there is drug use or dealing occurring on the premises, but are financially and legally encouraged to do so. Landlords who ignore crime violations face lawsuits from tenants hurt by other tenants; local, state, and federal fines based on nuisance civil laws; criminal charges; and, in some cases, loss of property. For example, laws in Rhode Island and Missouri allow tenants to break their leases if landlords refuse to evict tenants suspected of drug dealing or other illegal activities.

Landlords do not have the right to harass tenants or their employers at work for rent payments or other non-emergency reasons. Fair housing laws also prevent landlords from harassing tenants due to their sex, race, ethnicity, disability, marital status, and religion. Most states give landlords the right to control the number of people living within their rental properties, but some landlords use overzealous measures to enforce those limits, which may be considered invasion of privacy. For example, requiring tenants to register overnight guests can be considered an unreasonable invasion of privacy.

Although most state laws protect tenants' right to privacy from landlords' entry into their residences and business, tenants have little protection from landlords' access to prospective tenants' personal information. Landlords are legally encouraged to obtain information about prospective tenants through proof of identity and work status, rental applications, references, credit reports, background checks, and even casual questions. The amount of information landlords are able to obtain to identify "good tenants" is virtually unlimited, and most laws that protect personal information in both consumer and government databases allow landlords access. The **Fair Credit Reporting Act** and the Accurate Credit Transactions Act of 2003 give landlords legal access to tenants' credit history. Landlords have access to a

tenant's bank account, credit history, rent payment history, student loans, and car loan payments for the past seven years. They also have access to a tenant's conviction and, in some states, arrest history, eviction history, lawsuit participation record, and bankruptcy filings.

In most states, landlords not only have access to this information but may also charge prospective renters' fees to do credit checks. While most states protect tenants from fraudulent credit fees, tenants need to get either written or oral notice of the purpose of the fee and will need to check their credit reports to make sure the landlord did the credit check. Landlords are granted access to such information because it is assumed that credit, criminal, and prior rental relationships will protect landlords from renting to people who are likely to fail to pay rent and who pose a danger to rental properties. Thus, landlords are allowed to refuse to rent to prospective tenants who have bad credit, criminal histories, or inadequate income to afford rent for the property. However, if landlords use information obtained in the credit history to reject prospective tenants, they are legally required to notify them of the reasons and of their right to see their credit reports.

Tenants do not have access to landlords' or managers' credit histories and must rely on their own research to assess the desirability of a landlord. Just as landlords have a financial incentive to check their prospective tenants' backgrounds, a renter has an incentive to check the landlord's background to assess the likelihood that the landlord will mismanage the property or have to sell it. Legally, tenants must assess the ability of landlords to manage their properties based on the physical condition of the facilities and by asking other tenants and neighbors about the landlord or manager.

In addition to credit checks, landlords have the right to do further background checks on prospective tenants, including checks called investigative consumer reports. These checks have become more popular due to the increasing accessibility of individuals' personal information on the **Internet**. Credit bureaus may also interview friends, neighbors, and associates of prospective tenants to gain more information about their character, reputation, and living habits. Some credit-reporting companies now offer checks that reveal tenants' medical histories, including mental institutionalization and current medical conditions; therefore, landlords can select possible tenants on the basis of their health, their sexuality, their personal habits, and other personal characteristics. In addition to criminal records reported by credit reports, landlords may access court records regarding criminal activities committed by prospective tenants, including state and **Federal Bureau of Investigation (FBI)** databases of sexual offenders and child molesters. Although access varies by state, most landlords have access to local registries of **sex offenders** to enable them to protect their rental business.

As with credit checks, landlords can use background checks to screen out what may be deemed as undesirable tenants. However, landlords must universally apply credit and background checks to all tenants or they may face discriminatory charges under fair housing laws. Thus, landlords cannot impose criminal checks based on an applicant's race, gender, or perceived national origin. For instance, landlords cannot ask only Latino applicants about their work status, require only Arab applicants to provide proof of citizenship, or choose only single or younger applicants as subjects for background checks. This protection makes it less likely



that landlords will do deeper background checks since they are unlikely to afford the expense of such checks on all tenants. In addition, landlords must notify the tenant about why they rejected their application if the rejection was based on the background check. Landlords must also file “adverse action reports,” which give reasons for rejecting applications, imposing higher deposits, or requiring cosigners on a lease. These reports are necessary only if the landlord used a credit or tenant screening service. Thus, landlords who use the Internet or do personal checks are not required to disclose why they rejected a prospective tenant.

Unfortunately, despite state laws that protect tenants’ right to privacy, violations are often very difficult to enforce. Tenants without long-term leases or rent control have few protections from landlords if they pursue lawsuits. Tenants are encouraged to document all violations in writing and to write to landlords about complaints before taking legal action. Tenants can sue landlords for trespassing, invasion of privacy, breach of implied covenant of quiet enjoyment, and infliction of emotional distress. Although it is often hard for tenants to win cases, tenants who are able to show repeated trespassing, **sexual harassment**, or other problems with landlords can be successful at winning both civil and criminal cases against landlords. Unfortunately, if a tenant cannot prove a breach of covenant of quiet enjoyment by the landlord, moving, which often carries a financial burden, may be the only real recourse.

See also: **Home**

Suggested Reading: Portman, Janet, and Marcia Stewart. *Every Tenant’s Legal Guide*, 4th ed. New York: NOLO, 2005; Portman, Janet, and Marcia Stewart. *Renter’s Rights: The Basics*, 3rd ed. New York: NOLO, 2002; Stewart, Marcia, Ralph Warner, and Janet Portman. *Every Landlord’s Legal Guide*, 7th ed. New York: NOLO, 2004.

Evelyn A. Clark

Lawrence v. Texas, 539 U.S. 558 (2003)

In *Lawrence v. Texas* (2003), the U.S. Supreme Court made up for its prior—now admitted—mistake in *Bowers v. Hardwick*, **478 U.S. 186 (1986)**, by upholding a challenge to the constitutionality of a Texas **sodomy** statute that made adult consensual same-sex behavior a crime, even when performed in private. This vindication of the “Millian” notion of a self-regarding (i.e., private) act was brought under the Court’s interpretation of the liberty interest protected by the Due Process Clause of the Fourteenth Amendment. The Court’s majority opinion, however, focused only on intimate sexual relations between consenting adults. Thus, it may not be exceptionless. For instance, whether a constitutional challenge to a criminal law prohibiting the private possession of a controlled substance would survive constitutional muster is by no means clear.

Similarly uncertain is how the case might apply in a challenge to criminal laws prohibiting prostitution and the sale of adult pornography. Even with respect to state recognition of same-sex marriage, the majority was careful to state that the present case did not address that issue, which a future case might present, since the issue before the Court was neither the granting of any special recognition nor the establishment of an entitlement. Perhaps more surprisingly, it is not clear how the

Court's decision impacts criminal sodomy proscriptions in the Uniform Code of Military Justice since courts traditionally afford judicial deference to military decisions as falling outside their expertise and involving a separate society composed of non-commissioned and commissioned officers.

Notwithstanding these limitations, however, *Lawrence* is dispositive of the Court's recognition that noncommercial sexual relations among consenting adults in the civilian area can no longer be criminalized under the Court's current interpretation of the Due Process Clause of the Fourteenth Amendment to the U.S. Constitution. Here it is important to take note of Justice Kennedy's majority opinion, which stated, "In all events we think that our laws and traditions in the past half century . . . show an emerging awareness that liberty gives substantive protection to adult persons in deciding how to conduct their private lives in matters pertaining to sex." This recognition that such decisions bear constitutional dignity is the most salient point of the opinion.

The facts in *Lawrence* were almost identical to those in *Bowers*, except the sodomy concerned anal sex, not oral sex, and there was a different legal—though still unrelated to the charge of sodomy—reason for the police entry into the **home**. One very interesting aspect of the case is that it came down just 17 years after a similar Georgia statute was upheld as constitutional in *Bowers*. Kennedy dealt with this issue by showing that *Bowers* was wrong when decided and remains wrong today. This suggests that the Court really had changed its mind on the question of the constitutional protection afforded to adult consensual same-sex intimate relationships. Herein lies dissenting Justice Scalia's concern that *Lawrence* may open the door to eventual constitutional recognition of same-sex marriage. The change in description is important also because the move from act to relationship suggests a much more powerful grant of normative recognition to the parties' own self-identification. This is evident in Kennedy's observation that "[t]he case does involve two adults who, with full and mutual consent from each other, engaged in sexual practices common to a homosexual lifestyle. The petitioners are entitled to respect for their private lives." Another important difference between the two cases is that in *Lawrence*, the Court seemed willing to pay more attention to extralegal and nonlegal sources than had been done by the *Bowers* Court, suggesting that for only the second time in recent history a new body of outside source material was being brought into the area of U.S. constitutional interpretation. This widening of the range of sources the Court would consider brought a strong rebuff from Scalia and a nonbinding resolution in the House of Representatives against such further outreach. It has also become the subject of a question asked by Senate Judiciary Committee members of nominees to the Court.

In *Lawrence*, the Court explicitly overruled *Bowers*. Writing for the majority, Kennedy grounded his opinion in several earlier cases, including *Griswold v. Connecticut*, 381 U.S. 479 (1965), and *Roe v. Wade*, 410 U.S. 113 (1973), all of which were privacy cases in the Millian sense and all of which had been available to the *Bowers* Court, but which were distinguished there on the narrow reading that they concerned marriage or procreation. Kennedy's majority opinion read those earlier cases more broadly to recognize a fundamental liberty interest in intimate relationships protected by the Due Process Clause. Kennedy's majority opinion in effect displaced what dissenting Scalia noted was the previous view of the Court (and, no



doubt, was still the view held by himself, Chief Justice Rehnquist, and probably Justice Thomas), that a particular practice traditionally viewed as immoral could be “a sufficient reason for upholding a law prohibiting the practice.” To the contrary, Kennedy’s broader due process interpretation would seem to suggest that, absent a showing of real harm, moral opinion couldn’t be a determinative criterion.

Kennedy’s interpretation of the Due Process Clause in *Lawrence* would have been out of step with current law, however, if *Bowers* were still to be considered good law. As *Lawrence* and *Bowers* are not logically reconcilable, *Bowers*’ status as controlling law had to be overcome. Justice Stevens’s dissent in *Bowers* showing in what way the majority had gone wrong would now become the controlling law. It was necessary for the Court to find *Bowers* to be wrongly decided because, under a certain version of legal realism (under which American law is sometimes seen to operate), once *Bowers* was decided it became part of the very law that Kennedy had to interpret. Indeed, even from the position of a natural law theorist, Kennedy’s decision would be problematic if *Bowers* were deemed morally correct.

As a ground for overturning *Bowers*, Kennedy showed that the suppositions determining that decision—views of Western civilization toward homosexuality—were incorrect and inadequate ways of explaining both the law that preceded it and the law ensuing from it. First, Kennedy examined the history and weak enforcement of sodomy statutes that preceded *Bowers*. Second, he noted that the prior development of the Model Penal Code—put forward by legal scholars of the American Law Institute and adopted in some variation by the legislatures of a number of states—disavowed making private, consensual, adult sexual activity criminal. Third, the post-*Bowers* case of *Planned Parenthood of Southeastern Pennsylvania v. Casey*, 505 U.S. 833 (1992), re-affirmed *Roe v. Wade* and thus continued the recognition that the Due Process Clause protected deep-seated values in personal autonomy and human dignity. Finally, Kennedy focused on various recent international human rights documents and decisions affirming privacy and equality rights for gays and lesbians.

What is striking is that Kennedy’s opinion in *Lawrence* is difficult to fit into a standard positivist model of law, like that of English philosopher H. L. A. Hart. This difficulty exists because Hart not only treats positivism as separating law from morality and providing an analytical analysis of concepts, but also treats it as establishing formal criteria for determining what the law is. In other words, if a statute or case decision has the correct pedigree, it is the law regardless of whether we like its content. Kennedy’s view is arguably, however, more consistent with that of American philosopher Ronald Dworkin because Kennedy attempts to balance previously established principles against those raised in *Bowers*. However, the Dworkin model cannot easily explain why the weight of relevant principles may now have shifted. Internal principles, including those directing courts to take account of society’s changing views, are themselves relative to such change. What Kennedy did not do was articulate a clear way of answering these questions within the American constitutional framework. While Kennedy’s decision may appear intuitively correct, the task of formulating such an articulation of how to answer these questions within the American constitutional framework is still incomplete. In part, this may be because such changes in a principle’s weight reflect society’s changing idea of the classes to whom these principles applied. Still, connecting that change to law in a way that is not ad hoc requires some deeper view of rationality that must

underlie both law and morality. Neither Kennedy's opinion, nor any of the other concurring or dissenting opinions, addressed that deeper view.

See also: **Constitutional protections; Family; Privacy, philosophical foundations of**

Suggested Reading: Mill, John Stuart. *On Liberty*. London: Longman, Roberts & Green, 1869. www.bartleby.com/130/. Online, March 2006; Prosser, William L. "Privacy," *California Law Review* 48 (1960); "The Right to Privacy in Nineteenth Century America," *Harvard Law Review* 94 (1981), 1892–1910; Samar, Vincent J. "Gay Rights as a Particular Instantiation of Human Rights," *Albany Law Review* 64 (2001); Samar, Vincent J. *The Right to Privacy: Gays, Lesbians and the Constitution*. Philadelphia: Temple University Press, 1991.

Vincent J. Samar

Library records

The privacy and **confidentiality** of library patrons' use of library services and materials are protected both by statute in many national, state, and provincial jurisdictions and by the policies and ethical codes of many libraries and professional library associations. The American Library Association (ALA) defines privacy as "the right to open inquiry without having the subject of one's interest examined or scrutinized by others" and confidentiality as the condition that exists "when a library is in possession of **personally identifiable information** about users and keeps that information private on their behalf."

Protection of patron privacy was a core value of library practice in many countries long before digital technology was introduced and used to automate such library operations as maintaining circulation records. As in other sectors of society, however, the importance of privacy and confidentiality in library use has grown as information technology has both automated traditional functions and—via networking—become the primary vehicle for delivering library catalogs, indexes, journals, and reference services. For library users in many parts of the world, most interactions with a library are now mediated through technology capable of tracking and storing their questions, searches, and reading choices. In the United States, in particular, the terrorist attacks on September 11, 2001, and the legislative responses—especially the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)**—have raised important questions about the relationship between privacy rights and national security.

In the United States, state and federal laws have provided, directly and indirectly, some protections for the records of library patrons. Whether or not a library is publicly funded (by state or local governments) will typically determine how and to what degree it must offer its users legal protections for their data privacy. Public libraries and state-funded institutions such as university libraries generally fall under this protection, while private libraries owned and run by nonprofit organizations or commercial entities may not.

Federal law does not specifically protect or define the privacy rights of users of libraries. Broadly stated protections of the rights of the citizenry to their personal privacy can be understood to also cover library users' information to some degree.



The U.S. Constitution provides a framework for the development of laws that protect citizens' privacy without specifically mentioning privacy. The Fourth Amendment's "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" is a good example. Court cases have interpreted the wording of the Constitution to grant protections to its citizens in a variety of ways, as have new laws enacted to define those rights. An example of such a law is the **Privacy Act of 1974**, which helped develop the concept of **fair information practices** for the handling of personal information by the federal government.

State statutes, by contrast, typically provide some specific protections against the **disclosure** of records maintained or collected by publicly funded libraries. Under California state law, for example, personal information maintained by libraries is kept confidential, as are circulation records that include any information that would "identify patrons borrowing particular books and other material." A New York state statute defines more broadly and directly the kind of patron records and personal information that is protected and kept confidential, from circulation records to database searches and interlibrary loan requests, except as required for the running of the library, by proper permission of the library user, or by court order. The state of Texas exempts library records from its Open Government/Ethics statutes.

State statutes generally allow for disclosure of patron information under specific circumstances—for example, to library personnel for the running of the library, to the user or a designated proxy, or to legal entities when required by court order or subpoena. Overall, however, state statutes offer a degree of protection to the data generated by library users in their interactions with library resources and services. These data include personal status information like date of birth, address, and telephone number. Other protected data include information about whether the patron has checked out materials or viewed websites and the kind of assistance the patron has requested from library staff or automated services.

The passage of the USA PATRIOT Act amended over 100 sections of 15 federal statutes and lowered the bar for access to otherwise protected information of library users. These alterations now give federal agents access to "any tangible things (including books, records, papers, documents, and other items)" even if the person being investigated is merely a "suspect in a current investigation." The act also prohibits the disclosure of the federal request for the records or tangible items.

The codes of many national and international library associations tie privacy rights to intellectual freedom as core values of the library profession. In its Statement on Libraries and Intellectual Freedom, the International Federation of Library Associations and Institutions (IFLA) states that library users "shall have the right to personal privacy and anonymity. Librarians and other library staff shall not disclose the identity of users or the materials they use to a third party." Similarly, the American Library Association states that privacy "is essential to the exercise of free speech, free thought, and free association" and that "rights of privacy are necessary for intellectual freedom and are fundamental to the ethics and practice of librarianship" ("Privacy: An Interpretation of the Library Bill of Rights"). Its Code of Ethics declares that librarians must "protect each library user's right to privacy and confidentiality with respect to information sought or received and resources

consulted, borrowed, acquired, or transmitted.” Without assurance of privacy, the ALA argues, library users may be inhibited in their intellectual inquiries: questions posed at a reference desk; books requested, borrowed, or read; or **Internet** searches performed.

Furthermore, according to the ALA, patrons “have the right to use a library without any abridgement of privacy that may result from equating the subject of their inquiry with behavior.” Automated methods of information tracking make it possible to develop detailed intellectual profiles from the inquiries of individual patrons, and patrons who are aware of this possibility may be deterred in their inquiries. Moreover, these profiles can easily be misinterpreted, leading to erroneous conclusions regarding an individual’s purposes or intentions in making an inquiry. Library privacy policies therefore typically focus on safeguarding personally identifiable information rather than minimizing physical **surveillance**.

As noted above, the USA PATRIOT Act requires libraries to produce any tangible items upon demand by a law enforcement agent. Insofar as these items may bear personally identifiable information, the act conflicts with the ALA’s traditional position on patron privacy and confidentiality. In response, the ALA developed a privacy toolkit to help libraries understand, develop, and implement local privacy protection policies. In this toolkit, the ALA urges libraries to ensure that their policies limit the degree to which personally identifiable information is monitored, collected, disclosed, and distributed; avoid creating unnecessary records; discard records once they are no longer needed for efficient operation of the library; and avoid practices that place personally identifiable information in public view.

Increasingly, the information resources provided by libraries to their users—including electronic journals, citation databases, and online reference software (sometimes called “chat”)—are hosted not on the library’s own **computer** servers but on computers owned by the publisher or vendor. This may result in information being collected about library patrons without their knowledge and outside the control of the library that pays for the services. A statement by the International Coalition of Library Consortia (ICOLC) calls upon vendors of such electronic services not to disclose “information about any individual user of its products. . . , including information about the specific content of a user’s searches, to a third party without the permission of that individual user, except as required by law” (2002). At the same time, various library associations encourage individual libraries to ensure that their subscription contracts (licenses) include guarantees that vendors will maintain the confidentiality of usage data, including information relating to the identity of specific users and uses.

See also: **Public records**

Suggested Reading: Adams, Helen R., Robert F. Bocher, Carol A. Gordon, and Elizabeth Barry-Kessler. *Privacy in the 21st Century: Issues for Public, School, and Academic Libraries*. Westport, CT: Libraries Unlimited, 2005; American Library Association. *California Government Code*, §§6254 and 6267. <http://www.ala.org/ala/oif/ifgroups/stateifcchairs/stateifcinaction/californiaprivacy.rtf>. Online, March 2006; American Library Association. *Code of Ethics*. <http://www.ala.org/ala/oif/statementspols/codeofethics/codeethics.htm>. Online, March 2006; American Library Association. *New York Consolidated Laws Civil Practice Law and Rules*, §4509. <http://www.ala.org/ala/oif/ifgroups/stateifcchairs/stateifcinaction/newyorkprivacy.rtf>.



Online, March 2006; American Library Association. "Privacy: An Interpretation of the Library Bill of Rights." <http://www.ala.org/ala/oif/statementspols/statementsif/interpretations/Default675.htm>. Online, March 2006; International Coalition of Library Consortia. *Privacy Guidelines for Electronic Resources Vendors*. <http://www.library.yale.edu/consortia/2002privacyguidelines.html>. Online, March 2006.

Ada Emmett
Richard Fyffe

***Loving v. Virginia*, 388 U.S. 1 (1967)**

The private right to marry whom one chooses has been at the heart of due process judicial cases since the early 1960s. Laws that generally limit one's choice in marriage or that tend to restrict the rights of a class of persons to marry will not be upheld unless the state can show a compelling interest in the restriction or in maintaining the classification. *Loving v. Virginia* represents an early Supreme Court case that established the fundamental constitutional right to marriage and the notion that laws restricting this right should be subject to the strictest of scrutiny under the Due Process and Equal Protection clauses of the Fourteenth Amendment of the U.S. Constitution. The Supreme Court unanimously decided *Loving v. Virginia*, and Chief Justice Earl Warren delivered the opinion.

The decision in *Loving v. Virginia* concerned the legality of anti-miscegenation statutes, which were laws that banned the mixing of different ethnicities, especially in marriage. The Supreme Court declared the Virginia statutes unconstitutional and thus ended all race-based legal restrictions on marriage in the United States. At the time *Loving v. Virginia* was decided, Virginia was one of 16 states that prohibited and punished marriages on the basis of racial classifications.

In June 1958, Mildred Jeter, an African American woman, and Richard Loving, a white man, were married in the District of Columbia. Both were residents of Virginia but were forced to legalize their marriage in another state due to Virginia's anti-miscegenation statutes. The laws at issue in this case absolutely prohibited a white person from marrying any person of another race or ethnicity. After their marriage in the District of Columbia, the Lovings returned to Virginia and resided in Caroline County. In October 1958, the Circuit Court of Caroline County charged the Lovings with violating Virginia's ban on interracial marriage. They pleaded guilty to the charge and initially were sentenced to one year in jail. The trial court of Caroline County, however, suspended the Lovings' one-year jail sentence on the condition that the couple leave Virginia and not return for a period of 25 years.

To challenge the trial court's sentence in Virginia, the Lovings filed a motion in the state trial court on November 6, 1963, requesting that the judgment be set aside on the grounds that the laws in Virginia banning interracial marriage violated the Fourteenth Amendment of the U.S. Constitution. This amendment provides for equal protection of the laws and that no state shall deprive any person of life, liberty, or property without due process. The Lovings' motion to dismiss the judgment was denied by the state trial judge and was later affirmed by the Virginia Supreme Court of Appeals. The Lovings' case was appealed to the U.S. Supreme Court in April 1967.

The Supreme Court decision in *Loving v. Virginia* was significant because it established marriage as a fundamental constitutional right of privacy for all citizens that could not be restricted by laws that denied the right based solely on racial classifications. Laws that use only race to determine the validity of marriage violate the Equal Protection Clause and also deny citizens of due process by depriving the individual of the freedom of choice of whom to marry.

Concerning the Equal Protection Clause of the Fourteenth Amendment, there were two Virginia state statutes under which the Lovings were convicted and sentenced that the U.S. Supreme Court overturned. These statutes were part of a comprehensive body of law aimed at prohibiting and punishing interracial marriages. The first statute provided that if any white person and “colored” person left the state of Virginia for the purpose of being married and with the intention of returning to cohabit as man and wife, they shall be punished under the laws of the state. The second statute punished both parties of an interracial marriage with a felony conviction and confinement in the penitentiary for a period of one to five years. These and other parts of Virginia’s statutory scheme making interracial marriage illegal originated from the Racial Integrity Act of 1924.

With respect to marriage, privacy, and the Fourteenth Amendment’s guarantee of equal protection, the state of Virginia first argued for the validity of state statutes based on classifications deemed appropriate by state legislatures to regulate the private choice of marriage. The court decisions in Virginia that found the Lovings’ marriage illegal held that since marriage was traditionally subject to state regulation without federal intervention, the regulation of marriage should be left to exclusive state control under the Tenth Amendment of the U.S. Constitution. Furthermore, the state of Virginia argued that the Equal Protection Clause of the Fourteenth Amendment means only that state penal laws dealing with interracial elements must apply equally to members of each race. The miscegenation statutes at issue, according to the state of Virginia, punished both parties to the interracial marriage equally and to the same degree.

In a unanimous decision, the Supreme Court reversed the lower court’s decision and held that statutes banning interracial marriage violated the Equal Protection Clause of the Fourteenth Amendment and thus were unconstitutional. According to the Supreme Court, state powers to regulate marriage are not unlimited and that the mere equal application of a statute containing racial classifications does not remove the statute’s legality from the commands of the U.S. Constitution. The purpose of the Fourteenth Amendment was to remove “invidious racial classifications” from all forms of law. Whether the statutes punished both races equally was irrelevant since the restriction served no compelling state interest other than racial discrimination. Citizens are entitled to make the private choice of whom to marry free from arbitrary state regulation. In contrast, where discrimination is not based on racial classifications, the courts will tend to ask whether there is any rational foundation for discrimination and often will defer to the wisdom of state legislatures.

The opinion delivered by Chief Justice Warren was significant for issues of privacy and marriage because in cases following *Loving v. Virginia* any law that attempts to draw distinctions according to race would be subject to the most rigid scrutiny to determine constitutionality. The type of scrutiny to be applied to statutes restricting fundamental rights based solely on race had important implications for



how the court system in the United States would decide issues relating to privacy following the opinion. There was no doubt that Virginia's law banning interracial marriage rested exclusively upon distinctions based on racial classifications. Since these types of statutes must pass the most rigid scrutiny in order to be found constitutional, it must be shown that the laws in question are necessary to the accomplishment of some state objective that is independent of racial discrimination. While the state of Virginia attempted to argue that the scientific evidence concerning interracial marriage was substantially in doubt, the Supreme Court found that there was no legitimate overriding purpose to the anti-miscegenation statutes independent of "invidious racial discrimination" that could justify the classification. The clear and central purpose of the Fourteenth Amendment, according to Chief Justice Warren, was to eliminate all official state sources of racial discrimination in the U.S. legal system, and this was assuredly necessary in laws that attempted to regulate the most private choices of citizens.

Concerning how the statutes deprived the Lovings of liberty without due process of law, the Supreme Court explained that the freedom to marry is a vital personal right that is "essential to the orderly pursuit of happiness" by all citizens. To deny this important private right based on unsupportable racial classifications was directly subversive of the principles of equality guaranteed in the Fourteenth Amendment. Following *Loving v. Virginia*, there was no doubt that decisions about whether or not to marry, and whom to marry, were, at least for heterosexuals, personal and private rights residing solely with individuals, and could not be restricted by any law or regulation.

See also: **Constitutional protections; Family; Privacy and inequality**

Suggested Reading: Alonso, Karen. *Loving v. Virginia: Interracial Marriages (Landmark Supreme Court Cases)*. Berkeley Heights, NJ: Enslow, 2000; Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Hall, Kermit L. *Conscience, Expression and Privacy: The Supreme Court in American Society*. New York: Garland, 2000; Moran, Rachel. *Interracial Intimacy: The Regulation of Race and Romance*. Chicago: University of Chicago Press, 2003; Newbeck, Phyl. *Virginia Hasn't Always Been for Lovers: Interracial Marriage Bans and the Case of Richard and Mildred Loving*. Carbondale: Southern Illinois University Press, 2004; Smith, Robert Ellis. *Compilation of State and Federal Privacy Laws*. Providence, RI: Privacy Journal, 1992; Turkington, Richard C., and Anita L. Allen. *Privacy Law: Cases and Materials*. St. Paul, MN: West, 2002.

Ann Marie Neir

M



Manners

Manners refer to the quality of a person's conduct and comportment, particularly toward others. Manners express degrees of politeness, regard, and respect toward others. Manners are also believed to indicate something about the character of the person who exhibits them. Manners are moral matters; people are obliged to observe how they treat others, and in return, they are judged by their mannerly conduct. Manners are learned through socialization and are typically governed and sanctioned informally through interactions in everyday life.

Common sense suggests that manners are internalized, deep-seated, and ingrained in people's character. Thus, people have good or bad manners. An individual who displays good manners minimally demonstrates basic regard and courtesy toward others, if not deference and respect. Having no or bad manners may be indicated by the absence of behaviors that display positive regard or respect, as well as by conduct toward others that is perceived as impolite, disagreeable, or rude. While manners primarily characterize a person's actions toward others, they are also interpreted as reflecting the character of the individual displaying them. In everyday usage, having good manners may indicate that an individual is refined, urbane, or privileged; whereas having no or bad manners may indicate that one is common, coarse, or of a lower social class.

However, it may not be that simple. Sociologists such as Erving Goffman suggest that individuals deliberately manipulate their conduct, including their manners, to enhance their self-image and status by gaining others' approval. Everyday life is replete with such performances of the self. In both the commonsense and sociological views, manners may be more about the self than the other; through a person's actions toward others, the individual displays the self.

What is considered good or bad manners is to a great extent culturally and historically variable and relative; this does not negate the principle that being polite and respectful of others is a basic expectation of ordinary social life in most times and places. Common courtesies such as saying "thank you" for services rendered, waiting one's turn in line, or apologizing for negligible slights toward others are

widespread. Everyday courtesies usually require people to pay attention to the feelings of others, acknowledging and displaying regard for them when in their presence. However, these daily courtesies also include practicing “civil inattention,” ignoring and disregarding others engaged in private behaviors in publicly shared settings, as well as displaying tact—disregarding minor, accidental behavioral transgressions of others to spare them embarrassment. Thus, there are times when people should pay attention to others and times when they should purposefully not pay attention to others. For instance, while it is considered polite to greet one another, it is considered impolite to eavesdrop on someone’s conversation, to glance at someone using a urinal in a public **restroom**, to stand too close to someone making a financial transaction at an **automatic teller machine (ATM)**, or to draw public attention to the presence of food in someone’s teeth.

In showing respect toward others, maintaining the proper equilibrium between attention and inattention highlights another tension—social proximity; manners oblige us to distinguish and maintain the distinction between private and public spheres. While good manners might encourage inquiring about the well-being of another, such as by asking, “How are you?”, they also discourage inquiring too deeply or engaging in **gossip** about others, as well as imposing one’s own private matters on others. Good manners also prescribe a degree of spatial distance. Taking the seat right next to the lone person on a bus is likely to be perceived as an invasion of personal space. Being courteous to others requires negotiating a delicate balance between public and private spheres and interest and disinterest, as well as honoring an appropriate degree of social and spatial proximity.

Exhibiting good manners purportedly functions to harmonize social interaction and to facilitate civility in shared public space. Learning manners also purportedly helps individuals draw boundaries between acceptable public and private conduct. Recent technological advances have blurred this boundary and have created the potential for new forms of discourtesy. Impolite or uncivil conduct in impersonal forums such as **Internet** communications has given rise to “netiquette.” Similarly, conversing on the telephone, once confined to the private sphere, now is often quite public. The widespread ownership of **cellular telephones** enables users to carry on private conversations in public. While infractions of what is considered polite behavior are typically informally sanctioned, the incessant ringing of cell phones in public places such as restaurants, libraries, theaters, museums, and classrooms has become such a nuisance that many such public places have established formal policies governing their use. In addition, the inappropriate use of cell phones is regarded by some as a public menace. The potentially danger of using cell phones while driving has led to laws proscribing their use in **automobiles**. Also, for the first time, in 2005 the Sprint Corporation sponsored the declaration of July as “National Cell Phone Courtesy Month.”

Increasing stress associated with a fast pace of life, combined with congested public space, is credited with producing new forms of ill-mannered conduct, escalating formerly ordinary foul gestures while driving to the status of “road rage.” These social conditions and others, such as changing **gender** and sexual norms, have also led to ambiguity regarding what bodily parts can be properly exposed in public. Attempts to formally regulate the increasing exposure of the body, including **private parts**, in public have failed more often than they have succeeded.

Though still a highly contentious issue, it is no longer unusual for women to breastfeed their children in public. Most states in the United States now have breastfeeding laws that both permit and circumscribe breastfeeding in public places. Some states, such as Illinois, permit women to breastfeed at any public or private location; others, such as Virginia, allow breastfeeding in public places only on state-controlled property, permitting private property owners to establish their own policies. In 2005 the Virginia General Assembly made international news for considering a bill to criminalize “droopy drawers,” the trend among youth of wearing pants or skirts so low that underwear hangs visibly over the top. Changing norms governing the body and sexuality have also given rise to new terms for behavior once considered appropriate only in private, such as “public displays of affection.”

Changing norms of privacy have challenged previously held standards of politeness and courtesy in the other direction as well. During the colonial period in the United States, prospective married couples were expected to post a “bann” in the public square announcing their engagement and inviting public comment and objections from members of the community. Today, publicly voicing an objection to a couple’s engagement would be considered not only impoliteness but interference. Today, the public vows of marriage are deemed private matters.

Manners ostensibly function to show respect for others to enable people to peacefully coexist, to be civilized. Civility obliges people to exercise self restraint, as suggested by the phrase that a person can “disagree but not be disagreeable.” Critics have protested that manners have been invoked to maintain a “negative peace,” to minimize open conflict or quash disagreement or dissent, and to deny individual expression. In the name of manners, people may be expected not to disagree, however agreeably, because disagreement itself might “cause a scene,” or to accept practices that serve as a pretense for maintaining hierarchical social roles and class distinctions or that justify social inequality. The expectation that men should open doors for women and that black men should avoid direct eye contact with white women have been framed as chivalrous, cast in protectionist terms for all parties, and contested as sexist and racist.

Finally, the business of manners is big business. From advice columns to magazines, books, and institutes, specialists in the art of manners are devoted to civilizing people, helping them avoid faux pas, and cultivating habits that bestow an air of confidence, grace, and success in every social and professional occasion. The ephemeral boundary between public and private guarantees that minding one’s manners will remain an elusive pursuit.

See also: **Confidentiality; Public/private dichotomy; Secrecy**

Suggested Reading: Carter, Stephen L. *Civility: Manners, Morals, and the Etiquette of Democracy*. New York: Basic Books, 1998; Cott, Nancy F. *Public Vows: A History of Marriage and the Nation*. Cambridge, MA: Harvard University Press, 2002; Goffman, Erving. *Behavior in Public Places: Notes on the Social Organization of Gatherings*. New York: Free Press, 1963; Sumner, William Graham. *Folkways: A Study of the Sociological Importance of Usages, Manners, Customs, Mores, and Morals*. New York: Dover, 1906.

Christine M. Robinson



McCarthyism

The term “McCarthyism” was first used in a cartoon by Herbert Bloom published on March 29, 1950, in the *Washington Post*. It initially referred to an extreme form of conservative anti-Communism, associated with Senator Joseph McCarthy, aimed at identifying and eliminating domestic Communist threats to the U.S. government. This anti-Communist agenda was often pursued at the expense of basic civil liberties such as **freedom of association** and the right to privacy. McCarthyism is also used to refer to a more general cultural and political milieu in which concerns about national security and the threat of Communism took precedence over the protection of civil liberties and personal privacy. Generally associated with the Red Scare of the 1940s and 1950s, the term is still sometimes used pejoratively by political dissenters who believe government policies are encroaching on the basic rights of citizens.

McCarthyism, narrowly defined, began in 1950 when Senator McCarthy gave a speech in Wheeling, West Virginia, proclaiming that he had a list of known Communist loyalists who worked in the State Department. As a broader cultural and political phenomenon, it can be traced back to the 1930s. During this period a fundamental shift occurred in which liberal anti-Communism was abandoned in favor of a conservative anti-Communist agenda. The initial response by the U.S. government to the growth of American Communism was to undermine the Communist Party by integrating several of its key issues into government policy. By increasing the federal government’s involvement in dealing with poverty, unemployment, and social inequality, liberal anti-Communists hoped to make Communism a less appealing alternative. However, by the late 1930s, conservative anti-Communists had gained significant influence in both the Democratic and Republican parties and introduced a number of strategies aimed at eliminating Communist threats through coercion rather than appeasement.

The formation of the **House Un-American Activities Committee (HUAC)** in 1938 marked the arrival of conservative anti-Communism on the national political scene. HUAC played a central role in redefining domestic Communism from a matter of political opinion to one of national security, setting the stage for McCarthy’s rise to prominence. HUAC was the driving force behind the Alien and Registration Act of 1940, which criminalized the advocacy of revolutionary political ideologies and association with organizations that engaged in such advocacy. Furthermore, HUAC initiated a series of highly publicized hearings aimed at exposing the infiltration of Communists and Soviet sympathizers into American institutions and organizations, including the federal government and labor unions. In these hearings, HUAC members made sweeping, often unsubstantiated allegations. They offered a portrayal of American Communism that was severely distorted yet plausible enough to be persuasive. In this way, the HUAC hearings established a set of strategies that would be adopted by the Permanent Investigating Subcommittee of the Government Operations Committee chaired by McCarthy. But they also contributed to the dehumanization of Communists within American culture, portraying them as ideological outlaws that deserved to be punished.

The year 1950 marked the beginning of the McCarthy era proper. In the middle of that year, North Korean military forces invaded South Korea. Though the United States’ involvement in the conflict was defined as a police action, it

became a constant reminder that the Cold War was not simply a clash of ideologies, but had tangible costs. On the domestic front, Julius and Ethel Rosenberg were charged as Soviet spies for providing the Soviet Union with highly classified information on the development of atomic weaponry. Their arrests provided the ammunition conservative anti-Communists needed to legitimize their attack on domestic Communism. Congress was able to pass the **Internal Security Act of 1950**, which further restricted organizations and members of organizations deemed Communist. Also during this year, the newsletter *Counterattack* became the first publication listing entertainers believed to be Communist Party members or “fellow travelers”—a term used to refer to those with opinions and associations similar to those of Communists.

It was in the beginning of this year that McCarthy made the famous speech in which he proclaimed that he had a list of names of known Communists in the State Department, thus taking center stage in the anti-Communist movement. McCarthy quickly became the most sought-after political spokesperson for the Republican Party, receiving over 2000 invitations to speak at events leading up to the 1950 elections. He, along with many other Republicans, turned Communism into a major issue in the elections by labeling many Democratic candidates as soft on Communism. These charges were only moderately successful, as local issues tended to weigh more heavily on voters, and several Democratic candidates (such as Brion McMahon of Connecticut and Thomas Hennings of Missouri) won despite personal appearances for their opponents by McCarthy.

Charges of Communism by McCarthy and other extremists escalated during 1951 and 1952. Secretary of Defense George Marshall was accused of passively facilitating and even conspiring with Communists within the executive branch. Actor-director Charlie Chaplin was publicly accused of being Communist by **Federal Bureau of Investigation (FBI)** director **J. Edgar Hoover** and eventually had his visa revoked while he was out of the country on vacation. Extensive hearings by HUAC and the Senate Internal Security Subcommittee (SISS) continued to investigate Communist influence within government agencies and labor unions, and among high-profile celebrities and artists. During this time, HUAC alone spent 108 days in hearings encompassing 34 separate investigations. Yet the activities of these two committees would be overshadowed by McCarthy’s Government Operations Committee hearings, which began in 1953 and would last through the early part of 1954. Though limited to the investigation of government agencies and employees, McCarthy’s obstreperous personality and over-the-top tactics attracted a great deal of attention from the media, as did his sweeping claims of Communist infiltration.

The overarching purpose of these congressional hearings was twofold. Conservative anti-Communists used them to influence the broader social standards of political orthodoxy versus heresy in the United States. Yet they also were aimed at discrediting and marginalizing specific individuals. The hearings themselves could not convict suspect witnesses of any crimes and, in fact, had no practical legislative purpose. However, they were used to condemn individuals without adhering to the standards of due process. Hundreds of witnesses were fired by their employers and blacklisted in their industries. The hysteria spurred by the hearings also led to other forms of repression against perceived Communists and political dissidents. The



most infamous was the Hollywood blacklist, which caused the expulsion of thousands of actors, directors, writers, and technical workers from their labor guilds and denied them employment in Hollywood movie productions.

The response to the anti-Communist extremists by presidents Truman and Eisenhower was inconsistent. Both presidents adopted a conservative anti-Communist agenda, though one more moderate than that pursued by McCarthy. Truman did cooperate with the Tydings Committee, which was set up to investigate McCarthy and the validity of his claims, and viewed the activities of some loyalty boards to be un-American; yet he also gave numerous speeches on the threat of domestic Communism. His administration continued to emphasize the arrests of Communists and pushed for the loyalty standard for the termination of employment to be changed from “reasonable grounds” to “reasonable doubt.” The latter resulted in the termination of 565 public employees who had previously been vindicated in hearings before the Loyalty Review Board (LRB).

During the beginning of Eisenhower’s term, the president continually appeased McCarthy. His administration launched investigations for the denaturalization of 10,000 citizens and for the deportation of 12,000 aliens. It also expanded the ability of the executive branch to dismiss federal employees on loyalty issues, resulting in 1500 more employees being terminated (90 percent without receiving any form of hearing). However, by mid-1953 the administration began publicly denouncing McCarthy and openly challenging his attempts to investigate the American clergy and the CIA. Truman and Eisenhower did eventually challenge McCarthy, but both played significant roles in increasing the hysteria associated with McCarthyism.

McCarthy remained a powerful political player for only a few more years. As 1953 wore on, his image worsened in the national media, particularly in television interviews. Media personalities such as newscaster Edward R. Murrow increasingly ran stories that were critical of McCarthy’s tactics, further damaging his public reputation. The climax of McCarthy’s self-destruction came during the televised McCarthy-Army hearings on June 24, 1954. As McCarthy made another of his crass accusations of Communist leanings, Senator Joseph Welch interjected, “Have you no sense of decency, sir, at long last? Have you left no sense of decency?” The Senate chamber erupted in applause, and its reverberations were felt by television viewers across the country. McCarthy lost much of the public support he had previously enjoyed, and the Senate voted to condemn him on December 2.

McCarthyism itself would continue on for another two years. However, it too was crippled in the aftermath of the McCarthy-Army hearings, as television was no longer permitted to air the congressional hearings that had fueled the anti-Communist hysteria among the general public. The McCarthy era is generally considered to have ended in 1956, when a series of Supreme Court cases (including *Slochower v. Board*, 351 U.S. 551 (1956) and *Cole v. Young*, 351 U.S. 536 (1956)) began to curb the repressive policies initiated under the guise of national security and to reinstate basic civil liberties.

See also: Constitutional protections; Counter Intelligence Program (COIN-TELPRO)

Suggested Reading: Doherty, T. *Cold War, Cool Medium: Television, McCarthyism, and American Culture*. New York: Columbia University Press, 2003; Goldstein, R.J. *Political Repression in Modern America, from 1870 to 1976*. Chi-

cago: University of Illinois Press, 2001; Heale, M.J. *American Anticommunism: Combating the Enemy Within, 1830–1970*. Baltimore: John Hopkins University Press, 1990.

Brian L. Zirkle

Mere Evidence Rule

Mere evidence is evidence seized from a person's **home** that the government has no property interest in and that is intended only to be used as evidence against the property owner. Mere evidence cannot be the fruits or instrumentalities of a crime or contraband. Mere evidence was the subject of an evidentiary rule adopted by the Supreme Court in 1921 and abandoned in 1967. The rule prevented the admission of such evidence at trial. The intent of the rule was to prevent the compelled self-incriminating testimony of the homeowner. The rule barred the issuance of a **search warrant** when the goal was *only* to seize mere evidence. Instead, whether a search was conducted with a warrant, or without a warrant but under the appropriate circumstances, authorities could only seize fruits and instrumentalities of a crime or contraband.

The rule had its genesis in *Gouled v. United States*, 255 U.S. 298 (1921). In 1918, Gouled was suspected of conspiring to defraud the government in dealings for clothing and equipment needed for the war effort. The government induced an Army private who was a friend of Gouled to secure access to Gouled's office and records. The private did just that and, while Gouled was out of the room, seized several documents that were later offered in evidence against Gouled. Gouled had no idea the documents had been removed. After the first seizure, the government obtained two different search warrants and seized additional documents to use against Gouled at trial.

The Supreme Court had no difficulty resolving the case. It ruled that none of the documents had been properly admitted against Gouled. The initial search and seizure by the Army private were both unreasonable and unconstitutional.

The two search warrants used to seize the additional documents were proper on their face, as the documents were identified as instrumentalities of a crime. The problem for the Court lay in the nature of the documents seized. The Court noted, "There is no statement . . . of the contents of these papers, but it is said of them only, that they belonged to Gouled, that they were without pecuniary value, and that they constituted evidence more or less injurious to the defendant."

The Court relied on common law and prior Supreme Court rulings to find that only "stolen or forfeited property, or property liable to duties and concealed to avoid payment of them, excisable articles and books required by law to be kept with respect to them, counterfeit coin, burglars' tools and weapons, implements of gambling 'and many other things of like character' might be searched for in home or office, and if found might be seized." But search warrants could not be lawfully "used as a means of gaining access to a man's house or office and papers solely for the purpose of making search to secure evidence to be used against him in a criminal or penal proceeding."

The Court did note that there was no special protection for papers. Indeed, it listed several circumstances under which papers could legally be searched for and



seized, such as searches for stolen or forged papers, lottery tickets when it is illegal to possess them, or even contracts when their seizure will prevent further fraud. In this instance, however, the Court held that the seizure of papers solely for the purpose of using them as evidence against their owner was the equivalent of the owner's forced testimony against himself and was constitutionally protected. The Court's position was, in essence, based on property interests. When the government's property interest was superior to that of a homeowner, search and seizure was appropriate. When the government had no property interest in the items, search and seizure was unlawful.

In 1967, as the Supreme Court rejected the rule in *Warden v. Hayden*, 387 U.S. 294 (1967), Justice Brennan noted that in the years between 1921 and 1967, the mere evidence rule "spawned exceptions so numerous and confusion so great, in fact, that it is questionable whether it affords meaningful protection." Indeed, by 1967 the court had extended privacy rights to prohibit seizure "of the very items which at common law could be seized with impunity: stolen goods, instrumentalities, and contraband."

The facts in *Warden* were interesting, although, in truth, they did not play an overwhelming role in the Court's decision. During the early morning hours on March 17, 1962, an armed man stole \$363 from Baltimore's Diamond Cab Company and ran. Two taxi drivers outside the office saw the man flee and followed. During the chase they gave their dispatcher a description of the man and provided the address of the home the man had entered. The dispatcher relayed the information to police. Within minutes, police arrived at the scene and were given permission by the suspect's wife to search the home.

Officers searched through the two residential floors and the basement of the home looking for the suspect. He was found in an upstairs bedroom in bed pretending to be asleep. In other parts of the home, officers found guns hidden in a running toilet and the clothes the suspect had worn during the robbery in a washing machine. Ammunition for one of the guns was found under the suspect's mattress. Ammunition for another gun was found in a bureau. All the evidence was admitted at trial. On appeal in a habeas action, the federal Court of Appeals ruled the search proper, but the clothing was immune from seizure since it was mere evidence and it should not have been admitted at trial.

The Supreme Court rejected the argument, noting

Nothing in the language of the Fourth Amendment supports the distinction between 'mere evidence' and instrumentalities, fruits of crime, or contraband. . . . Privacy is disturbed no more by a search directed to a purely evidentiary object than it is by a search directed to an instrumentality, fruit, or contraband [and] nothing in the nature of property seized as evidence renders it more private than property seized, for example, as an instrumentality; quite the opposite may be true. Indeed, the distinction is wholly irrational, since, depending on the circumstances, the same 'papers and effects' may be 'mere evidence' in one case and 'instrumentality' in another.

Justice Brennan explained that the proposition that the Fourth Amendment was designed to protect property rights had long been discredited. Instead, he declared, "We have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property." To achieve the balance frequently needed, he

explained the court had adopted the “remedy of exclusion.” The idea that government must prove a superior property interest to justify a search and seizure was a fiction that obscured the fact that government had a serious interest in solving crime.

The Court held that “[t]he requirements of the Fourth Amendment can secure the same protection of privacy whether the search is for ‘mere evidence’ or for fruits, instrumentalities, or contraband.” It added that the possibility of suppression when rights are violated actually provides more protection to individuals because it allows them to assert constitutional protections without claiming any property interests. In effect, privacy rights under the Fourth Amendment were seen to be superior to property rights.

Privacy advocates, however, would not cheer the decision. *Warden* was arguably the death knell for any claim that the search of a person’s home for evidence constituted an impermissible effort by government to force the homeowner’s self-incriminating testimony. Indeed, the long-held notions of what constituted self-incrimination or testimony have fallen by the wayside as the courts will now allow seizure of conversations, voice and handwriting exemplars, demonstrative evidence, **fingerprints**, blood and urine samples, and fingernail and skin scrapings. In some instances, these seizures can be made without a warrant provided the government can show that its special needs are met.

The decision also effectively opened the doors of any home when officers can show probable cause to believe that evidence of a crime, fruits or instrumentalities of a crime, or contraband might be found in that home. The reliance on suppression provides little protection for the homeowner who didn’t want the sanctity of the home invaded in the first place.

Finally, a third consequence of *Warden*’s rejection of the mere evidence rule was that it opened the door for police to search the homes of third parties—people not personally suspected of committing crimes—for evidence to be used in the prosecution of another. This extension was confirmed in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), in which the Court held

Under existing law, valid warrants may be issued to search *any* property, whether or not occupied by a third party, at which there is probable cause to believe that fruits, instrumentalities, or evidence of a crime will be found. Nothing on the face of the Amendment suggests that a third-party search warrant should not normally issue. The Warrant Clause speaks of search warrants issued on “probable cause” and “particularly describing the place to be searched, and the persons or things to be seized.” In situations where the State does not seek to seize “persons,” but only those “things” which there is probable cause to believe are located on the place to be searched, there is no apparent basis in the language of the Amendment for also imposing the requirements for a valid arrest—probable cause to believe that the third party is implicated in the crime.

If the mere evidence rule still applied, the privacy of those third parties would be protected since the searches authorized by *Zurcher* would *only* be for mere evidence.

See also: Constitutional protections; Blood testing; Urine analysis; Voice identification



Suggested Reading: Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Dash, Samuel. *The Intruders: Unreasonable Searches and Seizures from King John to John Ashcroft*. New Brunswick, NJ: Rutgers University Press, 2004; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Hubbart, Philip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Newton, Charles T., Jr. "The Mere Evidence Rule: Doctrine or Dogma?" *Texas Law Review* 45 (1967): 526–564; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

David J. Brown

Microphones. See Electronic surveillance

Multi-State Anti-Terrorism Information Exchange (MATRIX)

The Multi-State Anti-Terrorism Information Exchange, or MATRIX, program was an attempt by state government to use **data mining** to fight crime and terrorism on the national and local levels following the attacks of September 11, 2001. MATRIX was a consortium of law enforcement and state agencies that joined law enforcement records with other government and private-sector databases in an attempt to find patterns, relationships, and links among people. The MATRIX project was administered by the Institute for Intergovernmental Research, funded under the Department of Homeland Security's (DHS) Office of Domestic Preparedness (\$8 million) and the Department of Justice's Bureau of Justice Assistance (\$4 million), and managed by the Florida Department of Law Enforcement.

The MATRIX program utilized the private data aggregation company Seisint Inc. and its locate-and-research tool called Accurant. The system digitally identified and tagged over 3.9 billion **public records** containing information and data on almost everyone within the United States. The program applied Factual Analysis Criminal Threat Solution (FACTS), which gave law enforcement the ability to query available public records even with incomplete information like partial license plate numbers or incomplete names. This massive data reservoir was then analyzed and scored to generate leads and expedite investigations. The resulting information was then shared with law enforcement.

The **computer**-generated scores created by the MATRIX program were referred to as a terrorism quotient or a high factor score for terrorism. Their purpose was to profile individuals to prevent terrorist attacks. The accuracy and potential impact of MATRIX's identification system was significant. The program claimed to have successfully identified five of the 9/11 hijackers and to have assisted the independent agency National Center for Missing and Exploited Children in tracking missing and abducted children.

Immediately after 9/11, the project was encouraged by the mandates set forth in the 2002 Attorney General's Guidelines on General Crimes, Racketeering Enterprise,

and Terrorism Enterprise Investigations. The guidelines empowered the **Federal Bureau of Investigation (FBI)** to carry out general topical research, including conducting online searches and assessing online sites and forums, to the same extent as the general public as long as the research was relevant to the purpose of facilitating or supporting the discharge of investigative responsibilities. Initially, 16 states joined the project. State participation diminished when it was learned that state-owned data had to be transferred to private MATRIX system administrators, which violated state privacy laws. Eventually the system was altered so that the information was stored in a remote, state-maintained and secured database as opposed to the MATRIX central data repository.

The MATRIX program was heavily criticized. Challenges were made to the quality of the data and the difficulty for individuals to correct faulty data. Critics complained of vast amounts of easily accessed, potentially private information. Other concerns included the characteristics used to profile individuals and the possibility that the government could, with the assistance of analytical software, conduct electronic searches on people whom they had no reason to suspect of criminal or illegal behavior. MATRIX supporters believed that the program served as an investigative tool with sufficient regulatory control to guard against indiscriminate surveillance on individuals or to engage in inappropriate or unauthorized use. In 2003, however, the program was terminated and condemned as a state-level version of the discredited federal-level “Total Information Awareness” project, which queried both public and private records, including mailing lists and credit histories.

See also: **Background checks; Banking and financial records; Carnivore; Surveillance**

Suggested Reading: Accurint for Law Enforcement. *2005 Manage Risk with More Intelligence* <http://www.accurint.com/lawenforcement.html>. Online, March 2005; Krouse, William J. “Congressional Research Service’s Report for Congress.” *The Multi-State Anti-Terrorism Information Exchange (MATRIX) Pilot Project*. U.S. Department of State (August 18, 2004). <http://fpc.state.gov/fpc/35968.htm>. Online, March 2006.

Jill Joline Meyers

N



***NAACP v. Alabama*, 357 U.S. 44 (1958)**

In 1956 the attorney general of Alabama brought a suit to the state circuit court of Montgomery, Alabama, challenging the National Association for the Advancement of Colored People (NAACP) for violation of a state statute requiring foreign corporations to qualify before doing business in the state. As part of its strategy to enjoin the NAACP from operating, Alabama required the association to reveal to the state's attorney general the names and addresses of all its members and agents in the state. The NAACP, a nonprofit membership corporation based in New York, had not complied with the statute, believing itself exempt. The suit sought both to prevent the association from conducting further business within the state and, indeed, to remove it from the state altogether. Referring to the association's involvement with the Montgomery bus boycott in 1955 and its role in funding and providing legal assistance to black students seeking admission to the state university, the suit charged that the association was "causing irreparable injury to the property and civil rights of the residents and citizens of the State of Alabama for which criminal prosecution and civil actions at law afford no adequate relief." On the day this suit was filed, the circuit court agreed to issue an ex parte order restraining the association from conducting business in the state or from taking steps to qualify it to do so.

The association responded by moving to dissolve the order on the grounds that its activities within the state did not merit its qualification under the statute, and that the state's suit was intended to violate its rights to freedom of speech and of assembly as guaranteed by the Constitution of the United States. Before a hearing date was set, the state issued a subpoena for much of the association's records, including bank statements and leases, but most notably the names and addresses of the "agents" or "members" of the association in Alabama. In its response to the lawsuit, the NAACP admitted that it was in breach of the statute and offered to attain qualification to continue business if that part of the ex parte order was lifted; because the association did not comply with the order to produce its records, however, that motion was denied and the association was held in contempt and fined



\$10,000. The contempt order allowed for reduction or remission of the fine if the production order was complied with within five days, after which the fine would be raised to \$100,000.

Contending that the state could not constitutionally force **disclosure** of the records, the association moved to dismiss the contempt judgment once more. According to Alabama case law, however, a petitioner could not seek a hearing to dissolve an order until it had purged itself of contempt.

The United States Supreme Court reversed the first contempt judgment. The Alabama Supreme Court then claimed that the U.S. Supreme Court had relied on a “mistaken premise” and reinstated the contempt judgment, which the U.S. Supreme Court again reversed. The NAACP moved to try the case on the merits; this motion was denied and again appealed to the U.S. Supreme Court, which remanded the case to Alabama, ordering the federal district court to try the case on the merits if the Alabama court system continued to refuse to do so. The Alabama circuit court finally heard the case on the merits, and decided the NAACP had violated Alabama law and ordered it to stop doing business in the state; Alabama appeals courts upheld this judgment, refusing to hear the NAACP’s appeals on constitutional grounds. Finally, the fourth time the case was heard by the U.S. Supreme Court, it granted certiorari and itself decided the case on the merits rather than remanding it to the balking Alabama court system, which had taken five years to get this far.

In an opinion delivered by Justice John Marshall Harlan II, the Supreme Court decided in favor of the petitioners, holding, “Immunity from state scrutiny of petitioner’s membership lists is here so related to the right of petitioner’s members to pursue their lawful private interests privately and to associate freely with others in doing so as to come within the protection of the Fourteenth Amendment.” It further held that **freedom of association** with organizations dedicated to the “advancement of beliefs and ideas” is an inseparable part of the Due Process Clause of the Fourteenth Amendment. Because the action of the state of obtaining the names of the association’s membership would likely interfere with the free association of its members, the state’s interest in obtaining the records was superseded by the constitutional rights of the petitioners.

The main principle that may be distilled from this case is that a vital relationship exists between freedom to associate and privacy in one’s associations (U.S.C.A. Const. Amend. 14). Justice Harlan held that the order requiring the association to produce records including the names and addresses of all members and agents was a denial of due process as it entailed the likelihood of a substantial restraint on members’ exercise of their right to freedom of association.

See also: **Constitutional Protections**

Suggested Reading: Barteo, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black’s Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Bodenhamer, David J., and James W. Ely, Jr. (eds.) *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000.

Tod J. Beavers

National Crime Information Center

The National Crime Information Center (NCIC) is a **computer** database of criminal justice information established by the **Federal Bureau of Investigation (FBI)** in 1967. The purpose of the NCIC system is to provide criminal justice agencies with access to cross-jurisdiction information about crimes and criminals. The original database was designed to provide law enforcement agencies with information on wanted persons, federal fugitives, and stolen property. Since then, the NCIC has expanded considerably to include information on missing persons, unidentified bodies, criminal history records, individuals who are believed to pose a threat to the president, foreign fugitives, gangs, and terrorists. Over the years the system has grown and new databases have been added. There are currently 17 separate databases maintained by the NCIC, containing more than 34 million records. It is available to federal, state, and local law enforcement agencies and is operational 24 hours a day, 365 days a year.

More than 80,000 law enforcement agencies nationwide have access to NCIC, and the number of transactions processed at the center has expanded dramatically over the years. In its first year of operation, NCIC handled 2 million transactions. During fiscal year 2005, NCIC processed over 1.6 billion transactions, for an average of 4.5 million transactions a day. This is close to an 18 percent increase in volume compared with 2004. The NCIC is often described as a federal-level database, but it is actually a system where data are contributed and maintained by individual state and local law enforcement agencies through a multilayered computer network. Information from agencies is intended to be timely; for example, when an agency makes an arrest, it submits all applicable arrest information within 24 hours. Agencies must also update the status of records (i.e., court disposition) as persons are processed through the system. The NCIC continues to incorporate the latest technological innovations. Currently the system is in the process of updating its technological capabilities to handle more information such as digital versions of **fingerprints** and photographs.

There are protections in place that limit access to agencies that have authorization. All records in the NCIC are protected from unauthorized access through administrative, physical, and technical safeguards. Some of these safeguards include restricting access to those with a need to know for performance of their official duties, and using locks, alarm devices, passwords, and/or data encryption. As the amount of information on persons in the NCIC has expanded, issues of information accuracy and privacy have come under scrutiny. The **Privacy Act of 1974** requires the FBI to make reasonable efforts to ensure the accuracy and completeness of records in NCIC system. Recently, however, the Justice Department has exempted the system from the accuracy requirements of this act. This is troubling to many, as there was a general understanding upon the passage of the act that the FBI would proceed with the NCIC database only if it complied with the act's obligations. Now the FBI is seeking to abandon that agreement, asserting that it is impossible to determine in advance what information is accurate, relevant, timely, and complete.

The lack of FBI commitment to the NCIC's accuracy represents a significant departure that has implications for individuals with records in the NCIC database. There have been documented cases of arrests made on the basis of inaccurate



information supplied by the NCIC. Furthermore, the legitimacy of the system itself as a law enforcement tool is jeopardized. As the number of cases in which inaccurate NCIC information is used to make arrests increases, so will the chances that these inaccuracies will be used in a court of law to challenge the legality of the arrests.

Suggested Reading: Mason, Richard O. "Four Ethical Issues of the Information Age," *MIS Quarterly* 10 (1986): 5–12; Nunn, Samuel. "Seeking Tools for the War on Terror: A Critical Assessment of Emerging Technologies in Law Enforcement," *Policing: An International Journal of Police Strategies & Management* 26 (2003): 454–472; Schneier, Bruce. "Guilty Until Proven Innocent?" *IEEE Security and Privacy* 1 (2003):88–87.

April Pattavina

National identity cards

In the United States, the creation of a national identifier system has been debated between national security advocates and civil libertarians for many years. Advocates suggest that a national ID is a means to unmask potential terrorists and guard against illegal immigration. Critics cite that the requirement of a national identifier will seriously jeopardize privacy rights. Historically, civil libertarians have won the debate. Extension of the **Social Security number** (SSN) to the status of a universal identifier has been rejected continuously since its inception in 1936. Both the Reagan administration and the Clinton administration have supported the opposition to a national identifier. The administration of George W. Bush, however, has expressed support for the national identifier concept.

The primary concern is that access to the information will be sought and secured by various unauthorized individuals. In addition, there is fear that the technology will be used in inappropriate ways to monitor citizens' movements and to harass and discriminate against minorities or certain suspect categories of people. In short, a national ID system would create a single, large, centralized database of personal information on all citizens. The potential privacy implications are profound. The storage of personal information in unrelated or non-centralized databases is an important protection to privacy. In a free society a law-abiding citizen can compartmentalize the particulars of his or her life, keeping personal matters separate from business affairs, for example. The consolidation of these "compartments" into one database can create the potential for significant problems if an error occurs. No longer will one's **credit rating** be the only aspect of life affected by a mistake in one's financial records. With the existence of a national ID system, an individual's entire life could be disrupted until the inaccuracy is corrected.

The lack of an official national ID system did not stop Congress from passing the Real ID Act of 2005, which established federal requirements for state driver's licenses and identification cards for those who live or work in the United States. The Act does not take effect until May 2008. Critics contend that the Real ID Act will convert one's driver's license into a de facto national ID card.

Additional concerns have been raised. The Act apparently requires that the new IDs include all of the information on current state-issued licenses and identification cards, including a digital photo for the purpose of entering the information into

multistate databases. To obtain the new ID, several types of documentation must be produced verifying one's name, date of birth, SSN, principal residence, and legal status in the United States. Only street addresses can be used; the use of a post office box as one's local address is prohibited. Thus, the law precludes homeless persons and those who, for safety reasons (e.g., potential domestic violence victims, police, and judges), currently withhold their addresses. Further, the IDs must use a common machine-readable technology that meets the requirements set forth by the Department of Homeland Security so that the information contained therein can be linked with all other state motor vehicle departments and can be easily incorporated in other federal databases. Additionally, the bill allows Homeland Security to add requirements in the future, possibly including the use of **biometric identifiers**. Critics fear that **radio frequency identification (RFID)** tags or enhanced **bar codes** will be included among the required features of the new IDs. Such tags could give the government the ability to track the cardholder's movements.

The identification card will be required in order for a person to obtain a valid driver's license, to gain access to a federal government service, to collect Social Security or other health benefits, to visit federal buildings, or to utilize banking or airline services. Although the government will confirm the data and issue the cards, there is no guarantee that the information included on the cards will be unavailable to commercial entities. It is common knowledge that some states allow their license data to be sold to third parties. Furthermore, the act does not include safeguard provisions such as encryption or methods to prevent the data from being remotely scanned.

See also: **Driver's Privacy Protection Act; Smart Cards**

Suggested Reading: eGov.Strategies. *Smart Card Tutorial*. smart.gov/tutorial/tutorial_56k/smartcard_56k.cfm. Online, December 2005; Electronic Privacy Information Center. *National ID Cards and Real ID Act, 2005*. www.epic.org/privacy/id_cards/. Online, December 2005; Privacy International. *Identity Cards: Frequently Asked Questions #13*. www.privacy.org/pi/activities/identitycard/identitycard_faq.html#13. Online, December 2005; Ramasastry, Anita. *Why the "Real ID" Act is a Real Mess*. CNN (August 12, 2005). www.cnn.com/2005/LAW/08/12/ramasastry.ids/index.html. Online, December 2005.

Jill Joline Myers

National Security Agency

The National Security Agency/Central Security Service (NSA/CSS) was created in 1952 through an executive order issued by President Harry S Truman. A division of the United States Intelligence Community, the NSA is considered to be America's code-breaking organization, established to protect the United States from threats to national security. The NSA employs some of the nation's most gifted mathematicians, who use Signals Intelligence (SIGINT) to decipher electronic transmissions intercepted from satellites. These transmissions can be communications via the **Internet**, telephone, fax, radio, or any other means of coded communication.

Working in conjunction with the Department of Defense, the NSA has become one of the largest divisions in government intelligence. The classified nature of this agency's work has raised concerns about issues of privacy. Although the word



“privacy” is not mentioned explicitly in the U.S. Constitution, privacy rights have been supported based on the First, Fourth, and Fifth Amendments. In relation to the NSA, privacy can be understood to constitute protection against the **disclosure** of personal information. An individual’s right to privacy is important because it impedes discrimination and fraud and provides protection from abuses of government power. Due to the NSA’s secrecy, its objectives and impacts are unclear. Nevertheless, we can be confident that the NSA affects Americans’ rights and expectations of privacy.

The original purpose of the NSA was to conduct military surveillance on foreign powers during World War II. This was accomplished through the interception and deciphering of foreign communications. Since the end of World War II, **surveillance** responsibilities of the NSA have shifted to focus on small, organized groups within the United States. Now, in addition to monitoring foreign communications for military purposes, the NSA focuses on drug smugglers and terrorists. Surveillance of small groups within the United States has often resulted in the random use of **wiretapping**. Also referred to as domestic spying, these wiretaps permit government offices to monitor domestic communication for traffic patterns. Traffic patterns indicate when, how often, and with whom communication occurs. Random wiretaps have raised concerns that Americans’ civil liberties are being infringed upon when the NSA monitors communication without consent or judicial warrant. Moreover, the effectiveness of wiretaps has not been demonstrated.

Electronic eavesdropping, in particular, is a contentious issue. On one hand, cases based on evidence from wiretaps are often dismissed in court on the grounds of invasion of privacy. On the other hand, the NSA and other U.S. intelligence divisions defend their actions by insisting that they maintain national security. For example, during World War II the NSA’s deciphering of a Japanese code enabled the United States to win the “Battle of Midway.” This military success ironically brought public attention to the previously secret procedures of the NSA. This awareness led many Americans to feel apprehensive about the NSA’s potential to violate their privacy.

Privacy advocates cite the “Keith” case (*United States v. United States Dist. Ct.*, 444 F.2d 651, 6th Cir. 1971), where District Court Judge Damon J. Keith ruled that the U.S. government has no authority to spy, without a warrant, on private citizens within the United States. The U.S. Supreme Court unanimously upheld this decision on June 19, 1972. However, some in the executive branch have argued that this decision applies only to domestic, not foreign, communication. Consequently, they contend that the president maintains constitutional power to authorize **electronic surveillance** without consent or warrant in order to protect national security. A direct result of this debate has been increased congressional oversight of the NSA. Congress passed the **Foreign Intelligence Surveillance Act of 1978 (FISA)**, which requires that the government obtain a warrant to conduct surveillance on U.S. soil. Warrants for surveillance must be issued by the Foreign Intelligence Surveillance Court. Warrants are granted based on probable cause that an individual is affiliated with a foreign power and a threat to national security.

However, presidential authority, justified by executive order, overrides Congress. Executive authority can be used to permit the installing of wiretaps without a warrant. In these cases, FISA has authorized surveillance warrants even after wiretaps have

been installed and monitored. These procedures have been upheld in court on grounds of national security. In addition, executive orders authorizing eavesdropping for national security reasons have not provided safeguards, guidelines, or limitations in conducting surveillance without consent. Executive orders that are not subject to judicial scrutiny prevent the development of judicial precedent on questions of domestic surveillance.

Civil liberties are often weakened when presidential authority circumvents the legislative and judicial branches. Although it can be argued that the lack of judicial regulation indicates that the NSA does not infringe upon civil liberties, the idea of unchallenged executive power remains a concern to privacy advocates. For example, President George W. Bush was accused of violating FISA when he authorized, without obtaining a warrant from the court, electronic eavesdropping on individuals allegedly linked to Al Qaeda within the United States. Nevertheless, broad presidential authority, granted by executive order, has been upheld by the U.S. Supreme Court. Charges that wiretaps were a violation of privacy were dismissed. The Court deemed the surveillance of individuals allegedly linked to Al Qaeda as necessary and appropriate to protect national security.

Proponents of electronic surveillance often emphasize the instances where wiretapping has been used to apprehend terrorists, win wars, and protect national security. Opponents argue that electronic surveillance is a violation of civil liberties. Also of concern is that the NSA's surveillance program violates the separation of powers established in the U.S. Constitution. The top-secret nature of the NSA, combined with broad presidential authority, is a significant privacy concern. The NSA has often been credited with protecting national security, yet there is strong support for the premise that the capability of the NSA to regulate privacy simultaneously poses a serious threat to civil liberties.

See also: **Federal Bureau of Investigation (FBI); Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities**

Suggested Reading: Best, Richard A., Jr. *The National Security Agency: Issues for Congress*. CRS Report for Congress, <http://www.fas.org/irp/crs/RL30740.pdf>. Online, March 2006; Halperin, Morton, Jerry Berman, Robert Borosage, and Christine Marwick. *The Lawless State: The Crimes of the U.S. Intelligence Agencies*. London: Penguin Books, 1976.

Christine Schneider

Nineteen Eighty-Four. See Big Brother

O



O'Connor v. Ortega, 480 U.S. 509 (1987)

Dr. Magno Ortega, respondent, a physician and psychiatrist, was an employee of a state hospital and had primary responsibility for training physicians in the psychiatric residency program. In 1981 hospital officials, including Executive Director Dr. Dennis O'Connor, became concerned about possible improprieties in his management of the program, particularly with respect to his acquisition of a **computer** and charges against him concerning **sexual harassment** of female hospital employees and inappropriate disciplinary action against a resident. While he was on administrative leave pending investigation of the charges, hospital officials, allegedly in an effort to inventory and secure state property, searched his office and seized personal items from his desk and file cabinets, which were then used in administrative proceedings resulting in his discharge. The hospital's investigation included multiple searches of his office and the seizure of a number of items. The items were used in proceedings before the California State Personnel Board to impeach the credibility of witnesses who testified on Dr. Ortega's behalf. No formal inventory of the property in the office was ever made, and all other papers in the office were placed in boxes for storage. Dr. Ortega filed an action against the hospital officials (petitioners) in federal district court under 42 U.S.C §1983, alleging that the search of his office violated the Fourth Amendment. On cross-motions for summary judgment, the district court granted judgment for the petitioners, concluding that the search was proper because there was a need to secure state property in the office. Affirming in part, reversing in part, and remanding the case, the court of appeals concluded that Dr. Ortega had a **reasonable expectation of privacy** in his office and that the search violated the Fourth Amendment. The court held that the record justified a grant of partial summary judgment for the respondent on the issue of liability for the search, and it remanded the case to the district court for determination of damages.

Did the supervisor's search of the office violate Dr. Ortega's "reasonable expectation of privacy" guaranteed by the Fourth Amendment? The court discussed whether probable cause is an inappropriate standard for public employer searches



of employees' offices. The court undertook a balancing test of governmental and private interests and determined that the public interest is best served by a Fourth Amendment standard of reasonableness that stops short of probable cause. The court stated that it "recognized the plethora of contexts in which employers will have an occasion to intrude to some extent on an employee's expectation of privacy." Also, "[t]he governmental interest justifying work-related intrusions by public employers is the efficient and proper operation of the workplace." The rationale appears to be that governmental agencies would be less efficient and the general public would suffer if employers were required to have probable cause before searching an employee's desk for the purpose of locating a file or office correspondence. The court reasoned that it makes little sense to apply the criminal concept of probable cause when the search is simply to retrieve a file or execute a routine inventory conducted by public employers for the purpose of securing state property. "To ensure the efficient and proper operation of the agency, therefore, public employers must be given wide latitude to enter employee offices for work-related, non-investigatory reasons."

Searches and seizures by government employers or supervisors of the private property of their employees are subject to Fourth Amendment restraints. An expectation of privacy in one's place of work is based on societal expectations that have deep roots in the history of the amendment. However, the operational realities of the workplace may make some public employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official. Some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable. Given the great variety of work environments in the public sector, the question of whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis. Although the record did not reveal the extent to which hospital officials may have had work-related reasons to enter Ortega's office, a majority of the district court agreed with the determination of the court of appeals that the respondent had a reasonable expectation of privacy in his office, or at least in his desk and file cabinets.

For a search conducted by a public employer in areas in which an employee has a reasonable expectation of privacy, what is a "reasonable" search depends on the context in which the search takes place and requires balancing the employee's legitimate expectation of privacy against the government's need for supervision, control, and the efficient operation of the workplace. Requiring that a **search warrant** be obtained whenever an employer wishes to enter an employee's office, desk, or file cabinets for a work-related purpose would seriously disrupt the routine conduct of business and would be unreasonable. Moreover, requiring a probable-cause standard for searches of the type at issue here would impose an intolerable burden on public employers. Intrusions on the constitutionally protected privacy interests of government employees for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all circumstances. Under this standard, both the inception and the scope of the intrusion must be reasonable.

In the procedural posture of the case, the court stated that it cannot be determined whether the search of Dr. Ortega's office and the seizure of his personal belongings satisfied the standard of reasonableness. Both courts were in error

because the summary judgment was inappropriate. The parties were in dispute about the actual justification for the search, and the record was inadequate to allow a determination of the reasonableness of the search and seizure.

To summarize, in a 5-to-4 decision, the court held that the search did not violate the Fourth Amendment. The court held that “the realities of the workplace” made some expectations of privacy among public employees unreasonable when the intrusion is by a supervisor rather than a law enforcement official. Work-related searches, the court found, were “merely incident to the primary business of the agency,” and a warrant requirement would “seriously disrupt the routine conduct of business.” The court thus held that a standard of “reasonableness” was sufficient for work-related intrusions by public employers.

See also: **Civil Service laws; Search warrants; Workplace privacy**

Suggested Reading: Barteo, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black’s Law Dictionary*, 7th ed, St. Paul, MN: West, 1999; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

Tod J. Beavers

Oliver v. United States, 466 U.S. 170 (1984)

This case was a consolidation of two cases involving similar facts. In the first case, officers received reports that Ray Oliver was growing marijuana on his farm in rural Kentucky, and went to investigate. They drove past Oliver’s **home** to a locked gate that featured a “No Trespassing” sign but had a footpath around one side. The agents walked around the gate and then along the road and found a field of marijuana over a mile from Oliver’s house. Oliver was charged with possession and manufacture of a controlled substance. He sought to suppress admission of the evidence discovered by the officers as a product of an unlawful search and seizure. The district court granted the motion and suppressed the evidence, determining that Oliver had a **reasonable expectation of privacy** in the area of the farm that was searched. Relying on *Katz v. United States*, **389 U.S. 347 (1967)**, the district court found that because of the locked gate and the “No Trespassing” sign, Oliver “had done all that could be expected of him to assert his privacy in the area of farm that was searched.” The state appealed; a panel of the Court of Appeals for the Sixth Circuit affirmed and then, upon an en banc rehearing, reversed the district court. The Sixth Circuit Court of Appeals held that the *Katz* decision had not impaired the “open fields doctrine” put forth by the U.S. Supreme Court in *Hester*, allowing officers to enter and search a field without a **search warrant**.

In the second case, officers in Maine received an anonymous tip that Richard Thornton was growing marijuana in the woods behind his home. The officers

entered the woods by means of a footpath between Thornton's home and the home of a neighbor. They discovered two marijuana patches, surrounded by chicken wire and "No Trespassing" signs, in the woods behind Thornton's home. The officers obtained a search warrant based on this information and went back to seize the marijuana as evidence against Thornton. The district court granted Thornton's motion to suppress the fruits of the second search, concluding that the initial warrantless search was unreasonable because Thornton had posted "No Trespassing" signs and "the secluded location of the marijuana patches evinced a reasonable expectation of privacy." The Maine Supreme Judicial Court affirmed the decision. The U.S. Supreme Court granted certiorari.

In an opinion delivered by Justice Powell, the Court reversed both lower courts' decisions suppressing the evidence. The Court relied on its earlier decision in *Hester v. United States*, 265 U.S. 57, 58–59, 44 S.Ct. 445, 68 L.Ed. 898 (1924), in which it first recognized the "open fields" doctrine. In *Hester*, the Court held that "the special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers, and effects,' is not extended to the open fields." The Court stated that the decision in *Hester* was based on the explicit language of the Fourth Amendment, which indicates with some precision the places and things its protections encompass. The Court further stated that its interpretation of *Hester* and open fields was consistent with the "right to privacy" concept extant in Fourth Amendment jurisprudence as put forth in *Katz*. The Court argued that the touchstone of Fourth Amendment analysis is whether a person has a constitutionally protected "reasonable expectation of privacy"; the Fourth Amendment does not protect a merely subjective expectation of privacy, but only those expectations that society is prepared to recognize as reasonable. The Court contrasted those areas in which a person has an expectation of privacy against open fields, opining that open fields "do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or **surveillance**. There is no societal interest in protecting the privacy of those activities, such as the cultivation of crops that occur in open fields." The Court held that open fields are, as a practical matter, accessible to the public and the police in ways a home, an office, or commercial structure would not be. Nor do fences or "No Trespassing" signs effectively bar the public from viewing open fields. Moreover, "the public and the police lawfully may survey the lands from the air. For these reasons, the asserted expectation of privacy in open fields is not an expectation that 'society recognizes as reasonable.'"

The Court cautioned courts against a case-by-case analysis for these types of situations because it would not provide a workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment. Likewise, courts should not consider whether the individual chooses to conceal a "private" activity as the correct test for legitimacy. Rather, in holding that Oliver and Thornton had no legitimate expectation that their open fields would remain free from warrantless intrusion by government officers, the Court defined the correct inquiry as "whether the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment." The *Oliver* court stated that it was reaffirming *Hester* and clarifying the rule therein—that an individual may not legitimately demand privacy for activities conducted out-of-doors in

fields, except in the area immediately surrounding the home, otherwise known as the **curtilage**. The Court remanded the cases back to the district courts and held that “from the text of the Fourth Amendment and from the historical and contemporary understanding of its purposes, . . . an individual has no legitimate expectation that open fields will remain free from warrantless intrusion by government officers.”

See also: *California v. Ciraolo*, 476 U.S. 207 (1986); *Chimel v. California*, 395 U.S. 752 (1969); **Constitutional protections**; *Payton v. New York*, 445 U.S. 573 (1980); **Trespass**; *United States v. Dunn*, 480 U.S. 294 (1987); *United States v. Steagald*, 451 U.S. 204 (1981); *Warden v. Hayden*, 387 U.S. 294 (1967)

Suggested Reading: Barte, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hubbard, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*. 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

Larkin R. Evans

***Olmstead v. United States*, 277 U.S. 438 (1928)**

In the 1928 case of *Olmstead v. United States*, the Supreme Court found no violation of the Fourth Amendment when federal government agents **wiretapped** individuals' telephone lines without first obtaining a judge's approval. Prosecutors used the telephone conversations that the wiretaps intercepted to convict the individuals of Prohibition era crimes. Justice **Louis Brandeis** disagreed with the Court's ruling and wrote a dissenting opinion in which he argued that **constitutional protections** must adapt to new technologies. In addition to predicting some of today's threats to privacy, Justice Brandeis eloquently articulated the “**right to be let alone**.” He described the right to privacy as the most comprehensive and valued of rights. Although the *Olmstead* decision did not prevent unauthorized government **surveillance** of telephone conversations, it defined the terms of a debate about how to conceive of and protect privacy under the Constitution.

Olmstead and 20 other men were convicted by a federal jury in Washington state of conspiring to violate the National Prohibition Act. During the period of 1920 to 1933, when Prohibition was written into the Constitution, federal law made it illegal to transport and sell intoxicating liquors. Olmstead was convicted and sentenced to four years in prison for managing a large-scale illegal importing business that transported liquor by boat from British Columbia to Seattle and then distributed it to numerous customers. The evidence produced during the trial showed that the conspiracy sometimes sold 200 cases of liquor a day and that it likely generated millions of dollars in sales each year. In addition, it appeared that local police, rather than rooting out the crime, were involved in it themselves.



During the trial, wiretaps produced almost all of the incriminating evidence against Olmstead and the other defendants. Federal Prohibition agents had installed the wiretaps on telephone lines leading from the homes and offices of the conspirators, and they had listened in, without detection, over a period of several months. Olmstead objected when prosecutors sought to have the agents testify about the telephone conversations they had overheard. He argued that the wiretaps violated the Fourth Amendment's prohibition of unreasonable searches and seizures because the government agents had not obtained a judge's approval before wiretapping. Olmstead argued that wiretapped evidence acquired in violation of the Fourth Amendment should not have been allowed in his trial.

By the time the Supreme Court heard the case, the trial court had denied Olmstead's request to keep the evidence obtained by wiretaps out of the trial, and two out of the three judges on the federal appellate court that reviewed the trial court's decision had affirmed it. The appellate court majority reasoned that listening into the telephone conversations that traveled over wires to and from the defendants' private homes and attorney's office was just like looking through windows or an open door into those spaces. The appellate court wrote that, even if wiretapping should be considered an "unethical intrusion upon the privacy of persons who are suspected of crime, it is not an act which comes within the letter of the prohibition of constitutional provisions."

The third judge on the appellate panel, Judge Rudkin, disagreed with that analogy and would have accorded telephone conversations the same constitutional protection as sealed letters. In an 1877 case entitled *Ex parte Jackson*, the Supreme Court had written that government agents could not open sealed letters in the mails unless they obtained a proper warrant under the Fourth Amendment. In that case, the Court viewed sealed letters obtained from the postal system as being entitled to the same constitutional protection as papers obtained through the searches of private **homes**. In his dissenting opinion, Judge Rudkin argued that the constitutional protection accorded private papers and sealed letters should be extended to telephone conversations, since there are no meaningful distinctions "between a message sent by letter and a message sent by telegraph or telephone." Because private papers or sealed letters obtained in violation of the Fourth Amendment cannot be used in a trial, the conversations obtained in the *Olmstead* case should have been kept out of the trial as well. Judge Rudkin expressed concern about the practice of using such wiretapped evidence in trials and wrote that "[i]f ills such as these must be borne, our forefathers signally failed in their desire to ordain and establish a government to secure the blessings of liberty to themselves and their posterity."

When it reviewed the appellate court's decision, the Supreme Court faced the question of whether to treat telephone conversations as analogous to sealed letters, and thus entitled to Fourth Amendment protection, or to agree with the lower courts that telephone conversations were constitutionally unprotected. Six out of the nine justices, a majority, declined to extend the protection accorded mail to telephone conversations, because they did not view the Fourth Amendment's protection as extending to intangible conversations intercepted without a physical invasion of private property rights.

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall

not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or Affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

In writing the majority opinion, Chief Justice Taft identified the Fourth Amendment’s historical purpose as preventing “the use of governmental force to search a man’s house, his person, his papers and his effects; and to prevent their seizure against his will.” According to Chief Justice Taft, the constitutional language limits the amendment’s protection to material things, such as persons and papers, and does not extend to intangible conversations. He wrote that it does not constitute a search or seizure for Fourth Amendment purposes when agents gather evidence by hearing, in the same way that there is no search or seizure when agents gather incriminating evidence by merely seeing it. Chief Justice Taft also rejected the analogy between sealed letters and telephone conversations posited by Judge Rudkin. In addition to the fact that letters are tangible things and telephone conversations are not, the chief justice viewed the mail as special because the Constitution provides for the postal system and Congress requires that all mail be sent through that system. Those features did not characterize either the telephone or the telegraph. Chief Justice Taft argued that the telephone wires form a network more like a highway system than the postal system.

The chief justice went on to explain that in prior cases the Fourth Amendment had protected people when they were searched or their papers or effects were seized, or when agents conducted an “actual physical invasion” of a house to obtain evidence. Although many of the defendants in *Olmstead* had been in their homes or offices when their telephone conversations were intercepted, government agents had installed the wiretaps without physically invading the defendants’ private property. Wiretaps targeting private homes had been placed on the street outside, and the office wiretap was installed in the basement of a large building that was apparently not owned by the conspirators. Although urged to regard the wiretapping as equivalent to agents hiding themselves in the defendants’ houses to listen to their conversations, Chief Justice Taft took an entirely different approach. He wrote, “The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment.”

The majority opinion ties Fourth Amendment protection to whether or not the government agents had “trespassed,” or unlawfully entered the defendants’ private property. In doing so, the Supreme Court used property law rules to limit constitutional privacy protection. The majority expressed concern that if the police could violate the Fourth Amendment without conducting a physical intrusion, then the scope of protection would be dramatically extended. Over time, the **trespass** rule was elaborated so that Fourth Amendment analysis was triggered whenever agents intruded upon a “constitutionally protected area.”

Three justices disagreed with the majority’s decision, and although each wrote a separate opinion, Justice Brandeis’s dissent has become the most famous. Justice Brandeis rejected the majority’s narrow reading of the Fourth Amendment and instead advocated a flexible interpretation of its text to encompass situations that the drafters of the constitution neither considered nor imagined. The Fourth

Amendment was designed to prevent government officers from breaking into homes by force to seize papers, and was drafted with that threat to privacy in mind. Referring to **electronic surveillance**, however, Justice Brandeis wrote that, at the time, “[s]ubtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain **disclosure** in court of what is whispered in the closet.” If the constitutional protections were confined to the old methods of invading privacy, Justice Brandeis warned, those protections would have little value.

Justice Brandeis predicted that the majority’s interpretation of the Fourth Amendment would leave unaddressed even greater threats to privacy in the future. “The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping,” he wrote. Justice Brandeis seemed to anticipate the development of networked personal **computers** when he predicted that “[w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the **home**.” The justice also accurately predicted that “[a]dvances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.” Justice Brandeis concluded his disturbing picture of the future with the rhetorical question “Can it be that the Constitution affords no protection against such invasions of individual security?”

In arguing that the underlying purpose of the Fourth Amendment rather than its literal language should guide the Court, Justice Brandeis articulated an understanding of privacy that has been enormously influential. He wrote, “The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man’s spiritual nature, of his feelings and of his intellect. . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.” Justice Brandeis concluded that the Fourth Amendment protects against “every unjustifiable intrusion by the Government upon the privacy of the individual.”

Justice Brandeis rejected both the majority’s refusal to liken telephone conversations to sealed letters and its suggestion that Fourth Amendment protection required a physical trespass under property law. As to the former, Justice Brandeis found the distinctions between telephone calls and sealed letters to be irrelevant, and he noted that telephone conversations had an even stronger claim to protection than sealed letters had. According to Justice Brandeis, because wiretaps indiscriminately capture all conversations between the target of the wiretap and those with whom he or she converses, “The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails.”

Because Justice Brandeis found unauthorized wiretapping to violate the Fourth Amendment, he regarded it as “immaterial where the physical connection with the telephone wires leading into the defendants’ premises was made.” In other words, the government invaded the defendants’ privacy rights even if they did not violate their property rights. Justice Brandeis also regarded as irrelevant whether the

government agents were motivated by their interest in enforcing the law: “The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.” In addition, Justice Brandeis expressed outrage that the Supreme Court refused to exclude the evidence derived from wiretaps when the wiretaps themselves violated state law. “If the Government becomes a lawbreaker,” he warned, “it breeds contempt for law; . . . it invites anarchy.”

A few years after *Olmstead* was decided, Congress passed §605 of the Communications Act of 1934, which made wiretapping a federal crime even though it did not violate the Constitution. Although the new law explicitly prohibited law enforcement’s use of wiretaps, government agents disregarded the law and continued to use wiretaps and the evidence they disclosed. Few prosecutions were brought against those who conducted illegal wiretaps, and none were brought against government agents under the federal law. Some argued that illegal wiretapping would be pervasive until it was recognized to be a violation of the Fourth Amendment.

That happened in 1967, when the Supreme Court held that wiretapping and eavesdropping did in fact fall under the protection of the Fourth Amendment. A few years before, the Supreme Court had extended Fourth Amendment protection to the intangible conversations that the *Olmstead* court had been unwilling to protect, but it did so in the context of a physical intrusion. In *Katz v. United States*, 389 U.S. 347 (1967), the Court extended Fourth Amendment protection to government eavesdropping that occurred without a physical trespass, declaring that “the Fourth Amendment protects people—and not simply ‘areas.’” In his concurring opinion, Justice Harlan formulated the “**reasonable expectation of privacy**” test to replace the “constitutionally protected area” test. Although the former test has been subject to criticism, it stands as the touchstone of Fourth Amendment protection. While the decision in the *Katz* case untethered rights under the Fourth Amendment from private property rights, courts have more readily found constitutionally protected privacy interests in the home than outside of it. As for statutory law, Congress passed the Wiretap Act in 1968, which codified the constitutional requirements established by the Supreme Court the year before.

Justice Brandeis’s dissent in *Olmstead* expanded our understanding of the right to privacy from one based in tort law to one enjoying constitutional protections. His eloquent articulation of the right to be let alone has often been quoted elsewhere, including the opinions from other cases that have expanded constitutionally protected privacy. For example, it was cited in the famous cases of *Griswold v. Connecticut*, 381 U.S. 479 (1965), and *Whalen v. Roe*, both of which charted new ground in defining the parameters of a constitutionally protected privacy right.

The *Olmstead* case illustrates the difficulty of bringing privacy protections in line with new technologies. The various opinions each compared new practices to ones for which there were established precedents, but demonstrated that there are often several possible analogies, and different choices can mean different legal results. As the first case considering the constitutionality of electronic surveillance, *Olmstead* began the ongoing discussion about how much privacy we should expect in new communications technologies when the government decides it wants to listen in.

See also: Constitutional protections; Anti-wiretap statutes; Bartnicki v. Vopper, 532 U.S. 514 (2001)



Suggested Reading: Dash, Samuel, Richard Schwartz, and Robert Knowlton. *The Eavesdroppers*. New Brunswick, NJ: Rutgers University Press, 1959; Diffie, Whitfield, and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press, 1999; Regan, Priscilla. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press, 1995; Smith, Robert Ellis. *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*. Providence, RI: Privacy Journal, 2004; Westin, Allan. *Privacy and Freedom*. New York: Atheneum, 1967; White, G. Edward. *The American Judicial Tradition*. Oxford: Oxford University Press, 1988.

Susan Freiwald

Open meetings laws

All 50 states and many localities as well as the federal government have enacted open meetings laws, or “Government in the Sunshine Acts,” as these laws are often called. **Disclosures** at such meetings, however, may threaten personal privacy. For this reason, many open meetings laws permit the closing of meetings to protect personal privacy. Enactment of these laws followed a public right-to-know movement in the 1960s and 1970s. Those campaigns also led to the passage of **public records** laws. Open meetings laws were adopted by several states prior to the passage in 1976 of the federal Government in the Sunshine Act.

This federal open meetings law illustrates the general aspects of these laws and demonstrates how they protect personal privacy. These laws rest on the proposition that the government’s business should be conducted in public. The federal act requires that the deliberations of councils, commissions, and other public agencies headed by multi-member bodies be open to the public. These laws secure one’s right to observe deliberations, not the right to participate in them. For example, in the federal Government in the Sunshine Act Congress contemplated that the public would observe meetings in the same room as agency members. These laws also assumed that representatives of the media would play an important role in reporting the actions of government officials.

The disclosures accompanying the observation of government deliberations not only inform the public and temper the decisions of boards and commissions, but also provide personal information about individuals discussed in these meetings. The disclosure and publication of personal information about individuals is a potential threat to their privacy; therefore, many, if not most, of these laws include provisions intended to protect personal privacy. A common provision allows meetings or portions of meetings to be closed to the public and the press.

One of the exemptions in the federal Government in the Sunshine Act exemplifies this protection. An agency covered by the law may close a meeting that is likely to disclose information of a personal nature if disclosure “would constitute a clearly unwarranted invasion of personal privacy.” Not all state provisions contain a privacy exemption, however, and even among those that do, some define privacy differently than federal law. Thus, the scope of privacy protection may vary.

The exemption contained in the federal Government in the Sunshine Act is similar to one contained in the federal **Freedom of Information Act**. In the Sunshine Act, the exemption extends to “information of a personal nature,” which means

information applicable to a specific person. If such information is likely to be disclosed at an open meeting, that meeting should be closed if the disclosure would constitute a clearly unwarranted invasion of personal privacy.

The language requires that the interest in privacy be weighed against the public interest in disclosure of the information as part of the process of deliberation. Moreover, the language demonstrates that the balance is clearly in favor of the interest in privacy. Under this test, however, Congress suggested that it might be appropriate to close a meeting in certain circumstances to protect from observation a discussion of a person's health or drinking habits and an assessment of a person's professional ability in connection with review of a person's finances to determine eligibility for financial assistance.

A person's status as a public official may affect the character of privacy protection. For example, the privacy interest of a high government official may be less than that of a lower-ranking official or of a private person. The lesser privacy interest of a high government official whose conduct is discussed at a public meeting reflects the greater public interest in the conduct or qualifications of such an official.

Another, narrower exemption permits the closing of a meeting when the deliberative body is to discuss whether to accuse a person of a crime or to formally to censure that person. Public discussions of these matters can invade the persons' privacy and harm his or her reputation even if the agency decides not to make the accusation or to impose the formal censure.

See also: **Civil Service laws**

Suggested Reading: Berg, Richard K., Stephen H. Klitzman, and Gary J. Edles. *An Interpretation of the Government in the Sunshine Act*, 2nd ed. Chicago: American Bar Association, 2005; *Government in the Sunshine Act—S. 5 (Public Law 94-409)—Source Book: Legislative History, Texts and Other Documents*, 94th Cong., 2d. Sess. (Comm. Print 1976); Koch, Charles H. "State Open Meeting Statutes." In *Administrative Law and Practice*, 2nd ed., §3.61. St. Paul, MN: West, 1997.

Robert G. Vaughn

Opt-in vs. opt-out

Opt-in and opt-out are two methods for exercising the choice principle of **fair information practices**. The choice principle states that personal information should not be collected for one purpose and shared or used for other purposes that are unrelated to the reason the information was originally collected unless the individual consents. For example, if a company collects customer information to complete a sale and subsequently uses that information to send the customer advertisements, or if it sells or rents its customer mailing list to other companies, it needs to offer the customer a choice.

With *opt-out*, consent is implied unless the individual objects to the new use, which means that it is the individual's responsibility to notify the organization that he or she objects to having personal information used or shared for other purposes. With *opt-in*, organizations may not share or use personal information for unrelated purposes unless the individual gives explicit consent. One form of opt-in is "permission marketing," where marketers ask permission before they send



advertisements to prospective customers. On the **Internet**, some of the distinctions between opt-out and opt-in have blurred, as both forms of choice may be provided as part of any online transaction; the individual decides whether or not to check a single box.

In the United States, there is a general consensus that opt-in should be used in cases where sensitive personal information is involved. Opt-out is viewed as appropriate for marketing uses of personal information, except when medical information or information collected from children is involved. The **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** requires that all organizations covered by the law obtain written authorization for any use or **disclosure** of protected health information that is not related to health care treatment, payment, or operations of the health care organization. Opt-in is required, for example, before health information may be disclosed to an employer or used for marketing. The **Children's Online Privacy Protection Act of 1998 (COPPA)** requires any website targeting children under 13 years of age to obtain parental consent before the child's information may be disclosed to third parties.

Recent U.S. laws, for example, mandate opt-out for certain third-party uses of financial information (e.g., the **Financial Services Modernization Act of 1999**, also known as the Gramm-Leach-Bliley Act), commercial **electronic mail** unrelated to a transaction or a subscription (CAN-SPAM Act), and most telemarketing calls (the Federal Trade Commission's **Do-Not-Call Registry**). The Direct Marketing Association's Privacy Promise is a self-regulatory program that requires all DMA members to honor consumer requests to opt out of having their customer information transferred to others for marketing purposes or receiving solicitations from the member company.

For global commerce, the U.S. Department of Commerce negotiated **Safe Harbor principles** with the European Union (EU) in 2000 to allow American companies to transfer personal information from European citizens outside of the EU. The Safe Harbor agreement requires companies to offer opt-out if personal information is to be disclosed to a third party or used for any purpose that is incompatible with the purpose for which the information was originally collected. For sensitive information, opt-in must be offered. The European definition of sensitive information is broader than the American definition and includes information on health, racial or ethnic origin, political opinions, religious beliefs, union membership, or an individual's sex life.

See also: **European Data Protection Directive; Privacy, definition of**

Suggested Reading: Culnan, Mary C. "Protecting Privacy Online: Is Self-Regulation Working?" *Journal of Public Policy and Marketing* 19 (2000):20–26; Krishnamurthy, Sandeep. "A Comprehensive Analysis of Permission Marketing," *Journal of Computer-Mediated Communication* 6 (2001). <http://jcmc.indiana.edu>. Online, March 2006; Regan, Priscilla M. "Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows," *Journal of Social Issues* 59 (2003): 263–287.

Mary J. Culnan

Orwell, George. *See* **Big Brother**

Osborne v. Ohio, 495 U.S. 103 (1990)

In *Osborne v. Ohio*, the United States Supreme Court established the special reasons why child pornography is not subject to any meaningful **constitutional protections** under the First Amendment (or the Fourteenth Amendment as applied to the states). This case clarified the uncertain scope of the right to possession of obscene material under the First Amendment. This landmark case extensively addressed the sociological data supporting an absolute ban on child pornography, regardless of any individual privacy rights in keeping such obscene material. Not surprisingly, the case is widely quoted by the United States Supreme Court and virtually every other lower court in the country in most cases involving challenges to child pornography criminal statutes.

The issue in the case was relatively straightforward. Writing for the majority, Justice White explained that the primary issue in the case was whether the state of Ohio could proscribe the possession and viewing of child pornography in light of the Supreme Court's earlier decision in *Stanley v. Georgia*, 394 U.S. 557 (1969). In that touchstone case, the Court struck down a Georgia law outlawing the private, **home** possession of obscene material based on the First Amendment. Despite this earlier decision in *Stanley*, the Court found that possessing and viewing child pornography is uniquely different and therefore not entitled to any constitutional protection.

To begin, Justice White recognized that an earlier decision issued by the Supreme Court had already established that the value of permitting child pornography to exist is "exceedingly modest, if not *de minimis*." Even accepting the defendant's argument that he had a First Amendment interest in viewing and possessing child pornography, Justice White found the facts of this case were distinct from the issue in *Stanley* "because the interests underlying child pornography prohibitions far exceed the interests justifying the Georgia law at issue in *Stanley*." As Justice White explained, "The difference here is obvious: The State does not rely on a paternalistic interest in regulating Osborne's mind. Rather, Ohio has enacted [its child pornography law] in order to protect the victims of child pornography; it hopes to destroy a market for the exploitative use of children."

To bolster this unique difference, Justice White examined the extensive, untested research about the life-altering damage caused to a child by his or her participation in child pornography. He noted that the legislature of Ohio had decided to make child pornography illegal because of its irreparable harm "to the physiological, emotional, and mental health of the child. That judgment, we think, easily passes muster under the First Amendment" (495 U.S. at 109). He also pointed out that crippling the child pornography market necessitated laws targeting all levels of the market, including production, distribution, and possession. He noted that to reduce the supply, it was legitimate for the state to curb the demand by making child pornography highly illegal and subject to extreme penalties. Equally compelling to the decision was the fact that "the material produced by child pornographers permanently record[s] the victim's abuse. The pornography's continued existence causes the child victims continuing harm by haunting the children in years to come." Finally, he noted the sad statistic that pedophiles often encourage and seduce children to participate in child pornography by showing them other works of child pornography. For all of these reasons, the majority found that



child pornography laws punishing the mere private possession of such material were constitutionally acceptable. As Justice White phrased it, “Given the gravity of the State’s interest in this context, we find that Ohio may constitutionally proscribe the possession and viewing of child pornography.”

In this case, the individual’s right to privacy was unquestionably different from the situation in *Stanley*. In the realm of the First Amendment, some types of material or speech are said to be “unprotected” within the meaning of the Constitution. Examples include “fighting words” or “obscenity.” In *Stanley*, the issue was simply the state’s interest in preventing an adult from reading obscene material in the privacy of his home. The state’s interest was thus considered relatively low, and the individual’s right to absolute privacy in the comfort of his home was deemed enormously high. Ultimately, this case was entirely different based on the critical difference in the type of obscene material. The Supreme Court found a special danger posed by child pornography to the children trapped within its production. This distinction made all the difference in this case, and although the majority seized on a technicality to force the state of Ohio to clarify how it charges defendants under its law, the overall attack on child pornography remained intact. It continues to be quoted extensively in modern cases.

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black’s Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Hall, Kermit L. *Conscience, Expression and Privacy: The Supreme Court in American Society*. New York: Garland, 2000; Smith, Robert Ellis. *Compilation of State and Federal Privacy Laws*. Providence, RI: Privacy Journal, 1992; Turkington, Richard C., and Anita L. Allen. *Privacy Law: Cases and Materials*. St. Paul, MN: West, 2002.

Ryan C. Hudson

P



Paparazzi

Paparazzi is the term used for freelance news photographers who specialize in candid photos or video of celebrities. Celebrities often complain that paparazzi invade their privacy or endanger them through the use of telephoto lenses and aggressive newsgathering techniques. Paparazzi were initially seen as responsible for the car crash that killed Diana, Princess of Wales, in 1997. That incident, in turn, spawned several attempts in the United States to limit access by photographers to celebrities.

The term “paparazzi” comes from a character in Federico Fellini’s 1960 motion picture, *La Dolce Vita*. Paparazzo, played by Walter Santesso, was a photographer who exhibited some of the characteristics now associated with his name. The U.S. publication *Time* first used the term in a 1961 article titled “Paparazzi on the Prowl” and described this new European phenomenon as a “ravenous wolf pack of freelance photographers who stalk big names for a living and fire with flash guns at point-blank range,” and who create scenes by goading celebrities into “arm-flail[ing] rage[s]” to produce salable photographs.

Americans were not immune to paparazzi. By the late 1960s, these photographers routinely stalked celebrities in the United States, selling their photos on both sides of the Atlantic. One constant target was Jacqueline Kennedy Onassis—widow of President John F. Kennedy—and her young children, Caroline and John, Jr. One photographer, in particular, made Onassis his life’s work. At one point this photographer, Ron Galella, caused John, Jr., to fall off his bicycle. In another incident, Galella hid behind the coatrack in a private restaurant to photograph Onassis. On other occasions, he endangered Onassis and the children as they swam, trespassed in the children’s schools, jumped at the family in the dark, and generally made their lives miserable. Eventually Onassis was able to get a restraining order against him, which he violated. In 1972 Galella was found guilty of harassment, assault, commercial exploitation, and invasion of privacy.

Jacqueline Onassis did not want the attention of Galella or of any other paparazzi. Other celebrities, however, have had a less clear relationship with these

photographers. Paparazzi have both helped to create, and capitalized on, a culture that values celebrity. Many people carefully follow the details of their favorite celebrities' lives, including the celebrities' relationships and daily activities. Most celebrities voluntarily participate in this through public appearances and interviews that provide exposure, which helps to continue their celebrity status. But the public wants more information, and the paparazzi provide it, usually through photos taken under less-controlled circumstances than the celebrities' preferred interviews and arranged appearances. Those circumstances, however, routinely infringe upon celebrities' privacy.

Paparazzi encroach upon celebrities' privacy in two key arenas; public and private. In the United States, the law limits anyone's privacy rights while that person is in public. When a celebrity—or any person—is in public or in a place where they cannot claim a **reasonable expectation of privacy**, anyone else generally has the right to photograph them. Because of this legal protection, paparazzi cluster in public places—outside buildings, on sidewalks—where they expect to see celebrities. The paparazzi then follow celebrities, sometimes quite closely and aggressively, for “candid” photos. In most situations, this behavior is legal, if not ethical.

A different legal and ethical issue surrounds photos taken in private settings, usually with the use of telephoto lenses. Celebrities—and others—can generally expect privacy when they are in places not normally seen or frequented by the public, including inside private buildings and on private property, if that property is far from public property. In the United States, it is usually illegal to take photos of individuals in private places, at least if they have taken steps—closing curtains or building fences, for instance—to try to gain privacy. Nevertheless, many paparazzi continue to try to photograph celebrities wherever they are.

Diana, Princess of Wales, was a prime target of paparazzi during and after her marriage to Britain's Prince Charles. From the time of her marriage to Charles in 1981, celebrity-oriented media followed Diana's every move. After the couple's separation and divorce, paparazzi attempted to get photos of Diana with the men she dated. In August 1997 she and her boyfriend, Dodi Fayed, were killed in Paris when their car crashed as their driver attempted to evade paparazzi on motorcycles.

Worldwide outrage against the paparazzi was immediate, with editorials in the United States calling them “vultures,” “bottom feeders,” “jackals,” and “reptilian.” Diana's brother confronted the issue directly, saying, “I always believed the press would kill her in the end. But not even I could imagine that they would take such a direct hand in her death as seems to be the case. . . . It would appear that every proprietor and editor of every publication that has paid for intrusive and exploitative photographs of her, encouraging greedy and ruthless individuals to risk everything in pursuit of Diana's image, has blood on his hands today” (Sharkey, 19). Although criticism muted somewhat when it was determined that Diana's driver—who was also killed—was drunk and driving at up to 120 miles per hour, paparazzi generally had suffered a substantial blow to their already poor reputation.

The months following the Princess of Wales's death saw legislative attempts to curtail paparazzi activity in the United States. In California, one bill would have barred photographers from going within 15 feet of unwilling subjects, and state senator Tom Hayden, the ex-husband of actress Jane Fonda, suggested licensing photographers and creating a “Commission of Inquiry into Paparazzi Behavior.”

In the U.S. House of Representatives, Representative Sonny Bono, himself a celebrity and paparazzi target, introduced the “Protection from Personal Intrusion Act” just 10 days after Princess Diana’s death. This legislation barred “harassing” behavior, defined as following a victim who had a reasonable expectation of privacy, for the purposes of taking a photo, video, or sound recording that would then be sold for profit. The punishment would have been between one and 20 years in prison. The following year, after Bono’s death in a skiing accident, U.S. senators Russ Feingold and Orrin Hatch introduced the “Personal Privacy Protection Act,” which would have outlawed following someone with the intent to take a photo for later commercial gain, when that following caused fear of bodily harm to the subject. While none of these bills at the state or federal level became law, they demonstrated the concern that lawmakers had with paparazzi and invasions of privacy.

California did, however, react to Princess Diana’s death by redefining existing privacy laws. Trespass and intrusion laws were changed in 1998 to include an offensive physical or electronic trespass or assault “with the intent to capture any type of visual image . . . [of another person] engaging in a personal or familial activity” (Invasion of Privacy to Capture Physical Impression). In 2006 that law was amended specifically in reaction to several incidents involving celebrities and paparazzi. The amended statute—signed by Governor Arnold Schwarzenegger, himself a paparazzi target—increased penalties to three times the actual damage caused by the incident and forfeiture of any money made from sale of photographs or video from the incident. The changes also made publishers—not just paparazzi—liable. A number of legal scholars have suggested that the statute as amended violates the U.S. Constitution.

See also: **Clinton-Lewinsky scandal; Confessional culture; Constitutional protections; Journalism**

Suggested Reading: Brown, William J., Michael D. Basil, and Mihai C. Bocarnea. “Social Influence of an International Celebrity: Responses to the Death of Princess Diana,” *Journal of Communication* 53 (2003): 587–605; Howe, Peter. *Paparazzi: And Our Obsession with Celebrity*. New York: Artisan Books, 2005; “Paparazzi on the Prowl,” *Time* (April 14, 1961): 81; Sharkey, Jacqueline. “The Diana Aftermath,” *American Journalism Review* 19 (1997): 19; Wober, J. Mallory. “A Feeding Frenzy, or Feeling Friendly? Events after the Death of Diana, Princess of Wales,” *Journal of Popular Culture* 34 (2000): 127–134.

Elizabeth Blanks Hindman

***Paris Adult Theatre I v. Slaton*, 413 U.S. 48 (1973)**

In *Paris Adult Theatre I v. Slaton*, 413 U.S. 48 (1973), the United States Supreme Court decided the validity of an injunction against the showing of allegedly obscene movies in adult theaters. Writing for the majority, Chief Justice Warren Burger decided that the Constitution did not prevent the state of Georgia from regulating allegedly obscene material shown to the public in an adult theater, so long as the Georgia regulations met First Amendment obscenity standards as required by the Supreme Court’s decision in *Miller v. California*, 413 U.S. 15 (1973).

The case arose over the ongoing showing of allegedly adult, obscene movies by two Atlanta, Georgia, movie theaters. The state of Georgia sought to have the

showing of these films halted by filing an injunction with the court. The evidence revealed that the two theaters were clearly marked as adult movie theaters, and there was no evidence suggesting that minors were either allowed in or excluded from the commercial theaters. Upon viewing the films, the Georgia Supreme Court decided, "The films in this case leave little to the imagination. It is plain what they purport to depict, that is, conduct of the most salacious character." That court found that the films were "hard core pornography," and that the showing of the films could be stopped by an injunction "since their exhibition is not protected" by the First Amendment. After a series of decision in the state courts of Georgia, the issue found its way to the United States Supreme Court.

Chief Justice Burger began by insisting that the Supreme Court did not want "to tell the States what they must do, but rather to define the area in which they chart their own course in dealing with obscene material. This Court has consistently held that obscene material is not protected by the First Amendment as a limitation on the state police power by virtue of the Fourteenth Amendment."

He further stated the majority "categorically disapprove the theory . . . that obscene, pornographic films acquire constitutional immunity from state regulation simply because they are exhibited for consenting adults." He pointed to "an unbroken series of cases extending over a long stretch" that "the primary requirements of decency may be enforced against obscene publications." Thus, from the very beginning, it was clear that Chief Justice Burger was not prepared to unconditionally protect the constitutional right of adults to watch pornographic films in a commercial, public movie theater.

To undercut the protection for pornography, Chief Justice Burger emphasized that "there are legitimate state interests at stake in stemming the tide of commercialized obscenity, even assuming it is feasible to enforce effective safeguards against exposure to juveniles and to passersby." Focusing on this issue, he listed the following as legitimate state interests at stake: "the interest of the public in the quality of life, the total community environment, the tone of commerce in the great city centers, and possibly, the public safety itself." To bolster the importance of limiting pornography to protect this final interest, Chief Justice Burger cited a congressional study establishing "at least an arguable correlation between obscene material and crime."

In response to the challenge that there was not any conclusive evidence establishing a measurable effect on crime or any harm to society from movies such as this, the majority responded by deferring to the legislative branch on policy issues. The Supreme Court refused to extend itself into the realm of making judgment calls based on statistics, and it declined the opportunity to question the methodology of the Georgia legislature in formulating its justifications for reducing pornography in the public sphere. As Chief Justice Burger phrased it, "We do not demand of legislatures scientifically certain criteria of legislation."

Focusing on privacy, Chief Justice Burger also noted the diminished privacy interest of an individual outside one's **home**. Quoting a sociologist, he noted that although the privacy within one's home should not be disturbed, the privacy of all other individuals in the public is affected if we allow pornography to run rampant in theaters. Thus, despite the argument in favor of the private right to view movies in public, the Supreme Court also focused on the alternative privacy right of the

vast majority of the public to be free from pornography in the public sphere. This was a new angle to the Supreme Court's discussion of the right to view pornography, and it proved to be persuasive.

Further, the Supreme Court also rejected that "totally unlimited play for free will" was a constitutionally recognized right for individuals to exercise. Instead, the majority focused on the numerous ways in which the First Amendment is limited despite its seemingly "absolute" nature. This restriction of rights carried on to the majority's classification of the movie theater in this case. The Supreme Court answered the claim that the right to view a pornographic film did in fact constitute a private, and not a public activity, by concluding that "the idea of a 'privacy' right and a place of public accommodation are, in this context, mutually exclusive."

Ultimately, the majority found that the state regulation would be legitimate so long as the Georgia regulation complied with the holding in *Miller v. California*, concerning the three-part test for constituting obscenity. Summarized, these three parts are (1) the work, taken as a whole, appeals to the prurient interest; (2) the work depicts, in a patently offensive way, sexual conduct specifically defined by applicable state law; and (3) taken as a whole, the work lacks serious literary, artistic, political, or scientific value. The majority reaffirmed "obscene material has no protection under the First Amendment." To this end, the majority "directed [its] holdings, not at thoughts or speech, but at depiction and description of specifically defined sexual conduct that States may regulate within limits designed to prevent infringement of First Amendment rights."

See also: **Constitutional protections; Gender; *Osborne v. Ohio*, 495 U.S. 103 (1990); *Stanley v. Georgia*, 394 U.S. 557 (1969); Women and privacy**

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hall, Kermit L. *Conscience, Expression and Privacy: The Supreme Court in American Society*. New York: Garland, 2000; Smith, Robert Ellis. *Compilation of State and Federal Privacy Laws*. Providence, RI: Privacy Journal, 1992; Turkington, Richard C., and Allen, Anita L. *Privacy Law: Cases and Materials*. St. Paul, MN: West, 2002.

Ryan C. Hudson

Partner notification

Historically known as contact tracing and modernly renamed partner counseling and referral services (PCRS), partner notification generally refers to the practice used by public health officials or counselors to assist persons with infectious conditions to identify and notify their unknowing sexual, drug-sharing, or other partners of the partner's potential risks of infection. Partner notification involves significant privacy concerns among individuals and their partners because (1) individuals infected with various conditions (e.g., HIV/AIDS, other sexually transmitted diseases, emerging infections like SARS) are asked to identify their partners, which itself is



private information; and (2) partners are informed of their potential exposure to infectious agents in ways that may infringe on the health information privacy interests of the infected individuals. To remedy these privacy concerns, public health authorities work to protect individual privacy while providing enough information to partners to allow them to avoid infection.

Partner notification is a common **public health and safety** intervention because it offers significant benefits to individuals with infectious conditions, their partners, and the community. Through partner notification, persons who may be unaware are informed of their potential exposure to infectious conditions. Notified partners are often advised to be tested, counseled about safe behaviors to avoid future exposures, and in some cases, offered medical treatment. Partner notification begins when persons infected with identified conditions are encouraged by public health authorities or private health care providers to volunteer specific information about their partners. Under this protocol, the infected individual, a doctor, or a public health counselor then informs known partners of their possible exposure to an infectious condition. Newly informed partners are referred for counseling, testing, and social and medical services as necessary, thus completing the partner notification cycle.

Partner notification as a public health practice has traditionally recognized that maintaining patient **confidentiality** is critical in accomplishing public health objectives and respecting individual autonomy. Still, the privacy implications underlying partner notification are profound. Individuals with an infectious disease may resist participating in partner notification efforts because they believe identifying their partners will or may result in a breach of privacy. Principles of law and ethics, however, suggest that individual privacy rights do not extend so far as to jeopardize the health of others. It is illegal and unethical, for example, for a person with HIV to knowingly expose others to this condition through unsafe sexual or needle-sharing practices. These partners have a right to know about those risks of which they are otherwise unaware. Ideally, partner notification is designed to be conducted anonymously—that is, the identity of the infected individual is not released to the partner. Partner notification counselors are required to maintain the privacy and security of an individual's identity under federal and state constitutional, statutory, and regulatory laws. This does not mean that the partner will not be able to identify the infected individual. For example, a spouse may be able to reasonably conclude that her husband has exposed her to HIV when anonymously informed of this situation by a public health counselor. Although not the intent of the counselor, the result is that private health information (the husband's HIV status) is disclosed and his privacy interests are infringed.

Partner notification is thus challenged based on the privacy interests of those infected and on the grounds that it violates constitutional, statutory, and common law privacy protections. These challenges regularly fail in light of the overriding governmental interests in preserving the public health, the voluntary nature of partner notification, and the non-applicability of privacy protections that are usually trumped by legislative or other legal provisions authorizing partner notification.

See also: **Anonymity; Blood testing; Health privacy**

Suggested Reading: Hodge, James G., and Lawrence O. Gostin. "Handling Cases of Willful Exposure through HIV Partner Counseling and Referral Services," *Rutgers Women's Rights Law Reporter* 22 (2001): 45–62; Hodge, James G., and

Lawrence O. Gostin. "Piercing the Veil of Secrecy in HIV/AIDS and Other Sexually Transmitted Diseases: Theories of Privacy and Disclosure in Partner Notification," *Duke Journal of Law and Gender* 5 (1998): 9–88.

James G. Hodge, Jr.

Password protection

Passwords are a commonly used mechanism for controlling access to secured resources. Users who have valid passwords can identify themselves to the system and gain access to the secured area. The system simply denies access to individuals without the proper credentials. Passwords, although commonly used in **computer** systems, date from ancient times. Soldiers guarding protected gates would challenge any person who approached them for a password. Only those who were able to give the appropriate response were allowed to "pass" through. In contemporary times, passwords form one of the cornerstones of electronic security and serve as a primary tool in preventing unauthorized access to secure resources such as file systems, **electronic mail** servers, databases, networks, bank accounts, **automatic teller machines (ATMs)**, and the like.

Each access-restricted resource typically has an access control matrix, which is essentially a list of identities; successful corroboration of an identity with the help of the password allows a user to gain access to that resource. Most systems do not store the actual passwords in plaintext for obvious security reasons; instead, systems store the passwords in a cryptographically protected format. One such format is a cryptographic hash such as SHA-1. Although there are several established ways for proving identity using a password, the simplest way involves a user sending the password in plaintext over an encrypted channel to the secure resource, which then locally computes the hash of the password and compares it with the stored value. More sophisticated methods include challenge-response based protocols and zero-knowledge proofs.

Although password-based protection is widely used in computer system security, this kind of protection is vulnerable to a number of attacks. Most commonly, password-based protection systems are prone to guessing or to dictionary-based attacks since most people pick passwords that are easy to remember and therefore are easy for attackers to guess as well. Additionally, a number of social engineering-based attacks are also possible. For example, if a system forces the users to pick very complex passwords, many people will write them down on paper to keep them handy. If the system forces the users to change their passwords frequently, the users tend to re-use old passwords to avoid memorizing a new one each time. Thus a password protection scheme needs to maintain a fine balance between ease of use and security.

Password-based protection schemes, while widely used and very convenient, have some inherent limitations. These schemes place a large burden on individual users to maintain and protect their passwords from attackers. It is difficult for an individual user to remember and maintain several difficult-to-guess passwords and protect these from various social engineering and phishing attacks. More sophisticated identification schemes, which overcome some of the limitations of password-based protection schemes, involve **biometrics** or cryptographic **smart cards**.

See also: **Cryptography; Internet**



Suggested Reading: Brown, Allan S., Elisabeth Bracken, Sandy Zoccoli, and King Douglas. “Generating and Remembering Passwords,” *Applied Cognitive Psychology* 18 (2004): 641–651; Menkus, Belden. “Understanding the Use of Passwords,” *Source Computers and Security* 7 (1988): 132–136.

Maithili Narasimha

Paternity

There is a long history of legal precedents for paternity and privacy. As early as 1923, in *Meyer v. Nebraska*, the United States Supreme Court broadened the scope of the Fourteenth Amendment and established the tradition of procreative liberty, ruling that the state cannot interfere with one’s decision to establish a family. Further, *Pierce v. Society of Sisters* (1925) stated that parents can raise their children in the manner in which they see fit. There have also been numerous cases, such as *Skinner v. Oklahoma* (1942), *Griswold v. Connecticut*, 381 U.S. 479 (1965), *Eisenstadt v. Baird*, 405 U.S. 438 (1972), and *Carey v. Population Services International* (1977), that specified the private nature of the decision to use or not to use contraceptives. Two other landmark cases were *Stanley v. Illinois* (1972), which gave parents the fundamental right to associate with and raise their children, and *Moore v. City of East Cleveland* (1977), which stated that family can be defined more broadly than as a traditional nuclear family.

While these legal precedents have protected the idea of several types of privacy and several types of paternity issues, they have also been challenged. Recent issues have arisen because there are practices that explicitly ignore privacy issues, there are gaps in laws, different laws can contradict one another, or courts can interpret laws differently. Some laws explicitly ignore privacy issues and do not directly relate back to any legal precedent. For example, a violation of maternal and paternal informational privacy can be seen in one state’s in-hospital paternity establishment program, where a new mother’s mere mention of the name of a man as a possible father gets recorded by hospital personnel and passed on to the state office of child support enforcement, which then tracks down the man.

Another example is the 2001 Sexual History Newspaper Requirement in Florida, also known as the Tell All Adoption Law, or what critics called the “Scarlet Letter Law,” which was aimed at single mothers who were putting their babies up for **adoption** and were unsure of the fathers’ identities. In an advertisement, the mother had to disclose her name, age, height, hair and eye color, race, and weight; her child’s name, date and place of birth, and—if it were the address that was unknown—the father’s name. Moreover, the mother had to publish her sexual history: a description of every potential father and the dates and places of their sexual encounters. The ad had to run once a week for four weeks in a newspaper in each city or county in which conception might have taken place in the year before the child’s birth. The point of such a law was for the father to be able to claim the child before it was put up for adoption, but the ads did not produce any wayward fathers. Six mothers brought the first suit to court in 2002, and the judge denied the motion for a declaratory judgment. He held that the two mothers who had conceived as a result of rape were not subject to the law, but the law was constitutional for the other four women. In 2003, however, the Florida appeals court struck down the law.

There have also been attempts explicitly aimed at controlling paternity through the invasion of informational privacy. For example, Iowa anti-choice advocates videotaped women on their way to **abortion** clinics in 2002. In the same year, authorities in Storm Lake, Iowa, tried to get Planned Parenthood to turn over records of pregnancy tests because they were trying to find out about a dismembered newborn. Although Planned Parenthood refused, a judge upheld the subpoena on the grounds that pregnancy tests are not covered by doctor-patient **confidentiality** since nonmedical personnel can perform them. And in 2005, the Kansas attorney general sought to open medical records of two abortion clinics as part of his investigation of child rape and illegal late-term abortions. The records were not opened as the court decided in 2006 that this would be a breach of patient privacy under the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**.

Other legal decisions have sought to control paternity through the invasion of decisional privacy, or the freedom to make autonomous choices about our private lives. In opposition to U.S. Supreme Court decisions that procreation is a basic human right, in 2001 a Texas district judge threatened a life prison sentence and ordered a man not to have sex with anyone until he was married, expressing fear that he would be a deadbeat dad. Concurrently, the Wisconsin Supreme Court sustained a lower-court ruling that would jail a man for eight years if he fathered another child without proving that he could support all his children.

Laws also constrain decisional privacy and go against procreative liberty when they define who cannot be parents. There are restrictions on gay people who do not necessarily have legal recognition of their relationships with their children, such as non-biological mothers seeking second-parent adoption. Other examples may come from state law that can determine when natural parents are unfit. Further, in one child custody case, a father ordered genetic testing of the mother to see if she had certain diseases in efforts to define her as an unfit mother. Forced medical testing would also have been an incursion into the mother's physical privacy, as well as her informational and decisional privacy.

Finally, over the past ten years nearly every state or federal welfare program has included a family cap that prohibits an increase in benefits for additional children. Some states have proposed legislation offering incentives for men to get vasectomies, for women on welfare to use long-lasting contraceptives, and for recipients to participate in family planning counseling. Not only is this verging on invading physical privacy, especially for low-income and/or nonwhite individuals, but the women's informational privacy is also being breached through requiring them to divulge confidential information to the state in reporting whether they are sexually active and able to become pregnant. A 2002 Pennsylvania ruling, aimed at controlling paternity through forced procreation, gave a boyfriend the right to bar his former girlfriend from getting an abortion. The decision was eventually overturned, but critics remark that cases aimed at controlling fertility invade both physical and decisional privacy and ring of either positive or negative eugenics—promoting or deterring procreation among certain segments of the population. Defying *Pierce v. Society of Sisters* (1925), laws also exist that specify how to parent, leading to possible breaches of both physical and decisional privacy. Some states have laws on prenatal screening and can even charge a woman with “prenatal abuse” or



“wrongful life” if she refuses the testing or exposes her fetus to prenatal dangers. The United States Office of Technology Assessment also found that some health insurance companies have attempted to withdraw their coverage if the women involved did not get prenatal testing. Along the same lines, some believe that a woman’s physical privacy is breached when her body is no longer considered a private sphere through such procedures as fetal surgery, where she becomes secondary as her health is put aside and the fetus gains almost full patient rights through medical and legal representation.

In other instances, it has been difficult to apply extant court cases to new practices. For example, there have been different interpretations as to who is actually the mother in surrogate motherhood—is it the adoptive mother, the genetic mother (egg donor), or the gestational mother? In another example, employers may collect genetic information about employees and their children, yet there are few laws about access and disclosure. Further, research studies may obtain information about a person that includes information about the person’s family members without their consent. As a side note, some also worry about breaches in privacy given that data from these studies can be hacked.

The above cases and examples outline breaches of privacy regarding paternity; there are also practices that attempt to protect this kind of privacy, although some have come into question. In 1998 a Georgia court sealed information about a woman who claimed she was the illegitimate child of a celebrity by citing invasion of privacy and the resulting embarrassment, yet the Georgia Supreme Court overruled this decision. Others claim that some privacy protections for paternity may have negative repercussions, such as the application of patient privacy in the delivery room whereby the medical staff may not know that the woman giving birth conceived through ovum transfer. This can cause confusion with blood typing and result in more procedures for mother and baby.

See also: **Gender; Medical privacy; Women and privacy**

Suggested Reading: Casper, Monica. *The Making of the Unborn Patient: A Social Anatomy of Fetal Surgery*. New Brunswick, NJ: Rutgers University Press, 1998; Freund, G. G., C. Finke, and S. A. Kirkley. “Anomalous ABO Inheritance Explained by Ovum Transplantation,” *Transfusion* 35, no. 1 (1995): 61–62; Pollitt, Katha. “Slut Patrol,” *Nation* 275, no. 10 (2002): 30; Rae, Scott B. *The Ethics of Commercial Surrogate Motherhood: Brave New Families?* Westport, CT: Praeger, 1994; Rothstein, Mark A. “Preventing the Discovery of Plaintiff Genetic Profiles by Defendants Seeking to Limit Damages in Personal Injury Litigation,” *Indiana Law Journal* 71 (1995–1996): 878–908; Shinaman, Aileen, Lisa J. Bain, and Ira Shoulson. “Preempting Genetic Discrimination and Assaults on Privacy: Report of a Symposium,” *American Journal of Medical Genetics* 120A (2003): 589–593.

Ophra Leyser

Patient rights

In the clinical context, the right to privacy refers to a myriad of expectations that include the **right to be let alone**, the right to physical privacy, the right to have the **confidentiality** of personal and sensitive information maintained, the right not to have medical procedures imposed without consent, the right to have treatment choices respected and not interfered with, the right to access personal information in

a medical record, and the proprietary right to aspects of a person's identity such as genetic information, pictures of oneself, and biological material that may lead to progeny (sperm, ova, and embryos). Privacy-related rights are protected by common law and federal and state regulations such as the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**. Agencies such as the Joint Commission on Accreditation of Healthcare Organizations require affiliated institutions to comply with patient privacy guidelines. Patient bills of rights have been adopted by such entities as the American Hospital Association and introduced for legislation in the United States.

The U.S. Constitution does not explicitly protect privacy, but several constitutional amendments, including the First, Third, Fourth, and Ninth Amendments are interpreted to create various privacy rights. A federal commitment to individual privacy is reflected in state privacy laws and case laws pertinent to patient care. In *Sanchez-Scott v. Alza Pharmaceuticals*, a woman claimed her privacy was invaded when a male pharmaceutical representative was in the examination room during a breast exam. Her oncologist misled the patient by suggesting that the representative was there in a clinical capacity. The California Appeals Court agreed that her privacy rights had been breached.

Patients reasonably expect health care providers to respect their privacy for at least two reasons. First, health care providers need private information for the purpose of treating patients. **Disclosure** of information to anyone who has a questionable role or no role in patient care would be exploitative. Second, patients will not seek help from clinicians if they do not believe sensitive information is kept in confidence; therefore, patient privacy is pertinent to **public health and safety**.

In the interest of their health, patients grant health care providers access to private domains, rendering patients vulnerable to exploitation if health care professionals do not respect patient confidentiality. Confidentiality is a centuries-old medical obligation reflected in the Hippocratic Oath: "What I may see or hear in the course of the treatment . . . which on no account one must spread abroad, I will keep to myself." The Health Insurance Portability and Accountability Act (HIPAA) requires health care providers to obtain patients' consent to disclose or use **personally identifiable information** (e.g., name and date of birth) or to release medical information to entities not directly involved in medical services or billing. HIPAA attempts to balance good patient care, which requires patients to relinquish some of their privacy, with patients' interests in keeping such information confidential. The act requires health care institutions to implement reasonable protections for privacy and confidentiality, and to inform patients of their privacy rights and the institution's privacy practices.

There are five realms of patient privacy that receive special attention in the law and bioethics: reproductive issues, end-of-life issues, infectious diseases, mental health issues, and genetic issues. *Griswold v. Connecticut*, 381 U.S. 479 (1965), by supporting the right of clinicians to provide information and instruction about contraception, established that state interference in reproductive decisions often violates a patient's right to privacy. An exception is when a woman's privacy right competes with the state's interest in protecting a viable fetus. According to *Roe v. Wade*, 410 U.S. 113 (1973), state **abortion** laws must protect a woman's right to an abortion until the fetus can live outside the woman's womb, or when continuing the pregnancy threatens the life or health of the woman.



Patient information about abortion procedures is considered highly sensitive. When, in preparation for a trial, the Department of Justice subpoenaed records of patients who underwent abortion procedures, the U.S. Court of Appeals ruled that the damage to patients and facilities where abortions were performed outweighed the probative value, even when identifying features were removed from the records.

Privacy rights are also often invoked regarding end-of-life decisions. The Patient Self-Determination Act of 1991 and state natural death acts protect patients' rights not to have treatments imposed against their wishes, and pertain especially to end-of-life treatment decisions. Patients may refuse resuscitation, tube feeding, dialysis, and ventilators in order to allow a natural death to occur.

More controversial is assisted suicide, in which competent patients ask physicians to write prescriptions for lethal medications in order to end their own lives. In the United States, Oregon is the only state where physician-assisted suicide is legal for terminally ill patients. Cases have been brought to other states' supreme courts in attempts to liberalize patient rights. In 1997, Charles E. Hall, a patient with HIV, asked the Florida court to place an injunction that would stop the state's attorney from prosecuting Mr. Hall's doctor if he helped Mr. Hall commit suicide in the future. The injunction was granted in the lower court by appealing to Florida's privacy law that states "every natural person has the right to be let alone and free from governmental intrusion into his private life." The Florida Supreme Court ultimately disagreed with the lower court. The appeals for privacy in end-of-life decisions are similar to those for reproductive and sexual privacy practices: the manner in which one lives one's life is personal, and individuals have the right not to have their end-of-life choices interfered with.

Patients expect higher standards of privacy and confidentiality with regard to information about infectious diseases, particularly sexually transmitted diseases, and psychiatric treatment. This is because of the potential harms that can come from disclosure, which include stigmatization, discrimination within and outside of the workplace, and inability to qualify for health insurance. Many state laws stipulate that health care institutions must ask patients for special authorization to release HIV, substance abuse, and mental health information.

There are limits to privacy protection when a person's disease may impact the health of others. Infectious diseases such as tuberculosis and HIV must be reported to local public health agencies for the purpose of **surveillance**, investigation, and intervention, and these disclosures need not be authorized by the patient. Still, only minimal patient identifiable information should be disclosed. In these cases the public health interest outweighs the patient's right to privacy.

Genetic information and testing also heighten privacy concerns. A genetic test might be used to predict a person's susceptibility to a disease such as breast cancer or Huntington's disease. Without strict confidentiality standards, insurance companies or employers might discriminate against patients based on predilection for a disease the person does not even have and may never contract. A number of states have anti-genetic-discrimination laws, and federal bills have been introduced in the Senate and House. Legal protection is important because patients may want genetic information to make prophylactic treatment choices or, as in the case of Huntington's

disease for which there is no cure, to make life plans. Such information impacts not only the patient but other family members who may carry the same gene.

Similarly, privacy is important in prenatal genetic testing. Parents' choices to terminate or continue pregnancies based on the results of genetic tests are considered as private as other reproductive decisions. Privacy issues are also raised in predictive genetic testing, where a female patient may need genetic information from a relative to determine her predilection for a specific disease such as breast cancer. The patient's family member may not want to know if she has the breast cancer gene, especially if she is currently healthy. Further, even without testing family members, when one family member confirms he or she has a gene associated with a disease, it raises questions about the genetic disposition of other family members. Because of these complicated patient right and privacy issues, genetic counseling is recommended for all patients who seek prenatal or predictive genetic testing.

Privacy is an essential patient right because without it, patients might be reluctant to share personal and sensitive health information with their care providers. In this way, patients' rights to privacy help protect their health.

See also: **Health privacy**

Suggested Reading : Allen, Anita. "Privacy in Health Care." In Stephen G. Post (ed.). *Encyclopedia of Bioethics*, 3rd ed., vol. 4, pp. 2120–2130. New York: MacMillan Reference, 2004; Beauchamp, T. L., and J. F. Childress. *Principles of Biomedical Ethics*, 5th ed. New York: Oxford University Press, 2001; *HIPAA Privacy Rule and Public Health: Guidance from CDC and the U.S. Department of Health and Human Services*. <http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm>. Online, December 2005; Winslade, William J. "Confidentiality." In Stephen G. Post (ed.). *Encyclopedia of Bioethics*, 3rd ed., vol. 1, pp. 494–503. New York: MacMillan Reference, 2004.

Denise M. Dudzinski

Payton v. New York, 445 U.S. 573 (1980)

In January of 1970, after two days of investigation, New York detectives had assembled sufficient evidence to establish probable cause to believe that Theodore Payton had murdered the manager of a gas station a few days earlier. On January 15, 1970, six officers arrived at Payton's **home** with the intent to arrest him without a warrant. Although there were significant signs and noise indicating that someone was in the residence, there was no answer to the officers' knock on the door. Emergency assistance arrived a short time later, and the officers used crowbars to enter the residence. No one was home, but in **plain view** was a shell casing that was seized and later admitted into evidence against Payton at his trial. Payton later surrendered and moved to suppress the casing. At the time in New York, there existed a statute that allowed police officers to enter a private residence without a **search warrant** and with force, if necessary, to make a routine felony arrest.

The trial judge held that the warrantless entry into Payton's home was allowed under the New York Code of Criminal Procedure. Furthermore, the judge held that the shell casing seized in plain view was properly seized. The rationale behind the judge's decision was that he found exigent circumstances justified the officers' failure to announce their presence before entering the residence. However, the judge failed

to decide whether the circumstances justified the failure to obtain a warrant, and rather concluded that the state statute supported the entry.

The issue before the Supreme Court was whether the New York statute was a violation of **constitutional protections**. The Court decided that the statute was, in fact, unconstitutional. The Fourth Amendment, made applicable to the states through the Fourteenth Amendment, prohibits police from making a warrantless and nonconsensual entry into a suspect's home to make a felony arrest. The Court's opinion pointed out that it was arguable that the warrantless entry to arrest Payton might have been justified by exigent circumstances. However, none of the New York courts relied on such justification. In fact, the New York statute circumvented the justification and treated such arrests as routine arrests.

Physical entry of the home, and the violation of the right to be secure in one's own house, is the chief evil against which the wording Fourth Amendment is directed. Entries into a house without a warrant are presumptively unreasonable. The protection of the Fourth Amendment of an individual's privacy is clearly in regard to the dimension of one's individual home. A person can retreat into his or her home and maintain a **reasonable expectation of privacy**. Without any exigent circumstances, a person is safe in his or her home, and the person's interest in the sanctity of his or her home outweighs governmental interests. In this case, there existed no exigent circumstances. Rather, there existed only a state statute that circumvented the requirement of exigent circumstances.

See also: California v. Ciraolo, 476 U.S. 207 (1986); *Chimel v. California*, 395 U.S. 752 (1969); *Curtilage*; *Harris v. United States*, 331 U.S. 145 (1947); *Trespass*; *United States v. Dunn*, 480 U.S. 294 (1987); *Warden v. Hayden*, 387 U.S. 294 (1967); *Weeks v. United States*, 232 U.S. 383 (1914)

Suggested Reading: Barte, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hubbard, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

Matthew M. Dwyer

Peer-to-Peer (P2P) technologies

Developed for their decentralized capabilities, Peer-to-Peer (P2P) technologies are **computer** networks that use nodes instead of the classic server-and-client model. These nodes are individual computers (peers) functioning together as equals, with both server and client forming a P2P network. One of the key aspects of this model is its distributive nature. That is, because the users are acting as servers as well as clients, the burden of bandwidth, storage space, and computing power is redistributed among the peers active on the network. This redistribution also eliminates single points of failure in the system because the network is not

relying on a central server to store and distribute data. Because of this aspect, Peer-to-Peer technologies have recently been used in the realm of scientific research. These networks can be used to run large programs or process large amounts of data.

A P2P network gives a user the ability to share any information stored on his or her hard drive with any other user on the network. With the rise of Napster in 1999 and its eventual collapse in 2001, P2P technologies became famous for enabling the sharing of music in the form of MP3s. Since Napster's demise, P2P networks have expanded to become a black market for the distribution of software, movies, e-books, pictures, and other unlicensed digital media. In the late 1990s, the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) led the fight to eradicate file sharing. They saw the use of P2P networks for these purposes as a clear violation of intellectual property rights and a direct threat to the future of their industries. Others in the technology community cited the U.S. Supreme Court case of *Sony Corp. v. Universal City Studios Inc.* (the Betamax decision), which essentially placed the burden of the law on the copies and copiers of intellectual property and not on the medium on which they were copied, indicating that individuals are responsible for piracy, not the P2P network.

P2P technology can be extremely hazardous to those using it. P2P networks can leave the computers in a network vulnerable to hackers and a number of forms of computer attacks. When connected to the P2P network, anyone with the right tools can access **personally identifiable information** that may be stored on a computer, such as **credit card** numbers, **passwords**, and personal correspondence. From copyrighted material being openly available to others to viruses and spyware, there have been a host of problems associated with this sharing medium.

P2P and other decentralized networks of peers have been used since Usenet in 1979 and FidoNet in 1984 and have grown considerably in popularity and use since their inception. With the advent of Voice-over-**Internet** Protocol (VoIP) and academic P2P networks such as LionShare, P2P technologies are becoming more mainstream and secure but are still subject to many privacy and security concerns.

Suggested Reading: Gurak, Laura. *Cyberliteracy: Navigating the Internet with Awareness*. New Haven, CT: Yale University Press, 2001; Schoder, Detlef, and Kai Fischbach. "Core Concepts in Peer-to-Peer (P2P) Networking." In Remesh Subramanian and Brian Goodman (eds.). *P2P Computing: The Evolution of a Disruptive Technology*, pp. 1–27. Hershey, PA: Idea Group.

Ian W. Staples

Pen register

The term "pen register" refers to a device or process that records or decodes all non-content dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted. The phrase "trap-and-trace" references a device or process that captures all non-content incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication. In telephone **surveillance**, pen registers record the telephone numbers of outgoing calls made from a

phone line, and trap-and-trace devices or processes record the telephone numbers of incoming calls made to a phone line. These devices are almost always referred to in tandem, and are treated as one in legal literature.

In 1979 the Supreme Court held that the use of these devices did not involve the Fourth Amendment since the devices do not intercept or acquire the contents of communications as defined by 18 U.S.C. §2510(8). These devices are capable only of receiving signaling information like pulses and tones, not sound. In fact, these data are placed on a different channel from the voice conversations, so the resulting technological barrier prevents the device from inadvertently accessing phone conversations.

Congress responded to the potential privacy issues resulting from unwarranted intrusions caused by the government's use of these devices with the **Electronic Communication Privacy Act (1986)**. The ECPA establishes that law enforcement officials must request authorization from a judge prior to using these devices on a specific target. Authorization for installation will be granted whenever the government certifies that the information likely to be obtained is relevant to an ongoing criminal investigation. Probable cause is not required. Nor is there any requirement that the target of the investigation ever be notified that such a device was used or that an application was ever sought. Furthermore, since the Fourth Amendment is not involved, there is no exclusionary remedy for unlawful usage.

With the advent of technology and the evolving need for **Internet** surveillance, Congress passed Section 216 of the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)** in an effort to update pen-register legislation for the Internet age. Section 216 modified certain ECPA provisions so that pen registers and trap-and-trace devices applied to Internet surveillance. The act required some mandatory reporting on the use of government-installed pen registers, but it also significantly expanded the government's surveillance powers by allowing for nationwide orders. These regulations extended the content and non-content theory by analogy to all electronic communications, including Internet communications. In other words, the content of telephone and Internet communications is now governed by the full warrant standards applicable to general wiretaps, whereas the non-content information like dialing, routing, addressing, or signaling information is governed by the pen register law. The government has developed new surveillance technology and methods for obtaining Internet pen register information, such as the **Carnivore** (DCS1000) system. However, the government usually just requests the information directly from an Internet service provider.

See also: **Anti-wiretap statutes; Electronic surveillance; Wiretapping**

Suggested Reading: Dash, Samuel, Richard Schwartz, and Robert Knowlton. *The Eavesdroppers*. New Brunswick, NJ: Rutgers University Press, 1959; Dempsey, James X. "Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy," *Albany Law Journal of Science & Technology* 8 (1997): 70–71; Diffie, Whitfield, and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press, 1999; Electronic Privacy Information Center. <http://www.epic.org>. Online, March 2006; Ottensmeyer, Edward J., and Mark A. Heroux. "Ethics, Public Policy, and Managing Advanced Technologies: The Case of Electronic Surveillance,"

Journal of Business Ethics 10 (1991): 519–526; Schneier, Bruce, and David Banisar. *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance*. Hoboken, NJ: Wiley, 1997.

Jill Joline Myers

Personally identifiable information

Personally Identifiable Information (PII) is a unique piece of data or indicator that can be used to identify, locate, or contact a specific individual. Permitting identification or recognition of a unique person is what distinguishes PII from other types of personal information (information that may be sensitive, embarrassing, or offensive that an individual may wish to control, keep private, or not have disclosed to others without consent).

Examples of PII are wide ranging and include an individual's name; geographic, physical, or postal address; phone number; **electronic mail** address; bank or credit account numbers; and **Social Security number**. PII is sometimes defined by exclusion. For example, PII is not data that are merely statistical or aggregate information that does not identify a particular person. Information that is not directly linked to an individual, such as any information that is collected anonymously, is not categorized as PII. Some examples of information that can be collected anonymously include statistical information, state of residence, age, gender, race, purchases, or salary.

Personal information such as last names, fingerprints, personal profiles, or **Internet** Protocol addresses are not by themselves PII. However, personal information from various sources can be pieced together to create PII. For example, an Internet Protocol address does not, by itself, identify a specific person. However, if the Internet Protocol address is combined with an Internet service provider's customer records that show which customer has been assigned to that address, the combined information becomes PII and may allow someone to identify, locate, or contact that specific individual customer.

PII is collected, stored, used, and shared by individuals, organizations, and institutions, including government entities. Exchange of PII is necessary to facilitate many activities, communicate, obtain benefits and services, and transact business. PII is necessary to performing various economic functions related to an individual, such as payroll, human resources, marketing, and banking.

While PII has always been in existence and used in a variety of contexts, its value as a commodity has increased with advances in information technology. The Internet and other technologies, including advancements in database and **data-mining** software and processes, have enabled faster and easier collection and exchange of PII. In addition, emerging information technologies have expanded the uses and value of PII in both commercial and noncommercial applications. Emerging technologies have permitted the development of new business models, including **data brokers**, and have facilitated the ability of marketing companies to share PII for profit. As a result, there has been an explosion in targeted marketing techniques that may be considered intrusive and may involve individuals' privacy rights. Examples include **spam** e-mail and **telemarketing**. Moreover, emerging technologies have expanded the definition of PII in the digital environment to include information that, if disclosed, could result in identifying an individual physically or electronically.



PII is used in combination with other information to predict an individual's tastes, interests, and future behavior. Predictive analysis and profiling increasingly have been employed in the commercial and law enforcement sectors. PII, combined with other personal information such as consumer purchases, can create an accurate electronic dossier or digital persona that can forecast how an individual might spend money or leisure time, how an individual may be inclined to vote, or an individual's propensity to commit crimes. Thus, PII used in this context has great commercial, governmental, and political importance.

While much PII is voluntarily disclosed by the person to whom it pertains, PII can also be disclosed and used without the person's knowledge or consent. There are serious ramifications to that person's privacy when PII is maintained by entities that do not take adequate security measures to protect personal information from unauthorized use or disclosure. Such acts may result in **identity fraud**, stalking, or other crimes as well as possible injury to a person's physical safety, finances, or reputation.

PII is stored on various objects like Social Security cards, drivers' licenses, passports, and **credit cards**. Because of the proliferation of new technologies and business models, PII will be increasingly stored on biometric devices, **smart cards**, and even medical emergency devices (for example, **radio frequency identification (RFID)** chips, that may be carried by or implanted in patients). These media may employ security measures that reduce the possibility that the included PII will be compromised and subject to unauthorized use or disclosure.

There is no comprehensive federal law protecting the privacy of PII. Further, there are slight variations in the meaning of PII when used in different legal contexts. The term "personally identifiable information" is mentioned in a number of federal and state statutes, but federal law provides few actual definitions. The Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 provides one useful explanation. It describes PII as "information concerning an identified individual that, if disclosed, will result in contacting or identifying such an individual physically or electronically." The U.S. Department of Education's definition of PII, as applied to student educational records under the **Family Educational Rights and Privacy Act (FERPA)**, includes "(a) The student's name; (b) the name of the student's parent or other family member; (c) the address of the student or student's family; (d) a personal identifier, such as the student's social security number or student number; (e) a list of personal characteristics that would make the student's identity easily traceable; or (f) other information that would make the student's identity easily traceable." The **Cable Communications Policy Act of 1984** does not define PII, but it states that PII "does not include any record of aggregate data which does not identify particular persons."

In passing the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**, Congress recognized that medical treatment requires the exchange of personally identifiable, often highly sensitive, medical information. The HIPAA Privacy Rule defines "individually identifiable health information" as data that involve an individual's physical or mental condition or payment for health care services and that also identifies the individual or creates "a reasonable basis to

believe the information can be used to identify the individual.” In addition to defining this form of PII, HIPAA mandated that every covered service provider provide “reasonable and appropriate administrative, technical and physical safeguards to ensure the integrity and **confidentiality** of the information.” The HIPAA Privacy Rule provides patients the right to access and amend their records. Patients also have the right to ask for **disclosures**, and limit the use and disclosure of their personal health records by health care entities.

The **Financial Services Modernization Act of 1999**, otherwise known as the Gramm-Leach-Bliley Act (GLBA), provides certain protections for the collection, use, and disclosure of customers’ personal financial information by financial institutions and others who receive such information. While GLBA does not expressly define protected financial information, financial records often contain data that are capable of identifying a specific person, and thus this information constitutes PII. Under the GLBA, consumers must be given notice as to the financial institution’s information-sharing policies and practices. Consumers also have the right to limit some, but not all, sharing of their personally identifiable financial information with others.

The **Children’s Online Privacy Protection Act (COPPA)** was enacted to limit the information, including PII, which commercial websites may collect from children online. Operators of commercial websites must provide clear and unambiguous notice of their privacy policies. COPPA also requires businesses to obtain parental consent to collect, store, and use PII from children.

In this age of global commerce, domestic companies are increasingly seeking efficient data processing outside the United States. As a result, a number of companies have out-sourced business processes to vendors in foreign countries, many of which have limited or no privacy protections for PII. These vendors are contracted to process a wide range of records containing PII, including medical research data and tax return information. Because out-sourced PII may be more vulnerable to unauthorized use or disclosure resulting from limited foreign protections, there is increasing concern that regulatory mechanisms need to be updated to protect PII in the global digital environment.

See also: **Anonymity; Biometric identifiers; Computers**

Suggested Reading: Garfinkle, Simson. *Database Nation*. New York: O’Reilly, 2000; Harrington, Susan J. “The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions,” *MIS Quarterly* 20 (1996): 257–278; Moore, Adam D. *Information Ethics*. Seattle: University of Washington Press, 2005; Rubin, Paul H., and Thomas M. Lenard. *Privacy and the Commercial Use of Information*. Amsterdam: Kluwer Academic Publishers, 2002; Solove, Daniel J. *The Digital Person*. New York: New York University Press, 2004; Straub, Detmar W., Jr., and William D. Nance. “Discovering and Disciplining Computer Abuse in Organizations: A Field Study,” *MIS Quarterly* 14 (1990): 45–60.

Leslie Ann Reis

Pharming. *See Internet*

Phishing. *See Internet*

**Physical privacy. See Privacy, definition of****Plain view doctrine**

This doctrine allows the admission of evidence seized by law enforcement officers during a warrantless search. It also allows the admission of evidence discovered and seized by police during a search authorized by a warrant even when the warrant did not specifically cover the items seized. In some instances, it is also interpreted to allow a warrantless search. In order to seize an item in plain view, there must be probable cause to believe the item is evidence of a crime, the instrumentality of a crime, or contraband. Although the doctrine usually applies to objects that can be seen, it is frequently argued that it may be extended to items that can be smelled, heard, tasted, or felt.

One of the earliest Supreme Court cases to address the question of what an officer can do when contraband is in plain view was *Steele v. United States*, 267 U.S. 498 (1925). In that case, two federal Prohibition agents watched through an open garage door as cases of whisky were unloaded for storage. They had no warrant, but they used their observations as the basis to obtain one. Despite the nature of the primary “search,” the court authorized the subsequent warrant and approved the eventual seizure of more than 200 cases of whisky and gin, two 50-gallon drums of whisky, several 5-gallon jugs, and dozens of filled whisky bottles. The violation of privacy, however, was not addressed.

Steele was distinguished from *Taylor v. United States*, 286 U.S. 1 (1932), in which probation agents had been able to look through a garage window and had seen boxes of liquor. In that instance, rather than get a warrant, the agents broke into the garage and seized 122 cases of whisky. The Supreme Court called that seizure a violation because the officers did not first seek a warrant after observing the contraband in the garage.

Officers’ ability to seize contraband observed while looking through a doorway from inside a **home** received the Supreme Court’s approval in *Ker v. California*, 374 U.S. 23 (1963). In that case, officers were arresting Ker in his living room when they looked through a doorway to the kitchen and saw a brick of marijuana sitting on a scale. Seizure of the drug, despite the fact that there was no **search warrant**, was upheld. “The discovery of the brick of marijuana did not constitute a search, since the officer merely saw what was placed before him in full view.”

The plain view doctrine has been applied by the courts in many instances of warrantless seizures. An officer who accompanies a student to the student’s dorm room to get an identification card may lawfully seize marijuana seeds and a pipe in plain view (*Washington v. Chrisman*, 455 U.S. 1 (1982)). Officers securing a home after arresting a robbery suspect may seize evidence of the robbery, such as clothing worn by the suspected robber, when it is on the floor in plain sight (*Maryland v. Buie*, 494 U.S. 325 (1990)).

The court extended the plain view doctrine to **automobiles** in *Harris v. United States*, 390 U.S. 234 (1968), a robbery case. There, after legally impounding Harris’s car, an officer opened a car door to close the window to protect the interior from rain that had begun to fall. In opening the door, the officer found a robbery victim’s registration card that was later used as evidence against Harris. The Court ruled: “Once

the door had lawfully been opened, the registration card, with the name of the robbery victim on it, was plainly visible. It has long been settled that objects falling in the plain view of an officer who has a right to be in the position to have that view are subject to seizure and may be introduced in evidence.” According to the Court, the same logic applies if an officer stops a car for a traffic violation but sees contraband on a car seat (see, e.g., *Texas v. Brown*, 460 U.S. 730 (1983)).

What if the item is not exactly in “plain view”? In *New York v. Class*, 475 U.S. 106 (1986), officers stopped a speeder and needed to locate the vehicle identification number of his car. One officer opened the car door to look on the doorjamb for the number and then realized the number for that model car was on the dash. To see the number, the officer moved some papers out of the way. In doing so, he uncovered a gun handle. Police seized the gun and Class was arrested for illegal possession of a handgun. In allowing the admission of the gun as evidence, the Supreme Court stated, “A citizen does not surrender all the protections of the Fourth Amendment by entering an automobile. Nonetheless, the State’s intrusion into a particular area, whether in an automobile or elsewhere, cannot result in a Fourth Amendment violation unless the area is one in which there is a “constitutionally protected **reasonable expectation of privacy**.”

For many years, the Supreme Court required that discoveries under the plain view doctrine must be inadvertent. As the Court noted in *Coolidge v. New Hampshire*, 403 U.S. 443 (1971),

What the “plain view” cases have in common is that the police officer in each of them had a prior justification for an intrusion in the course of which he came inadvertently across a piece of evidence incriminating the accused. The doctrine serves to supplement the prior justification—whether it be a warrant for another object, hot pursuit, search incident to lawful arrest, or some other legitimate reason for being present unconnected with a search directed against the accused—and permits the warrantless seizure. Of course, the extension of the original justification is legitimate only where it is immediately apparent to the police that they have evidence before them; the “plain view” doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges.

Nevertheless, the Supreme Court did away with the requirement that the discovery be “inadvertent” in *Horton v. California*, 496 U.S. 128 (1990). In *Horton*, after an armed robbery, a police officer obtained a warrant to search a suspect’s home for items stolen during the robbery. To obtain the warrant, the officer had expressed a desire to search for stolen property and weapons used during the crime. For unknown reasons, the warrant only allowed a search for stolen property. While executing the warrant, the officer found none of the stolen items, but found and seized weapons used during the crime. The Court held there were no violations of the defendant’s privacy rights in this case since a valid warrant had been issued. Therefore, seizure of the guns was authorized under the plain view doctrine, even though it was clear the discovery was not “inadvertent.”

In applying the decision in *Horton*, courts have basically adopted a three-part test to determine if the plain view doctrine applies: (1) was the officer engaged in lawful activity at the time; (2) was the object’s incriminating character obvious and not hidden; and (3) did the officer have lawful access to the object—was it in plain view?

There have been cases where the courts have refused to extend the plain view doctrine, the most notable of which is *Arizona v. Hicks*, 480 U.S. 321 (1987). In that case, police responded to Hicks's apartment after a bullet fired through his floor hit an occupant in an apartment a floor below. Officers arrived to search for the shooter, other possible victims, and the weapons used. While looking around the squalid living quarters, however, an officer saw an expensive stereo that seemed out of place given the condition of the apartment. The officer moved the stereo equipment to take down serial numbers. Then, when he called the police station, he learned that the turntable had been taken in an armed robbery. Hicks was charged with armed robbery after it was determined all the stereo equipment had been taken in the same heist.

The *Hicks* Court took a two-step analysis to determine the plain view doctrine did not protect police in this case. First, it ruled that moving the equipment to get the serial number was a search "separate and apart from the search for the shooter, victims, and weapons that was the lawful objective of his entry into the apartment." The second question was whether the search was "reasonable" under the Fourth Amendment. The Court found that the search was unreasonable because the officer did not have probable cause to believe the stereo equipment had been stolen. The officer's reasonable suspicion did not equate to probable cause.

See also: Automobile search; Constitutional protections

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

David J. Brown

Pornography. *See Osborne v. Ohio*, 495 U.S. 103 (1990); *Paris Adult Theatre I v. Slaton*, 413 U.S. 48 (1973); *Stanley v. Georgia*, 394 U.S. 557 (1969)

Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) is a software program designed to make digital data more secure through encryption and **authentication**, particularly for data communications. It was developed in 1991 by Phil Zimmermann as freeware, and it was the first widespread program to use asymmetric, public key, encryption algorithms to ensure privacy of data during transmission. Mainly for performance reasons, PGP uses the public key to encrypt the shared secret key, which is in turn used to encrypt the data. Public-key encryption relies on there being two keys for any data transmission, a private key and a public key. The user of such software can disseminate the public key widely, as it does not help an individual discover the corresponding private key or decrypt intercepted messages to which that person is not entitled. The use of

public-key encryption systems depends on there being a “web of trust,” or a public-key infrastructure (PKI) that can provide validation for users of the system. This is one of the major drawbacks for widespread public use of such systems. An early impediment to the growing **Internet** community’s adoption of PGP was the relatively complex structure and installation requirements. The software is usually used for the encryption of **electronic mail**, although current versions offer wide flexibility in their data security and authentication options.

The initial release of the code led to a criminal investigation for export violations. The United States government saw strong encryption as ammunition for export purposes, and thus subject to licensing and export restrictions. Although the case against the primary author, Phil Zimmermann, was dropped in 1996, a number of issues relating to national security, freedom of expression, and the ability to restrict the distribution of **computer** code were raised by this episode. There were also some early issues with the use of the International Data Encryption Algorithm and the Rivest-Shamir-Adleman algorithm (IDEA and RSA), with claims that their use was in breach of patent. Following the incorporation of the company, PGP was acquired by Network Associates, Inc., in 1997, but reformed as PGP Corporation in 2002. The Internet Engineering Task Force has adopted OpenPGP as a proposed standard that may be implemented by anyone without a license. There are also some free programs available that employ strong encryption, such as GnuPG and freeware versions of the commercial PGP.

See also: **Cryptography**

Suggested Reading: Garfinkel, Simson. *Web Security, Privacy and Commerce*, 2nd ed. New York: O’Reilly Media, 2002; OpenPGP Software. www.openpgp.org. Online, November 2005; Pretty Good Privacy Corporation. www.pgp.com. Online, November 2005; Singh, Simon. *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*. New York: Doubleday, 1999.

Mark Perry

Prisoners

Privacy is at a premium for the incarcerated. Many prisoners in America’s jails and prisons live in large dormitories with beds lined up next to each other. Sometimes their beds are separated by partitions. They share group lavatory and shower facilities. Many prisoners live in cells with other inmates who also share an unenclosed sink and commode. Most prisoners eat their meals in a common area. They are assigned jobs that group them with other inmates and have little control over their assignments or with whom they work. Recreation facilities are designed to accommodate groups of prisoners. Prisoners who live in single cells are housed in cellblocks or pods, where multiple cells are built next to each other and in rows above and below each other. Although they may not be able to see other inmates directly, prisoners can hear others talk and shout around them.

Adding to the lack of privacy in their living, working, and recreation arrangements is constant supervision by correctional staff. Correctional officers regularly patrol cellblocks, dormitories, chow halls, recreation areas, and job sites. They watch group showers and lavatories. They peer into cells and may witness prisoners

using commodes, and dressing and undressing. Other staff members watch closed-circuit television monitors with images from cameras positioned in critical places throughout the facility. Included among the most significant pains of incarceration is losing the right to engage in basic and intimate human activities in private.

When the U.S. Supreme Court ruled in *Cooper v. Pate* (1964) that federal courts must be accessible to prisoner lawsuits that allege violations of **constitutional protections**, a prisoners' litigation revolution was unleashed. Naturally, prisoners filed lawsuits challenging policies that limited their privacy interests. Few of those lawsuits have been successful.

In *Rhodes v. Chapman* (1981), for example, prisoners double-celled in a maximum security prison alleged that housing more than one inmate in a cell originally designed to accommodate one violated the Eighth Amendment's Cruel and Unusual Punishment Clause. The Supreme Court ruled the Constitution does not require that inmates be housed in single cells. Although the Eighth Amendment argument was based on the deleterious effects of overcrowding, the Court's decision seriously impacted the privacy interests of prisoners as well.

Until the Supreme Court decided *Procunier v. Martinez* (1974), prison administrators freely censored prisoners' incoming and outgoing mail for a myriad of reasons, including the right to censor material they thought expressed inflammatory political, religious, and political views. In 1974, the Supreme Court found such unfettered censorship violated the First Amendment rights of people who corresponded with prisoners. The Court acknowledged that legitimate security concerns give administrators the right to read mail sent and received by inmates, but the Court concluded that censorship is warranted only if it furthers a substantial governmental interest, and it must be no greater than necessary. In addition, when censorship is warranted, administrators must extend notice to both internal and external correspondents and give them a right to appeal. Even though correctional administrators retain the right to read prisoner correspondence, *Procunier* is significant because it protected prisoners' rights to send and receive uncensored mail.

Issues involving inmate correspondence, however, continued to trouble the courts. The Supreme Court relied on a different legal standard than it applied in *Procunier v. Martinez* to consider whether prohibiting prisoners from corresponding with other prisoners violated the Constitution. In *Turner v. Safely* (1984), the Court concluded such a regulation could be supported by legitimate security concerns and upheld its constitutionality. In *Thornburgh v. Abbott* (1989), the Court applied the legal standard used in *Turner* to uphold the constitutionality of regulations prohibiting inmates from receiving publications that authorities judged were detrimental to institutional security, even though there was no evidence that refusing to deliver them served a substantial governmental interest and was the least restrictive means available. In explaining its decision, the Court noted that the strict *Procunier v. Martinez* test, which required correctional authorities to demonstrate that correspondence regulations served a significant governmental interest, only applied to mail sent by prisoners to individuals outside the institution. That mail presented a lower security risk than mail sent to prisoners. The legality of regulations governing the mail inmates receive can be evaluated under a lesser standard: does the regulation further a legitimate governmental interest in providing a secure institution? The *Thornburgh* decision gives officials significant discretion to

restrict what inmates can read. The *Turner* decision allows officials to institute a blanket ban on inmate-to-inmate correspondence.

Although the Fourth Amendment protects against “unreasonable searches and seizures,” the scope of that protection is significantly diminished for anyone who is incarcerated. Officials regularly search cells and dormitories for contraband and weapons. In *Hudson v. Palmer*, 468 U.S. 517 (1984), the Supreme Court ruled that officials may conduct those searches without a prisoner’s consent or knowledge, and for any reason or no reason at all. Prisoners simply do not have a reasonable expectation of privacy in their housing areas. In addition to having their “houses” searched, prisoners are also subject to regular searches of their bodies. From walking through metal detectors, to pat-down searches of outer clothing, to **strip searches** (which often include visual inspection of a prisoner’s body cavities), prisoners’ bodies have no Fourth Amendment protections. As long as a pat-down or strip search is conducted in a professional manner and not done to harass or humiliate an inmate, officials have enormous discretion to conduct such searches for virtually any reason. Even individuals detained in jail, even though they are not yet convicted and are still presumed innocent, have no Fourth Amendment protection against body-cavity searches. As a consequence, strip searches and visual body-cavity searches are quite common in both jails and prisons. Much less common are searches inside a prisoner’s body cavity, such as probing his or her mouth, genital areas, or a stomach using an **x-ray device**. These more intrusive searches require reasonable suspicion that a crime or serious rule violation has occurred, and that the examination is necessary. These examinations must also be conducted professionally and in a sanitary manner. Although not legally required, medical personnel generally conduct such a search.

Both men and women serve as correctional officers, and equal employment laws prohibit restricting their job assignments to same-sex prisons. Consequently, male officers work in women’s units and women work in men’s units. Several prisoner lawsuits have alleged that cross-sex supervision, which includes supervising inmate living areas and conducting pat-down and strip searches, violates their right to privacy. Some courts have supported a prisoner’s right to be protected from unrestricted cross-sex supervision and have limited the situations under which it can occur, including limiting when members of the opposite gender can conduct searches or be assigned to certain housing areas. Other courts have supported correctional officials who argue a prisoner’s right to privacy takes a back seat to institutional security and affording equal employment opportunities to correctional staff. Several courts have ruled that cross-gender searches of female inmates raise different legal issues from cross-gender searches of male inmates. As a result, there are a variety of different policies on cross-gender supervision in prisons and jails across the United States.

Having HIV-positive prisoners has raised serious privacy issues for correctional administrators. The U. S. Supreme Court has not addressed these issues, but several lower federal courts have rendered decisions on specific questions. One of the most important issues has been whether correctional officials can or must require prisoners to be tested for HIV. Some prisoners have argued that mandatory testing is necessary to ensure their health. Other prisoners have maintained that mandatory testing sounds constructive, but it violates the Fourth

Amendment and puts at risk a prisoner's right to have his or her medical condition kept private. In the close and intense prison environment, there are few secrets that even careful administrators can protect. Related to HIV testing is the legality of segregating HIV-positive inmates from the rest of the inmate population. Segregation not only reduces inmates' opportunities to participate in prison programs, but it also effectively advertises their medical condition to the prison community. It also makes them vulnerable to assault by other inmates and harassment by staff. In *Harris v. Thigpen* (1991), the Eleventh Circuit Court of Appeals upheld the constitutionality of mandatory HIV testing of all prisoners admitted to Alabama's prisons as well as the policy segregating HIV-positive inmates. The court concluded that neither mandatory testing nor segregation violate the cruel and unusual punishment clause. The court refused to rule, however, that mandatory testing was required by the Constitution. Several other federal courts have also ruled that agencies are free to institute mandatory testing programs but are not required to do so. In addition, most courts have ruled that correctional agencies may choose to segregate HIV-positive inmates or mainstream those who do not pose a security risk to the general population.

The law is less clear about if and under what circumstances authorities can reveal a prisoner's HIV-positive status when he or she has not been placed in segregated housing. It has been settled that officials violate the Constitution's Cruel and Unusual Punishment Clause if they reveal a prisoner's HIV-status to humiliate a prisoner or put that prisoner at risk of attack. It is less certain if officials violate the Constitution when they reveal a prisoner's HIV-positive status in order to protect other prisoners or staff. Although there are cases that recognize an inmate's constitutional right to privacy regarding medical conditions, many courts have ruled the right is limited by policies that serve legitimate security and safety interests.

It is obvious that prisoners' privacy rights are extremely restricted under the Constitution. Courts have struggled with defining the scope of those restricted rights, but there is little disagreement that the scope is quite narrow. Unlike other areas where prisoner lawsuits have been quite successful in reforming correctional policies and practices—including freedom of religious expression, use of due process in the disciplinary process, access to legal materials, and the right to adequate health care—fundamental and overriding security needs generally trump privacy concerns. Courts are reluctant to second-guess administrators in these matters, and there is every indication this trend will continue.

See also: **Health privacy; Manners; Private parts; Surveillance cameras**

Suggested Reading: Belbot, Barbara A., and Rolando V. del Carmen. "AIDS in Prison: Legal Issues," *Crime and Delinquency* 37 (1991): 135–152; Buchanan, Kim Shayo. "Beyond Modesty: Privacy in Prison and the Risk of Sexual Abuse," *Marquette Law Review* 88 (2005): 751–813; Conrad, John P. "From Barbarism toward Decency: Alabama's Long Road to Prison Reform," *Journal of Research in Crime and Delinquency* 26 (1989): 307–328; Feeley, Malcolm, and Van Swearingen. "Taking Stock of the Accomplishments and Failures of Prison Reform Litigation: The Prison Conditions Cases and the Bureaucratization of American Corrections: Influences, Impacts and Implications," *Pace Law Review* 24 (2004): 433–475; Jacobs, James. *New Perspectives on Prisons and Imprisonment*. Ithaca, NY: Cornell University Press, 1983; Silver, Mara. "Testing Cruzan: Prisoners and

the Constitutional Question of Self-Starvation,” *Stanford Law Review* 58 (2005): 631–662.

Barbara Belbot

Privacy, definition of

Privacy concerns exist in every society, erupting in daily life as problems of etiquette, ethics, religion, and law. Illuminated by recent scholarship, discussion, and debate, privacy is no longer the opaque concept it once seemed. The boundaries of privacy are readily discernible through close attention to its ordinary applications. Privacy is as privacy does, and what it mainly does is describe and demand limits on the appropriation of others’ peaceful seclusion, personal information, intimate choices, and identities.

An exact definition of privacy remains elusive. Lawyers have said that the gist of privacy is the “**right to be let alone**.” Philosophers have shown that privacy often means “inaccessibility to others’ senses and **surveillance** devices.” Privacy means “control over personal information” for policy makers designing data protection and electronic communications practices. Outside of narrow academic circles, constructing an exact definition of privacy has proven less important than addressing concrete claims for privacy protection. Seclusion, solitude, **anonymity**, **confidentiality**, modesty, intimacy, **secrecy**, autonomy, and reserve—securing these social goods is what privacy is all about.

In contemporary American parlance, losses of what is called “privacy” include rude house guests overstaying their welcomes, and nosy employers reading employees’ personal **electronic mail**. They include court decisions denying same-sex couples the legal right to marry, and identity thieves stealing **Social Security numbers**. Privacy takes on a straightforward aspect when we see that, despite the problem of pinning down an overall philosophical definition, appeals to privacy tend to fall into one or more of four recurring categories reflected in the previous examples. We do well to distinguish physical privacy, informational privacy, decisional privacy, and proprietary privacy.

Overstaying house guests result in a loss of physical privacy. Solitude can be vital to privacy in a physical or spatial sense. Although no guarantor of repose, the **home** is the heart of private life, and a domain culturally marked for the enjoyment of the highest expectations of physical privacy from strangers. The desire for physical privacy often drives complaints about unlawful search and seizure, peeping toms, **trespass**, and “ambush” **journalism**. Bodily integrity, which comes up in discussions of everything from medical care and roadside **sobriety checkpoints** to assault and battery, is an additional important physical privacy concern.

Employers who read employees’ personal e-mail messages without a legitimate business purpose offend morals and manners, violating expectations of informational privacy. Confidentiality, data protection, data encryption, data security, secrecy, anonymity, and adherence to fair information practice standards comprise the informational dimension of privacy.

Opposition to same-sex marriage illustrates a denial by government of decisional privacy. Not without special controversy in jurisprudential circles, the term “privacy” has come to denote freedom from government interference with personal life. Like it



or not, the rights of individuals, married couples, and families to direct their own lives are commonly styled as privacy rights. Disagreements about the proper limits of decisional privacy fuel heated moral debates over gay rights, abortion, and physician-assisted suicide.

Identity thieves accessing personal financial data illustrate a loss of proprietary privacy. Government regulators and the general public characterize identity theft as a privacy problem because it entails seizing otherwise confidential information and personal identifiers. In a related vein, the rights of celebrities and others to control the attributes of their personal identities—their names, voices, trademarks, traits, and **DNA**—are commonly styled as privacy concerns.

Despite the tenor of its beginnings, the goal of this entry is not conceptual mapping alone. Rather, the goal is to introduce privacy by addressing the ambivalent posture in which the United States now finds itself respecting informational and physical privacy values. A nation of extensive privacy laws, with a history and culture of privacy protection driven by a concern for civil liberties and human rights, the United States is also a nation in which people can be surprisingly indifferent to privacy and lax about privacy protection.

The United States is notable for the quantity and quality of its positive constitutional, tort, and statutory privacy law. First, the United States Supreme Court has recognized that five of the original Bill of Rights amendments and the Fourteenth Amendment protect privacy interests. Second, in U.S. tort law, interests against intrusion upon seclusion; public **disclosure** of private fact; publications placing another in a false light; and misappropriation of a person's name, likeness, or identity are potentially protected through civil actions styled as invasions of privacy. Third, more recent than common law and provisions of the U.S. Constitution, federal and state statutes protect interests in privacy. Access to health records, educational records, financial transactions, electronic communications, and children's **Internet** use are all regulated by statute. Tax, video rental, library, **adoption**, and many other types of records about individuals are private as a result of state and federal informational privacy statutes.

Much of the privacy law of the United States is designed to promote informational privacy, suggesting a nation with uniquely strong informational privacy commitments. Yet the United States is currently notable as a polity inclined toward sacrificing informational privacy as needed to meet short-term policy objectives and toward voluntary self-disclosure to meet consumer and lifestyle objectives. Assuming these empirical observations about the practices of privacy protection are correct, how then do we make sense of the value gap between what the people of the United States have written into their positive privacy laws and how they live out their daily lives? When it comes to personal information, is the United States a privacy-loving or a privacy-indifferent society?

Although this question is posed about a single country, the implications of the inquiry are not parochial. People in other parts of the world, including Canada, Great Britain, Europe, and Australia, plainly value informational privacy. Informational privacy is valued in Africa, Asia, and South America, too. What counts as a privacy intrusion and why privacy is important varies considerably from place to place. As customs, traditions, religions, and resources vary, so, too, will attitudes about privacy. An American woman may demand health information privacy for

the sake of her autonomy. An Iranian, Pakistani, or Kenyan woman may demand medical privacy for the sake of her modesty, religious obligation, or reputation.

Not only is privacy held as a value around the world, but there are privacy laws on the books in countries around the world. Few countries rival the U.S. in the quantity of privacy laws enacted for the sake of shielding personal data from non-consensual public disclosure. But quality is telling, too. European Union countries and Canada arguably surpass the U.S. in the vigorous enforcement of informational privacy rights governing financial or other personal data. In Canada, professional public privacy commissioners tend to privacy law enforcement. A “Directive of the European Parliament and the Council of Europe on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data” (see **European Data Protection Directive**) went into effect in October 1998. It called for European Union member states to enact policies that protect the right to privacy in the processing of personal data. Laws currently in place in member states forbid certain types of data collection and demand that information gathered in commerce be limited to authorized users and uses. In much of Western Europe, individuals have more control over whether financial, race, religion, ethnicity data can be shared.

In any country there can be gaps between positive privacy protections on the one hand, and political and cultural practices on the other, and for a variety of reasons. Concerns about national security played a major role in the relaxation of civil liberties in the United States after the terrorist attacks on New York and Washington on September 11, 2001. Terrorism, genocide, civil war, and HIV/AIDS have led contemporary governments around the world to more intrusively monitor personal conduct.

To the extent that popular culture, technology, and changes in **gender** roles are driving down the taste and market for privacy, one could expect to see changes in the value placed on various dimensions of privacy in countries other than the United States. The willingness to have personal conversations on **cellular telephones** in public places is not just a U.S. phenomenon, nor is it only American women who are delivering sexual services and babies live on the World Wide Web.

Why care if privacy is poorly protected or too readily given up? Why does privacy matter? Some of the traditional answers to this question are that privacy promotes values of personhood, intimate relationships, autonomy, tolerance, and limited government. Privacy creates and enhances a sense of individual personhood. Opportunities for privacy allow people to express themselves, relax, reflect, and thereby develop as individuals. Privacy allows for the independent development and exercise of moral judgment. Opportunities for privacy enable people to keep some persons at a distance, so that they can enjoy intense intimate relationships with others, including friends, families, and spouses. Privacy allows the individual or groups of like-minded individuals the ability to plan and live out their own lives. Privacy makes it possible for people to determine their own destinies. Privacy rights against government ensure that government will remain limited and unobtrusive, as liberal democracy requires. Privacy rights ensure that those who disagree with us will not be permitted to impose their personal values and preferences on us, or force us to live as they live. Decisional privacy that sets individuals free to make their way—and their own mistakes—is good for society, too. As John



Stuart Mill argued in *On Liberty*, toleration promotes the full-flowering of individual artistic, spiritual, and commercial genius. Mill's principle of liberty rejected accountability to the state for "self-regarding" conduct. Persons are not answerable to the community for conduct that is truly self-regarding, that is, not significantly harmful or injurious to others.

1. Bountiful Constitutional Privacy Law

Privacy has value. By virtue of the federal Constitution, Americans have enjoyed protection of privacy since the founding of the nation in the late eighteenth century. The word "privacy" does not appear in the U.S. Constitution. The Supreme Court has interpreted five of the ten original Bill of Rights guarantees and the Fourteenth Amendment as protective of privacy. Furthering family and group privacy, the First Amendment guarantees freedom of religion and **freedom of association**. The Third Amendment prohibits military appropriation of private homes.

Also protective of the home and its contents, the Fourth Amendment prohibits arbitrary search and seizure of persons and property. In the 1960s, the Supreme Court gave the term "privacy" a central role in the interpretation of the Fourth Amendment. Whether at home, in bed, or in a phone booth, citizens have a right to a "**reasonable expectation of privacy**," as determined by the Court in an important group of cases concerning government search and seizure, the first of which was *Katz v. United States*, **389 U.S. 347 (1967)**.

The Fifth Amendment prohibits compulsory self-incrimination, allowing for privacy of thought and belief. The Ninth Amendment reserved unenumerated traditional rights to the people, including rights of bodily integrity, possession, and independent decisionmaking associated with privacy.

The federal Constitution was amended after the Civil War to reflect the abolition of slavery. The new amendments included the Fourteenth Amendment, which asserted that no state may deprive a person of life, liberty, or property without due process of law. Designed to protect the rights of freed slaves, the general language of the Fourteenth Amendment is now an important source of protection for substantive liberties sought by private individuals and families. In their written opinions interpreting the Fourteenth Amendment and the Bill of Rights, justices of the Supreme Court have frequently invoked the concept of privacy as a substantive due process value.

In the 1960s and 1970s, the Supreme Court also gave the term "privacy" an important role in cases about the regulation of reproduction, sex, marriage, and personal information. In *Griswold v. Connecticut*, **381 U.S. 479 (1965)**, the Court held that there is a fundamental right to privacy that prohibits laws criminalizing birth control. In the *Griswold* decision, the Court argued that privacy has always been an implicit constitutional value, residing in the "penumbra" of the Bill of Rights. In *Loving v. Virginia*, **388 U.S. 1 (1967)**, the Court recognized privacy and equality interests in interracial marriage, and in *Stanley v. Georgia*, **394 U.S. 557 (1969)**, it recognized privacy interests in personal use of pornography at home. Increasingly after *Roe v. Wade*, **410 U.S. 113 (1973)**, in which the Court held that the Fourteenth Amendment was a source of a fundamental right to privacy strong enough to block the categorical prohibition of abortion, the Fourteenth Amendment has become the major legal tool for persons asserting controversial privacy rights against government. *Whalen v. Roe*,

429 U.S. 589 (1977), recognized a Fourteenth Amendment privacy interest requiring confidentiality and security to protect prescription drug use data collected by the state.

Constitutional privacy jurisprudence has been successfully applied in some landmark “right to die” cases, most notably in a New Jersey state supreme court case, *In Re Quinlan*, 355 A.2d 647 (1976), although not consistently in other decisions. The Supreme Court held in *Cruzan v. Director, Missouri Dep’t of Health*, 497 U.S. 261 (1990), that states may require families, prior to terminating life support, to demonstrate by “clear and convincing evidence” that a family member in a hopeless vegetative state would have wanted to die under those circumstances. In 2006, the Supreme Court upheld an Oregon statute permitting physician-assisted suicide, but declined in *Vacco v. Quill*, 521 U.S. 793 (1997), and *Washington v. Glucksberg*, 521 U.S. 702 (1997), to recognize a right to physician-assisted suicide that would invalidate all state laws making it a crime for doctors to end the lives of terminally ill patients. In the question of the right of people to engage in consenting homosexual relations, the Court held in *Lawrence v. Texas*, 539 U.S. 558 (2003), that the Constitution does not to permit states to criminalize adult homosexual sodomy. On the other hand, lower courts have repeatedly held that states may criminalize prostitution, rape, and domestic violence consistent with the constitutional right to privacy.

The Court’s substantive due process jurisprudence fell on to hard times in the 1980s and 1990s, but an influential body of Supreme Court privacy precedent remains. Like the federal Constitution, many U.S. state constitutions include implicit privacy protections by virtue of provisions modeled after the federal Bill of Rights. In the period after 1970, many states, including Alabama, California, and Florida, amended their state constitutions to include explicit provisions guaranteeing privacy rights. In some instances state courts have held that state constitutions offer stronger protections against intrusion, interference with decisionmaking, and surveillance than those afforded by the federal constitution.

II. The Common Law Contribution

Constitutional law is only one aspect of America’s legal devotion to privacy. Common law doctrines inherited from English common law protected aspects of personal privacy at our nation’s inception. For example, the trespass tort deterred physical privacy invasions. Judge Thomas Cooley’s *A Treatise on the Law of Torts* (1880) identified a right of personal immunity, a right to be let alone from which the privacy tort descended. Some noteworthy early cases recognized that women have a legitimate sphere of immunity in areas surrounding their modesty. In *DeMay v. Roberts*, 46 Mich.160, 9 N.W. 146 (1881), a Michigan judge declared a right to the privacy of childbirth. In *Manola v. Stevens* (1890), a New York judge granted an actress an injunction against publication of a photograph of herself in tights.

In Samuel Warren and **Louis Brandeis**’s famous 1890 article, “The Right to Privacy,” these two Boston lawyers called for the creation of a new legal right to privacy, a right of “inviolable personality.” Inspired by the article, a privacy tort was first recognized by American judges in the early twentieth century.

In *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68 (1905), the tort law privacy right was fully born. No state’s supreme court officially recognized the right to privacy until 1905 when the Georgia high court in *Pavesich* allowed a man whose



photograph was used without his consent in an insurance advertisement to assert a right of privacy. In *Roberson v. Rochester Folding Box Co.* (1902), the New York court declined to create a right to privacy as a remedy for a woman whose photograph was used without her consent in an advertisement. However, the New York Civil Rights Act, Sections 50–51, was quickly enacted in 1903 and created a right against commercial appropriation of name or likeness in response to the *Roberson* case. The statute has remained on the books.

Today the common law of privacy recognizes four basic physical, informational, and proprietary privacy rights (but no decisional privacy right as such), first distinguished by William L. Prosser. Recognized by the American Law Institute's *Restatement of Torts (2d)* (1964), the four privacy rights are rights against (1) intrusion upon seclusion, (2) publication of embarrassing private facts, (3) publicity placing a person in a false light, and (4) appropriation of name likeness and identity.

A distinctive feature of the common law **privacy torts** is that, subject to exceptions for newsworthy publications and First Amendment freedoms, they permit lawsuits against persons who intentionally and in a highly offensive manner publish or disclose intimate truth. The right to privacy aims to protect persons whose feelings and sensibilities are wounded by having others discover truthful but embarrassing or intimate matters of fact as a consequence of highly offensive conduct. The Restatement presentation of the four torts has been adopted by statute or precedent in a number of states.

III. A Statutory Privacy Movement

The salience of tort and constitutional privacy law in daily life is eclipsed by the prominence of federal and state privacy statutes. In the 1960s the Cold War, the Vietnam conflict, and racial turmoil heightened concern about the government's techniques of espionage, surveillance, and social control. The surveillance technologies used for spying could also be used to monitor ordinary citizens and suspected criminals. The government's ability to discern the details of private lives through covert **wiretapping**, powerful lenses, microphones, and cameras made citizens concerned about the fate of freedom and democracy. Congress enacted the Omnibus Crime Control and Safe Street Act in 1967, permitting, but setting limits on, wiretapping and certain other forms of surveillance.

Concerns about data banks containing personal profiles emerged in the 1970s. The potential for unfair use of personal information and misinformation stored in commercial and government data banks led to the enactment of several federal laws, including the **Privacy Act of 1974**, the **Family Educational Rights and Privacy Act (FERPA)** of 1974, and the Right to Financial Privacy Act 1978. A national commission formed by federal lawmakers, the U.S. Privacy Protection Commission, published its two-volume report, *Personal Privacy in an Information Society*, in 1977.

The report recommended a list of **fair information practices** governing the collection, storage, and use of personal information about individuals. Under various models of fair information practices, standards such as these should be met to the extent possible: (1) the existence of data systems containing personal information should not be a secret; (2) personal information should only be collected for narrow,

specific purposes; (3) personal information should only be used in a ways that are similar to and consistent with the primary purposes for its collection; (4) personal information should be collected only with the informed consent of the persons about whom the information is collected or their legal representatives; (5) personal information should not be shared with third parties without notice or consent; (7) for the sake of accuracy and relevancy, the duration of storage of personal information should be limited; (8) individuals should have access to personal information about themselves and should be permitted to correct errors; and (9) those who collect personal data should ensure the security and integrity of personal data and systems.

Originating before widespread **computer** use, ideals of fair information practices are thriving today. Of course, lawmakers are at liberty to pick and choose which, if any, fair information practice standards they will incorporate into statutes. Existing state statutes protect the privacy of many types of communications, including telephone communications that could be recorded or intercepted by police or private investigators. Statutes enacted by lawmakers in individual states protect the privacy of information contained in many types of business and professional records. Access to adoption records, criminal histories, and **library records** is commonly regulated under state law. The private sector has begun to adopt fair information practices in business practices. In the 1990s, private firms engaged in the electronic commerce industry established TRUSTe and similar privacy seal organizations to certify that companies operating over the World Wide Web pledged to adhere to fair information practice standards, such as providing **privacy notices** informing site users of privacy policies and practices.

The federal government began to enact national laws in the 1970s in response to developments in computer, surveillance, and other technologies. Some statutes were simply a response to heightened awareness of privacy interests unrelated to technology, such as awareness of privacy interests in traditional school records. Primarily as a result of the Internet and further developments in communications technologies, recent decades have witnessed further growth in the number and variety of state and federal statutes, short of a European Union–style privacy law, protecting informational privacy and embodying fair information practices standards. On May 22, 2000, the Federal Trade Commission (FTC) released its third report on the state of online privacy protection, “Privacy Online: Fair Information Practices in the Electronic Marketplace.” The report called for legislation, perhaps similar to European Union laws, to protect consumers’ online privacy.

The **Children’s Online Privacy Protection Act of 1998 (COPPA)** went into effect in 2000. It prohibits commercial websites from gathering personal information from children under 13 without parental consent. However, no U.S. statute comprehensively regulates Internet privacy. In the absence of such legislation, the FTC, which regulates certain online business practices, has become a significant enforcer of existing privacy-related trade practices and statutes. The U.S. **telemarketing** industry balked at the FTC’s establishment of a highly popular national **Do-Not-Call registry** that limits commercial vendors from calling the homes and cell phone numbers of people who register with the government, arguing that government should not coerce privacy through commercial speech restrictions.



The United States government holds a vast quantity of personal information gathered in the course of census taking, tax collection, military management, law enforcement, intelligence gathering, and the administration of health, labor, and human services programs. The Privacy Act of 1974 was enacted in direct response to the increased use by government of computers to collect, store, and analyze personal information. Although the **Freedom of Information Act (FOIA)** opens government records to the public, FOIA works in tandem with the Privacy Act and exempts from disclosure medical, personnel, and similar files. Many agency regulations and statutes (the tax code, for example) limit access to personal information held by the federal government.

Off-line and online, personal information is also gathered and stored by the private sector. Privacy law includes comprehensive statutes enacted by Congress, mainly after 1974, governing, for example, the privacy and confidentiality of **banking and financial records**, school records, video rentals, and telephone calls. This legislation limits access to records and communications, but also regulates the basis for lawful government and other third-party accesses. The most important statute regulating communications is the **Electronic Communication Privacy Act of 1986 (ECPA)**, formerly known as Title III. It requires judicial approval for secret access to telephone calls, e-mail, and voice mail.

Additional major privacy legislation includes Title V of the **Financial Services Modernization Act of 1999** (Gramm-Leach-Bliley Act), and provisions of the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** that regulate access to health information held by physicians, hospitals, insurers, and researchers.

IV. A Culture of Accountability

Privacy law is plentiful, flourishing, and even expanding. A competing trend, accountability for private life, has become a salient feature of contemporary American culture. The accountability the public demanded of President Bill Clinton (see **Clinton-Lewinsky scandal**) and the civil rights leader Reverend Jesse Jackson for the details of their extramarital affairs are just two examples.

Some observers attribute the new accountability for sex to feminism's rallying cry that the "personal is political." Many feminists indeed reject classic liberal conceptions of accountability. Feminists are among those who are skeptical about the existence of realms of action and conduct without significant, relevant impact on others. Purely self-regarding conduct is, indeed, something of a myth. People's lives are importantly interconnected and interdependent. If someone uses cocaine, neglects his or her children, gambles, has unprotected sex, or drives a gas-guzzling automobile, that person's seemingly personal choices affect others. Some feminists entirely reject liberalism, but even feminists who are liberal feminists disagree sometimes with other liberals about when conduct is hurtful to others, by locating meaningful externalities where classical liberals find none. From their perspective, lives are importantly interconnected and interdependent.

Much accountability to the state and private sectors for personal life has been the historic rule. Accountability for personal matters is older than feminism, cell phones, and reality television. The organization of American society has always featured diverse requirements that individuals report, explain, justify, face sanctions for,

and routinize their private lives. The breadth of accountability for personal life that emerged in the United States in the late twentieth century is nonetheless remarkable.

The new accountability reflects an overdue public response to the social consequences of harmful conduct in nominally private spheres of sex, **family**, and health. After 1980, concerns about rampant domestic violence, **sexual violence** and crimes, and gender inequality intensified accountability demands. Over the ensuing decades, changes in American legal doctrines, law enforcement policies, and the judiciary met some of the pleas for fair intervention and sanctions made by feminists and others. In the wake of the AIDS epidemic, new levels of accountability between sexual partners gained public acceptance. At the same time that a public health crisis was intensifying, the media was signaling in response to government and celebrity sex scandals that the public could demand accountability for sex. A president accused of **sexual harassment** and adultery would not be sheltered from exposure. Leaders are accountable for their judgment and character; and the public is entitled to trust its government.

Adding to the mix, a popular culture of self-disclosure emerged. Accountability for private life is often voluntary. Individuals from all walks of life now believe that speaking openly about intimacies is socially permissible and advantageous, if not an outright imperative of responsible family ties, friendship, and citizenship.

V. A Sacrifice of Civil Liberties

Jurists and scholars who assert that privacy is important uniformly agree that privacy rights are not absolute. No one can have or expect to have all of the privacy he or she may want, even in a free, liberal society based on market principles. Sometimes protecting privacy is simply impractical. It is common for courts to “balance” privacy interests against interests in, inter alia, law enforcement, **public health and safety**, national security, business, efficiency, and the public’s right to know. Courts have held that even where privacy interests are fundamental, they can be overcome by compelling state interests. And courts do not regard some controversial types of privacy-infringing surveillance, such as placing cameras on public street corners to deter crime, as invasions of privacy at all.

Since the events of September 11, 2001, the concept of “homeland security” has come to play a role in public life. The mandate of homeland security requires stepping up practices of search and surveillance in the name of national defense, military necessity, criminal law enforcement, and public health and safety. Sometimes privacy concerns are set aside in the context of homeland security simply because invading privacy is the more efficient or pragmatic way to get or seek information. In 2006, the administration of President George Bush admitted to secret communications monitoring of American citizens, justified by the importance of swift action to deter potential terrorists. President Bush claimed constitutional powers and Congressional authorization. Opponents labeled the program illegal domestic spying in the name of what was supposed to be a war on terrorism. Opponents pointed out that the **Foreign Intelligence Surveillance Act of 1978 (FISA)** established a court and a process that afford government authorities an expeditious means to obtain judicial approval for sensitive covert communications surveillance. Moreover, the Fourth Amendment and the federal wiretapping laws enacted as the Electronic



Communications Privacy Act (formerly Title III) prohibit and punish domestic spying without a warrant or court order.

VI. The Privacy Give Away

As some civil libertarians claim, privacy is being taken away. But clearly physical and informational privacy is being given away all the time. In 1999 a nurse chose to broadcast her double mastectomy live over the Internet, in order to educate the public about breast cancer. In 1998 a married woman chose to share the delivery of her third child with other expectant parents by delivering her baby live over the Internet. Men and women have chosen to train cameras on the interiors of their dwellings and then sell or give away real-time images of their daily lives. While their cameras and computers broadcast images of themselves to others, they have no physical privacy to speak of, and others possess otherwise private information about their home life. The adult entertainment industry reflects the willingness of performers and sex workers to sell access to bodily intimacies. The law barely and inconsistently seeks to enforce public decency standards geared toward compelling privacies in this area.

Consumers willingly give away personal data, hoping to reap benefits of discounts for travel and merchandise. They also do it simply for the sake of convenience, for example, to make a **credit card** purchase on line. Knowing the risk of **identity fraud**, consumers and vendors take precautions to protect personal information transmitted on line. Nonetheless, consumers are remarkably free when it comes to sharing personal data. Even though financial services companies expressly offer the option to opt out of personal data information sharing with the organization's business partners, most consumers do not bother. When retail clerks ask shoppers for their phone numbers and zip codes when they make off-line purchases, many consumers readily comply out of a felt need to be cooperative, even though such disclosures are merely routinely requested not required.

VII. Reconciling the Contradictions

On the one hand, the United States is awash in informational privacy laws. On the other hand, American culture is characterized by expectations of accountability for personal life and people's dispositions to willingly give up personal information, even when doing so is avoidable, risky, and undignified. What explains this apparent contradiction?

The gap between strong positive legal norms protective of privacy and the cultural surrender of privacy to government, business, and the general public makes sense if it is assumed that the underlying aim of privacy law is to protect privacy to the extent that people want it protected. So positioned, the United States, then, is less in the business of imposing privacy than of seeing to it that people have the privacy they want.

Imposed, coerced informational and related physical privacies are far from rare in the United States, however. Exotic dancers may be required to wear G-strings and pasties against their will, and people are not allowed to live in glass houses. Lawyers are required to keep client information confidential and so are physicians.

Yet coerced professional confidences are not inalienable rights, and they can be overridden by a decision to disclose made by a competent client or patient.

Privacy laws creating inalienable information privacy rights are few and far between. One example, however, are informational privacy rules imposed on children. Young children, fit beneficiaries of government paternalism and parental protection, cannot themselves waive the privacy protections of the federal Children's On-line Privacy Protection Act or the Family Educational Rights and Privacy Act.

The message of U.S. privacy laws is that privacy rights are extremely important because they protect individual, relational, and political goods people generally value. But why not have privacy laws that protect important individual, relational, and political goods that people do not happen generally to value, but perhaps should? This is a normative question of some importance. Is it a good thing that U.S. privacy law, and the privacy law of other Western nations, is at bottom more privacy neutral than not? It is privacy neutral in the sense that the law does not, in the final analysis, insist upon privacy for adults. The underlying goal of privacy law is evidently to foster the ideal of freedom of choice, and to thereby fight subordination, moralism, or paternalism.

Focusing on the privacy-neutral stance of U.S. privacy law makes it easier to comprehend the willingness to weaken privacy law as needed in the name of national security, public safety, and public health. The national and popular commitment is to choice, not to privacy itself. When faced with a policy priority of any magnitude, violating expectations of privacy can easily be read as merely removing an opportunity for one specific choice in a nation otherwise rich with choices.

See also: **Constitutional protections; Privacy, philosophical foundations of**

Suggested Reading: Agre, Philip E., and Marc Rotenberg (eds.). *Technology and Privacy: The New Landscape*. Cambridge, MA: M.I.T. Press, 1997; Alderman, Ellen, and Caroline Kennedy. *The Right to Privacy*. New York: Random House, 1995; Allen, Anita L. *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability*. Lanham, MD: Rowman & Littlefield, 2003; Ariès, Philippe, and Georges Duby (series eds.), *A History of Private Life*, vols. I–V. Cambridge, MA: Belknap Press, 1992; Bennett, Colin, and Rebecca Grant (eds.). *Visions of Privacy: Policy Choices for the Digital Age*. Toronto: University of Toronto Press, 1996; DeCew, Judith Wager. *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*. Ithaca, NY: Cornell University Press, 1997; Flaherty, David H. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill: University of North Carolina Press, 1992; Kersch, Ken I. *Constructing Civil Liberties: Discontinuities in the Development of American Constitutional Law*. Cambridge: Cambridge University Press, 2004; Regan, Priscilla. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press, 1995; Rössler, Beate (ed.). *Privacies: Philosophical Evaluations*. Stanford: Stanford University Press, 2004; Schoeman, Ferdinand David. *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press, 1984; Solove, Daniel J. *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press, 2004; Westin, Allan. *Privacy and Freedom*. New York: Atheneum, 1967.

Anita L. Allen



Privacy, philosophical foundations of

There is wide agreement that most Americans take privacy seriously, value it highly, and worry about its erosion. Unfortunately there is little agreement as to what privacy is, what it does protect, and what it should protect. The term “privacy” is used frequently in everyday language as well as in philosophical, political, and legal discussions, yet there is no single definition or analysis or meaning of the term. There has been extensive discussion of privacy in the philosophical literature. While this discussion does not provide definite answers, the ideas set forth in this entry provide alternative philosophical definitions or defenses of privacy, and can help illuminate various understandings of what the concept of privacy is, what it means, and why it has value. [Portions of this paper are drawn from discussions in my book *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Cornell University Press, 1997) and my paper, “Privacy,” *Stanford Encyclopedia of Philosophy* (2002).]

1. Historical Roots of Privacy

The concept of privacy has broad historical roots in anthropological and sociological discussions about how extensively it is valued and preserved in various cultures and societies. For example, Margaret Mead and other anthropologists have shown the ways different cultures protect privacy through concealment, seclusion, or restricting access to secret ceremonies. Alan Westin has also surveyed studies of animals demonstrating that a desire for privacy is universal and not restricted to humans.

Discussions of privacy by Mead and Westin give rise to the question of whether or not privacy as a concept is relative. Ferdinand Schoeman has pointed out that the question of whether or not privacy is culturally relative can be interpreted in two ways. One question is whether privacy is deemed valuable to all peoples, or whether its value is relative to cultural differences. A second question is whether or not there are any aspects of life that are inherently private and not just conventionally so. In response to the first question, most writers have come to agree that while almost all cultures appear to value privacy, cultures vary in their ways of seeking and obtaining privacy, and probably do differ in the extent to which they value privacy. There has been far less agreement on the second question. Some have argued that matters relating to one’s innermost self are inherently private. Philosopher Jeffrey Reiman states, “I can sum up that value [of privacy] as: the protection of freedom, moral personality, and a rich and critical inner life.” Yet characterizing privacy and its value more succinctly and less vaguely has remained an elusive task. Thus it may well be that one of the difficulties in defining or characterizing the realm of the private is that privacy is a notion that is strongly culturally relative, contingent on such factors as family structure and economics as well as on the technology available in a given cultural domain.

Beyond anthropological and sociological references, the concept of privacy also has historical origins in well-known philosophical discussions. Perhaps the best historical examples of allusions to privacy in philosophical texts date as far back as writings by Aristotle. As Jean Bethke Elshtain has argued, a wide array of thinkers “of the Western political tradition assumed and deployed *some* form of a distinction between the public and the private as conceptual categories and as private and public imperatives, to conceal as well as reveal. As conceptual categories, public

and private ordered and structured diverse activities, purposes, and dimensions of human social life and thinking about that life.” For Aristotle, the **public/private dichotomy** was interpreted to differentiate political and domestic spheres of life. Sometimes the split between public and private has reflected a differentiation between property held in the public domain and property held by individuals. Also the public/private distinction has at times been understood to reflect differences between the appropriate scope of governmental regulation as opposed to self-regulation by individuals. While explained in different ways, each of these views describes some type of public/private dichotomy.

Aristotle differentiated two distinct spheres of life. He saw the polis as the seat of government and the province of political activity, a public sphere where the proceedings of government in a city-state were developed. This public political arena was one where men, but not women or slaves, could participate in the functions of government. Aristotle describes man as a political animal who joins with others to participate in the polis. In contrast, separate from this public sphere was the *oikos*, the private or domestic sphere of the family, the private **home** or household where women and children lived and functioned, although men were the masters of their households in the *oikos*.

John Locke provided a second example of an allusion to privacy when he distinguished public and private property in his *Second Treatise on Government* (1690). According to Locke, in the state of nature all property is held in common by all, and no person has exclusive rights to the earth and all the bounty produced by nature. However, each person has a right to his own person and a right to self-preservation. Moreover, each individual has a right to extend his property rights through labor. Thus what one mixes one’s labor with becomes one’s own private property and is distinct from that owned publicly in common by all. There are other contexts in which there is a separation between public and private realms in Locke’s *Second Treatise*, although the relationship between the two spheres there is more complex. For example, those who voluntarily and mutually consent to form a political society and government thereby use public means to assure protection of their private ends, namely the protection of life, liberty, and property in the broadest sense.

A third historical example of a distinction between public and private in philosophical literature is evident in John Stuart Mill’s *On Liberty*, where Mill distinguished the appropriate realm of governmental authority as opposed to the realm reserved for self-regulation. Mill states and defends his famous harm principle, that the only reason government or society is justified in infringing on individual liberty is to prevent harm to others. In doing so, he focuses on that realm of activity where one’s behavior affects others, and where government may intervene to prevent harm, namely a sphere of action that is open to public scrutiny. This realm is distinguished from the sphere of actions that affect oneself only, or if they affect others, only with their free, voluntary, and undeceived consent. This latter sphere of activity, self-regarding actions, is the arena where governmental or social interference is unjustified, and thus this sphere of action is not legitimately open to public concern and is in this sense private. Mill is well aware that there are serious difficulties in determining how to distinguish those actions that he would call self-regarding from other-regarding actions. Nevertheless, his harm principle presupposes that there are two distinct realms, one where the government can legitimately interfere, and one where it can not.



These examples demonstrate that what is viewed as private in these different contexts varies: privacy can refer to forbidden views or knowledge, restricted access, a domestic sphere separate from government, property that one may call one's own that does not belong to others, and a domain inappropriate for governmental interference, to list just a few. In each case, however, the underlying assumption is that there is a boundary marking off that which is public from that which is private.

II. Categorizing the Philosophical Literature on Privacy

Early treatises on privacy appeared with the development of privacy protection in the law from the 1890s onward. The legal discussion of privacy began with the famous *Harvard Law Review* essay by Samuel Warren and **Louis Brandeis**, titled "The Right to Privacy," and their justification and recognition of a new privacy right in tort law that was made largely on various moral grounds. The philosophical debate concerning definitions of privacy intensified and became more prominent in the second half of the twentieth century. This literature helps us distinguish descriptive accounts of privacy, detailing what is in fact protected as private, from normative accounts of privacy, defending its value, and both why and the extent to which privacy should be protected. In these discussions, some treat privacy as an interest with moral value, something that is a good thing to have, while others refer to it as a right, moral or legal, that ought to be protected by society or by law or by both. Clearly one can be insensitive to another's privacy interests without violating any right to privacy, if there is one.

One way of understanding the growing philosophical literature on privacy is to view it as divided into two main categories, which can be called "reductionism" and "coherentism." Reductionists are generally critical of privacy, while coherentists defend the coherent and fundamental value of privacy interests. Ferdinand Schoeman introduced somewhat different terminology, which makes it easier to understand this distinction. According to Schoeman (1984), a number of authors have believed that

there is something fundamental, integrated, and distinctive about the concerns traditionally grouped together under the rubric of "privacy issues." In opposing this position, some have argued that the cases labeled "privacy issues" are diverse and disparate, and hence are only nominally or superficially connected. Others have argued that when privacy claims are to be defended morally, the justifications must allude to principles which can be characterized quite independently of any concern with privacy. Consequently, the argument continues, there is nothing morally distinctive about privacy. . . . I shall refer to the position that there is something common to most of the privacy claims as the "coherence thesis." The position that privacy claims are to be defended morally by principles that are distinctive to privacy I shall label the "distinctiveness thesis."

Theorists who deny both the coherence thesis and the distinctiveness thesis argue that in each category of privacy claims there are diverse values at stake of the sort common to many other social issues and that these values exhaust privacy claims. The thrust of this complex position is that we could do quite well if we eliminated all talk of privacy and simply defended our concerns in terms of standard moral and legal categories.

These latter theorists may be referred to as reductionists, for they view what are called privacy concerns as analyzable or reducible to claims of other sorts, such as infliction of emotional distress or property interests. They deny that there is anything coherent or distinctive about privacy, and they deny that there is anything useful in considering privacy as a separate concept. They conclude, then, that there is nothing fundamental or special or illuminating about privacy interests.

Probably the most famous reductionist view of privacy was presented by Judith Jarvis Thomson in 1975. According to her well-known argument, there is no right to privacy, or at least there is nothing special about privacy, because any interest protected as private can be equally well explained and protected by other interests or rights, most notably rights to property and bodily security. First noting that there is little agreement on what privacy is, Thomson then examines a number of cases that have been thought to be violations of the right to privacy. Thomson argues that, on closer inspection, all those cases can be adequately explained in terms of violations of property rights or rights over the person, such as a right not to be listened to or a right not to be touched. Ultimately the right to privacy, in Thomson's view, is merely a cluster of rights, and those rights in the cluster are always overlapped by, and can be fully explained by, other property rights or rights to bodily security. The right to privacy, in her view, is "derivative" in the sense that there is no need to find what is common in the cluster of privacy rights. Privacy is derivative in its importance and justification, according to Thomson, since any privacy violation is better understood as the violation of a more basic right.

Numerous commentators such as Thomas Scanlon have argued strongly against Thomson's critique of privacy. Scanlon has persuasively countered that it is surely as plausible that just the reverse of Thomson's view is true, and that rights such as those of ownership or even liberty are "derivative" from privacy rights. Scanlon apparently finds this ordering likely since he believes there is something unique and of special value to privacy.

Many other theorists have agreed with Scanlon (i.e., Inness, Rachels) in rejecting reductionism's claim that privacy is reducible to other values, and have argued that privacy is a coherent concept. In this view, there is something fundamental and distinctive about the various claims that have been called privacy interests. Ruth Gavison, for example, claims that most individuals believe privacy is a useful concept, and according to Gavison, privacy has value as a coherent and illuminating concept. Those who endorse such a view may be called coherentists. Nevertheless, it is important to recognize that coherentists have quite diverse although sometimes overlapping views on what it is that is distinctive about privacy and what links diverse privacy claims.

III. Coherentists on the Meaning and Value of Privacy

Although most theorists have taken the coherentist view that privacy is a meaningful and valuable concept, their characterizations and defenses of privacy differ. Narrow views of privacy focusing on control over information about oneself that were defended by Warren and Brandeis in their 1890 law review article and by other legal theorists such as William Prosser have also been endorsed by more recent commentators, including Charles Fried and William Parent. Westin also



describes privacy as the ability to determine for ourselves when, how, and to what extent information about us is communicated to others.

Perhaps the best example of a contemporary defense of this view of privacy as control over information about oneself is put forth by Parent in two related papers. Parent urges that he proposes to defend a view of privacy that is consistent with ordinary language and does not overlap with or confuse the basic meanings of other fundamental terms. He defines privacy as the condition of not having undocumented personal information known or possessed by others. Parent stresses that he is defining the “condition” of privacy as a moral value for people who prize individuality and freedom, and not as a moral or legal right to privacy. Personal information is characterized by Parent as factual (otherwise it would be covered by libel, slander, or defamation), and these are facts that most persons choose not to reveal about themselves, such as facts about health, salary, weight, or sexual orientation. Personal information is documented, in Parent’s view, only when it belongs to the public record, that is, in newspapers, court records, or other public documents. Thus, once information becomes part of a **public record**, there is no privacy invasion in future releases of the information, even years later or to a wide audience, nor does snooping or **surveillance** intrude on privacy if no undocumented information is gained. In cases where no new information is acquired, Parent views the intrusion as irrelevant to privacy, and better understood as an abridgement of **anonymity**, **trespass**, or harassment. In sum, there is a loss of privacy, in Parent’s view, only when others acquire undocumented personal information about an individual.

Parent’s account of privacy has the valuable feature of defending privacy as a coherent concept, and he also takes the view that there is something unique, fundamental, and of special value in privacy. But his characterization of privacy has some troubling consequences. First, once information becomes part of a public record, then the individual concerned has no recourse if there is any further publication of the information because it is not a privacy violation, even if it occurs far in the future and involves a much wider distribution. That seems counterintuitive, especially if the original disclosure is made in error or is accomplished through moral wrongdoing. Second, even insidious snooping will not count as a privacy invasion on Parent’s account if all the information gathered is already a part of the public record. And unjustified spying will not give rise to a privacy intrusion if no new undocumented knowledge is acquired. Methods of acquiring information are not always determinative of a privacy invasion, but the mode of acquisition cannot be said to be irrelevant, as is apparently the case on Parent’s view. Insidious snooping and unjustified spying seem to give rise to reasonable claims of a privacy invasion even if no new knowledge is gathered or if whatever is learned is already part of a public record. Third, Parent’s emphasis on what is as a matter of fact a part of the public record, seems to ignore or blur the important distinction between a descriptive sense of privacy and a normative concept of privacy encompassing what is worthy of protection.

Edward J. Bloustein, in an article written partly as a defense of the Warren and Brandeis law review essay on privacy, also argued that there is a common thread in the legal cases protecting diverse privacy issues. Despite appearing in a law review, the article gives a philosophical defense of privacy that is perhaps best seen as

being very Kantian. According to Bloustein, Warren and Brandeis failed to give a positive description of privacy; however, they were correct that there was a single value connecting the privacy interests, a value they called “inviolable personality.” In Bloustein’s view it is possible to give a general theory of individual privacy that unifies and reconciles its divergent strands, and then conclude that “inviolable personality” is the social value protected by privacy. It defines one’s essence as a human being, and it includes individual dignity and integrity as well as personal autonomy and independence. Respect for these values is what grounds and unifies the concept of privacy. Bloustein defends the view that privacy rights are important because they protect against intrusions demeaning to personality and against affronts to human dignity. Using this analysis, Bloustein urges that privacy violations leave an individual open to scrutiny in a way that leaves one’s autonomy and sense of self as a person vulnerable, violating one’s human dignity and moral personality. Invasion of privacy is best understood, in sum, as an affront to human dignity. Although Bloustein admits the terms he uses are somewhat vague, he defends this analysis as conceptually coherent and illuminating.

A third coherentist and more common view have been to argue that privacy and intimacy are deeply related. In one account defended by numerous philosophers, including Thomas Gerety and Richard Gerstein, privacy is valuable because intimacy would be impossible without it. Charles Fried, for example, defines privacy narrowly as control over information about oneself. He extends this definition, however, by arguing that privacy has intrinsic value and is necessarily related and fundamental to one’s development as an individual with a moral and social personality able to form intimate relationships involving respect, love, friendship, and trust. Privacy is valuable because it allows one to control information about oneself, which in turn allows one to maintain varying degrees of intimacy and define oneself and one’s relations to others. Indeed, love, friendship, and trust are only possible if persons enjoy privacy and accord it to each other. Fried argues that privacy is essential for such relationships, and this helps explain why a threat to privacy is a threat to people’s very integrity as persons. By characterizing privacy as a necessary context for love, friendship, and trust, Fried bases his accounts on a moral conception of persons and their personalities, on a Kantian notion of human beings with basic rights and the need to define and pursue their own values free from the impingement of others. Privacy allows us the freedom to define our relations with others and to define ourselves. In this way, privacy is also closely connected with self-respect and respect for others.

Gerstein argues as well that privacy is necessary for intimacy, and urges that intimacy in communication and interpersonal relationships is required for people to fully experience their lives. Intimacy without intrusion or observation is required for people to have experiences with spontaneity and without shame. Shoeman also endorses these views and stresses that privacy provides a way to control intimate information about oneself, and that it has many other benefits, not only for relationships with others, but also for the development of one’s personality and inner self. Julie Inness has also identified intimacy as the defining feature of intrusions properly called privacy invasions. According to Inness, intimacy is based not on behavior but on motivation, and so intimate information or activity is that which draws its meaning from love, liking, or care. It is privacy that protects one’s ability to retain



intimate information and activity so that one can fulfill one's needs of loving and caring.

A number of commentators have defended views of privacy that link closely with accounts stressing privacy as required for intimacy, but they emphasize not only intimacy but also the general importance of developing diverse interpersonal relationships with others. James Rachels, for example, acknowledges there is no single answer to the question of why privacy is important to us, because it can be necessary to protect one's assets or interests, or to protect one from embarrassment, or to protect one against the deleterious consequences of information leaks, to name just a few. Nevertheless, he explicitly criticizes Thomson's reductionist view and urges that privacy is a distinctive right. He basically defends the view that privacy is necessary to maintain a variety of social relationships, not just intimate ones. Privacy accords us the ability to control who knows what about us and who has access to us, and thereby allows us to vary our behavior with different people so that we may maintain and control our various social relationships, many of which will not be intimate. An intriguing part of Rachels's analysis of privacy is that it emphasizes ways in which privacy is not merely limited to control over information, because individuals' ability to control information and access to themselves allows them to control relationships with others, and thus is connected to their decisions and behavior.

Another group of theorists present a fifth coherentist view that characterizes privacy in terms of access, usually describing privacy as exclusive access of a person to a realm of his or her own. Sissela Bok discusses the complex relationships between privacy and **secrecy**, and she argues that privacy protects people from unwanted access by others—either physical access or personal information or attention. Ruth Gavison has defended this more expansive view of privacy in greater detail. Her extended definition is “privacy is a limitation of others' access to an individual. . . . [An] individual enjoys *perfect* privacy when he is completely inaccessible to others. . . . [I]n perfect privacy no one has any information about X, no one pays attention to X, and no one has physical access to X.” Noting that perfect privacy is impossible in any society, she argues that interests in privacy are related to concerns over accessibility: what others know about us, the extent to which we are the subject of the attention of others, and the extent to which they have physical access to us. Thus the concept of privacy is best understood as a concern for limited accessibility, and one has perfect privacy when one is completely inaccessible to others. In sum, privacy can be gained in three independent but inter-related ways: when one has secrecy because no one has information about one, when one has anonymity because no one pays attention to one, and when one has solitude because no one has physical access to one. Gavison's view is that the concept of privacy is this complex of concepts that are all part of the notion of accessibility. Furthermore, she concludes that the concept is also coherent because of the related functions privacy has, namely “the promotion of liberty, autonomy, selfhood, and human relations, and the furthering the existence of a free society.”

Anita Allen also characterizes privacy as denoting a degree of inaccessibility of persons, their mental states, and information about them to the senses and surveillance of others. She views seclusion, solitude, secrecy, **confidentiality**, and anonymity as forms of privacy. She also urges that privacy is required by the liberal

ideals of personhood, as well as the participation of citizens as equals. While her view appears to be similar to Gavison's, Allen suggests her restricted access view is broader than Gavison's. This is in part because Allen emphasizes that in public and private, women experience privacy losses that are unique to their **gender**. Noting that privacy is neither a presumptive moral evil nor an unquestionable moral good, Allen nevertheless defends more extensive privacy protection for women in morality and in the law. Using examples such as **sexual harassment**, victim anonymity in rape cases, and reproductive freedom, Allen emphasizes the moral significance of extending privacy protection for women.

IV. The Feminist Critique of Privacy

Despite these many defenses of privacy, discussion of the concept is complicated by the fact that privacy appears to be both something we value in order to provide a sphere within which we can be free from scrutiny, coercion, or the judgment of others, and yet it also appears to function negatively, as feminists have emphasized, as the cloak under which one can hide domination, degradation, or physical harm to women and others. This is the feminist critique of privacy, namely that granting special status to privacy is detrimental to women and others because it is used as a shield to dominate and control them, silence them, and cover up abuse. There is no single version of the feminist critique of privacy, yet it can be said in general that many feminists have worried about what they view as this darker side of privacy. If distinguishing public and private realms leaves the private free from any scrutiny, then feminists such as Catharine MacKinnon are correct that privacy can be dangerous for women when it is used to cover up repression and physical harm to them by perpetuating the subjection of women in the domestic sphere and encouraging nonintervention by the state. Elshtain and Gavison have suggested that it appears feminists such as MacKinnon are, for this reason, rejecting the public/private split, and are, moreover, recommending jettisoning or abandoning privacy altogether. But as Elshtain and Gavison point out, this alternative seems too extreme. A more reasonable view, according to Allen and my own analysis, is to recognize that while privacy can be a shield for abuse, it is inadequate to reject privacy completely based on harm done in private. These accounts may be viewed as one reply to the feminist critique of privacy, allowing that privacy can be a shield for abuse, but can also be so valuable for women that privacy protection should be enhanced, not diminished.

A total rejection of privacy makes everything public, and it leaves the domestic sphere open to complete scrutiny and intrusion by the state. Yet women surely have an interest in privacy that can protect them from state-imposed **sterilization** programs or government-imposed drug tests for pregnant women—and mandating that results be sent to police, for instance—and that can provide reasonable regulations granting rights against marital rape, for example. Thus collapsing the public/private dichotomy into a single public realm is inadequate. What puzzles feminists is how to make sense of an important and valuable notion of privacy that provides them a realm free from scrutiny and intervention by the state, without reverting to the traditional public/private dichotomy that has in the past relegated women to the private and domestic sphere where they are victims of subjection and abuse. The challenge is to find a way for the state to take very seriously the domestic abuse

that used to be allowed in the name of privacy, while also preventing the state from insinuating itself into all the most intimate parts of women's lives. This means drawing new boundaries for justified state intervention and thus understanding the public/private distinction in new ways.

V. The Scope of Privacy

A further issue that has generated disagreement, even among those theorists who believe privacy is a coherent concept, is whether or not privacy cases in constitutional law, involving personal decisions about lifestyle and family such as **birth control**, interracial marriage, viewing pornography at home, **abortion**, and so on, delineate a genuine category of privacy issues, or are merely concerns with liberty of some sort. Parent explicitly excludes concerns about one's ability to make certain important personal decisions about one's family and lifestyle as genuine privacy issues, saying the cases focus solely on liberty. Reductionist Thomson shares this view, as do others who characterize privacy narrowly as control over information about oneself. Allen defines privacy in terms of access and excludes from her definition protection of individual autonomous choice from governmental interference, which she terms a form of liberty. Yet she refers to this latter protection as "decisional privacy" and says determining its category is purely a definitional point and one of labels. Ultimately she believes interference with decisions involving procreation and sexuality raise the same moral concerns as other privacy intrusions that offend the values of personhood.

The Supreme Court has claimed that there are two different dimensions to privacy: (1) an "individual interest in avoiding disclosure of personal matters" and (2) an "interest in independence in making certain kinds of important decisions" (see *Whalen v. Roe*, 429 U.S. 589, 599, 600 (1976)). Influenced by this reasoning, a number of theorists have defended the view that privacy has broad scope, inclusive of the various types of privacy issues described by the Court, even though there is no simple definition of privacy. Most of these theorists have explored the links between the types of privacy interests and the similarity of reasons for valuing each. Some stress that privacy is necessary for one to develop a concept of self as a purposeful, self-determining agent. Privacy enables control over personal information as well as control over bodies and personal choices in order to develop and maintain a concept of self (Kupfer). Some emphasize the importance of intimacy for all privacy issues, noting the need for privacy to protect intimate information about oneself, access to oneself, intimate relationships, and decisions about one's actions (Inness). Some focus on the importance of privacy as a set of norms that allow one to control or restrict others' access to oneself, as well as norms that enable and enhance personal expression, choice, and the development of relationships. Privacy provides protection against overreaching social control by others through the others' access to information as well as through their control over decisionmaking (see Schoeman). DeCew argues that privacy is best understood as a coherent cluster concept covering interests in control over information about oneself; control over access to oneself, both physical and mental; and control over one's ability to make important decisions about family and lifestyle in order to be self-expressive and to develop varied relationships. These three interests are related and coherent as a cluster because in each of these three contexts there are threats—threats of

information leaks, threats of control over individuals' bodies, and threats to individuals' power to make their own choices about their bodies and activities—that all make individuals vulnerable and fearful that they are being scrutinized, pressured, or taken advantage of by others. Privacy is a coherent concept with moral value because it shields us by providing certain freedom—freedom from scrutiny, prejudice, pressure to conform, exploitation, and the judgment of others.

Despite disagreements over the meaning and value of privacy, and the appropriate scope of privacy protection, it is safe to conclude that most philosophers defend the unique and fundamental value of privacy protection despite the difficulties inherent in its definition and its potential use to shield abuse.

See also: **Constitutional protections; Gender; Privacy, definition of; Reproductive rights; Women and privacy**

Suggested Reading: Allen, Anita L. *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability*. Lanham, MD: Rowman & Littlefield, 2003; Aristotle. *The Politics*, trans. Benjamin Jowett. In Richard McKeon (ed.), *The Basic Works of Aristotle*, pp. 1127–1324. New York: Random House, 1941; Bloustein, Edward J. "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser," *New York University Law Review* 39 (1964): 962–1007; Bok, Sissela. *Secrets: On the Ethics of Concealment and Revelation*. New York: Pantheon, 1982; DeCew, Judith Wagner. *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*. Ithaca, NY: Cornell University Press, 1997; Elshtain, Jean Bethke. *Democracy on Trial*. New York: Basic Books, 1995; Elshtain, Jean Bethke. *Public Man, Private Woman: Women in Social and Political Thought*. Princeton, NJ: Princeton University Press, 1981; Fried, Charles. *An Anatomy of Values*. Cambridge, MA: Harvard University Press, 1970; Gavison, Ruth. "Feminism and the Public/Private Distinction," *Stanford Law Review* 45, no. 1 (1992): 28–29; Gavison, Ruth. "Privacy and the Limits of Law," *Yale Law Journal* 89 (1980): 421–471; Gerety, Thomas. "Redefining Privacy," *Harvard Civil Rights-Civil Liberties Law Review* 12 (1977): 233–296; Gerstein, Richard. "Intimacy and Privacy," *Ethics* 89 (1978), 76–81; Inness, Julie. *Privacy, Intimacy and Isolation*. Oxford: Oxford University Press, 1992; Kupfer, Joseph. "Privacy, Autonomy and Self-Concept," *American Philosophical Quarterly* 24 (1987): 81–89; Locke, John. *The Second Treatise on Government*, ed. Thomas P. Reardon. New York: Macmillan, Library of Liberal Arts, 1988; MacKinnon, Catharine. *Toward a Feminist Theory of the State*. Cambridge, MA: Harvard University Press, 1989; Mead, Margaret. *Coming of Age in Samoa*. New York: New American Library, 1949; Mill, John Stuart. *On Liberty*. New York: Penguin, 1976; Parent, William. "A New Definition of Privacy for the Law," *Law and Philosophy* 2 (1983): 305–338; Parent, William. "Privacy, Morality and the Law," *Philosophy and Public Affairs* 12 (1983): 269–288; Paul, Jeffrey, Fred Miller, and Ellen Paul (eds.). *The Right of Privacy*. Cambridge: Cambridge University Press, 2000; Prosser, William. *Handbook of the Law of Torts*, 2nd ed. St. Paul, MN: West, 1955; Rachels, James. "Why Privacy is Important," *Philosophy and Public Affairs* 4 (1975): 323–333; Reiman, Jeffrey. "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future," *Santa Clara Computer and High Technology Law Journal* 11 (1995): 27–42; Scanlon, Thomas. "Thomson on Privacy," *Philosophy and Public Affairs* 4 (1975): 315–322; Schoeman, Ferdinand. *Privacy and Social Freedom*.



Cambridge: Cambridge University Press, 1992; Schoeman, Ferdinand F. (ed.). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press, 1984; Thomson, Judith Jarvis. "The Right to Privacy," *Philosophy and Public Affairs* 4 (1975): 295–314; Warren, Samuel, and Louis Brandeis. "The Right to Privacy," *Harvard Law Review* 4 (1890): 193–220; Westin, Alan. *Privacy and Freedom*. New York: Atheneum, 1967.

Judith Wagner DeCew

Privacy Act of 1974

The Privacy Act of 1974 was the first comprehensive privacy law enacted in the world. It regulates the collection, use, maintenance, **disclosure**, and disposition of personal information by U.S. federal executive branch agencies, and provides rights to certain individuals about whom records are maintained. It establishes civil and criminal penalties for violations of the law and assigns the Office of Management and Budget as the agency responsible for providing guidance and overseeing implementation by the other agencies. The Privacy Act recognizes that government must collect information necessary to run its programs and carry out its various missions, but it seeks to limit unnecessary intrusions or unfair practices associated with government use of information.

Prior to passage of the Privacy Act, changes in American society generated growing concern about the use of automated data systems to keep records about people, especially by the federal government. At that time, the federal government was one of few organizations that had significant **personally identifiable information**, access to large data storage and processing capabilities, and the resources to use them. The public concern about the issues posed by automation of personal record-keeping systems prompted the secretary of what was then the Department of Health, Education, and Welfare to convene the Advisory Committee on Automated Personal Data Systems. The Advisory Committee's report recommended passage of a code of **fair information practices** comprising five basic principles that became the foundation for the act: (1) there must be no personal data recordkeeping systems whose very existence is secret; (2) there must be a way for individuals to find out what data about them are kept and how the data are used; (3) there must be a way for individuals to prevent information about themselves obtained for one purpose from being used or made available for other purposes without their consent; (4) there must be a way for individuals to correct or amend records about themselves; and (5) any organization creating, maintaining, using, or disseminating records including personally identifiable information must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

The Privacy Act was passed on December 31, 1974, in the final week of the 93rd Congress, in the wake of the Watergate scandal. Instead of the usual practice of convening a conference committee of senators and representatives to reconcile differences between bills passed by the two houses of Congress, staff members from the key committees of the House and Senate put together the final bill that ultimately was enacted. In lieu of the traditional accompanying conference report, the staff produced a document, titled "Analysis of House and Senate Compromise Amendments to the Federal Privacy Act," that was submitted to both houses of

Congress and is generally considered more reliable than the original committee reports as legislative history for interpreting the statute.

In passing the Privacy Act, there was a desire to circumscribe the scope of coverage of the law. The law does not cover all personally identifiable information, nor all such information held by the federal government, but only that which falls into the ambit of certain key definitions. In general, the protections extend only to information about an individual maintained by a United States federal executive branch agency, connected to an identifier particular to the individual, and retrieved by that identifier. Such information is said to be in a “system of records.”

The act explicitly includes as examples of identifiers, in addition to name or identifying number, a **fingerprint**, voice print, or photograph. For example, a system of records might be a cabinet of files arranged alphabetically or by **Social Security number** that would allow someone to retrieve the file about a particular person directly. The same information filed chronologically would not be covered, since getting to any particular individual’s record would potentially require searching through the entire file cabinet to locate the record.

Only persons who are natural United States citizens or lawful, permanent resident aliens enjoy the protections of the act. Neither deceased persons nor organizations or businesses of any kind are covered, although in some cases sole proprietors of businesses may have Privacy Act rights. Likewise, information in the custody of the Congress, the Supreme Court, the immediate office of the White House, or a state or local governments is not covered.

A system of records may be composed of paper or electronic files. However, despite the fact that the law emerged as a result of concerns stemming from developments in automatic data processing, it was not written to accommodate modern, sophisticated electronic records systems. In the era of databases searchable by keyword, **data mining**, and other innovations, almost anything might be considered a system of records. This issue was directly addressed by the Court of Appeals for the District of Columbia Circuit in *Henke v. Commerce* (1996), when it held that it is not just the ability to retrieve the records that involves the Privacy Act, but the fact that an agency must actually retrieve records in order for a system of records to exist.

The major responsibility of agencies is to safeguard from improper disclosure the information in its systems of records. The Privacy Act model established the framework for many disclosure laws that succeeded it, setting up the basic rule that an agency may not disclose information by any means without the written consent of the subject individual unless the disclosure falls into one of a number of exceptions. The most often used statutory exception permits disclosures within an agency to other employees who have a need for the information to carry out their duties. Another commonly used exception permits disclosures that are required by the **Freedom of Information Act**. There are also disclosure exceptions to accommodate law enforcement requests and court orders that meet certain standards; in the case of “compelling circumstances” affecting the health or safety of an individual; for carrying out censuses and other statistical uses; to the Congress or the comptroller general; and to the National Archives and Records Administration (NARA) for managing the process of accumulating permanently valuable records.

In addition to these specific statutory disclosure exceptions, the Congress enacted another provision, the use of which permits agencies to add, via an administrative

process, new disclosures that might be necessary to conduct business. This provision accommodates disclosures that were not contemplated and could not be predicted or anticipated at the time of passage of the act. The controversial exception, called a “routine use,” is a term of art that refers to a disclosure of a record outside the custodial agency “for a purpose which is compatible with the purpose for which it was collected.” These generally fall into three categories: (1) those where there is a direct connection to the reason for which the information was collected—for example, disclosure to a contractor for contracted work; (2) those that are necessary and proper—for example disclosure to a law enforcement agency to investigate fraud in an agency’s program; or (3) those disclosures required by statute, whether or not related to the program purpose of the system of records. An agency wishing to add a routine use disclosure must publish notice of a new or significantly altered routine use in the *Federal Register*; solicit comment from the public, and report the disclosure to Office of Management and Budget and both houses of the Congress. This ability to add new disclosures and broaden the use of personal information through a simple administrative process has generated considerable criticism.

Although widely thought of as merely an access and disclosure law, the Privacy Act is more properly classified as an information resources management statute in that it regulates how federal agencies collect, use, maintain, and dispose of significant collections of records. The law limits an agency to collecting only that information “relevant and necessary” to its mission, and requires that information be collected “to the greatest extent practicable” from the subjects themselves when it may be used as the basis of any significant decisions about them. It further requires that the agency maintain the records in a manner that is accurate, relevant, timely, and complete, and that it review the records for these characteristics prior to disseminating them outside the agency. Agencies are required to establish rules of conduct for their employees handling Privacy Act records as well as appropriate safeguards to guard against anticipated threats to the security of the records.

To implement the code of fair information practice’s first principle that there should be no secret recordkeeping systems, agencies are required to publish in the *Federal Register* a notice about the existence and character of each system of records. Such notices describe the name, location, and manager of the system of records; the categories of individuals, sources of information, and types of records maintained; the policies of the agency regarding storage, security, retention, and disposal; the routine uses associated with the records, and the agency procedures whereby subjects of the records can gain access or contest the content of the records.

In addition, when collecting information, agencies are required to notify individuals at the time of the collection about the authority for the collection, whether responding is mandatory or voluntary, the purpose of the collection, the routine uses, and the consequences, if any, that would result if the individual failed to respond to the request.

Besides the right to these two types of notices, the Privacy Act affords individuals the right to see and, for a nominal fee, to obtain a copy of information maintained about them. It also affords individuals the right to request an amendment of information that is not accurate, relevant, timely, or complete. In the case of an

agency's refusal to amend a record, an individual may request to add a concise statement describing the reasons for disagreement with the agency. If an agency refuses to provide access, make the requested amendment, or simply fails to respond to a request, an individual may appeal for a further review, and the individual may also seek a civil remedy through a judicial review of the reviewing official's determination.

In addition to civil actions related to access or amendment requests, an individual may bring suit against the agency in the district courts of the United States if an agency fails to maintain records in accordance with the standards set forth in the law, or fails to comply with any other provision of the act, and the individual suffers some adverse consequence. An individual is entitled to actual damages sustained, with a minimum recovery of \$1000, plus costs and reasonable attorney fees. However, it is extremely difficult to prevail in a civil action under the Privacy Act, and not many suits are brought under the law. Success requires a showing of willful and intentional misconduct, a connection between the agency's failure to comply and the harm done to the individual, and actual out-of-pocket damages.

Congress established criminal penalties for violation of the Privacy Act as well. It is a crime for an officer or employee of an agency to willfully disclose Privacy Act records knowing they are protected by the act. It is a crime to maintain a secret system of records, that is, without having published the proper notice in the *Federal Register*. Finally, it is a crime for any person—an employee of an agency, an individual, or a corporate entity—to knowingly and willfully request or obtain a record under false pretenses. Criminal violation of the Privacy Act is a misdemeanor and carries a maximum fine of \$5000. There are only two known prosecutions for criminal violation of the Privacy Act. This is because it is difficult to prove beyond a reasonable doubt that a defendant knowingly and willfully disclosed information, and because the penalties are scant compared to other priorities of the Justice Department.

Under some circumstances, an agency may promulgate regulations to exempt itself from certain provisions of the Privacy Act. Two general exemptions permit the **Central Intelligence Agency (CIA)** or any agency that performs as its principle function the enforcement of criminal laws to exempt itself from most of the requirements of the Act. While the CIA may exempt any system of records under this provision, a criminal law enforcement agency may only exempt those records compiled for a criminal law enforcement purpose. An agency cannot exempt itself from the provisions regarding disclosures; keeping and maintaining an accounting of disclosures; publishing notice in the *Federal Register*; making reasonable efforts to disseminate records that are accurate, relevant, timely, and complete; prohibiting maintenance of records on how an individual exercises rights guaranteed by the First Amendment; establishing rules of conduct for employees and appropriate administrative, technical, and physical safeguards; or establishing routine uses.

Seven specific exemptions apply to particular types of information that an agency may maintain, permitting an agency to exempt itself from the requirements to make the accounting of disclosures available to the subject; grant access, amendment, and appeal rights; limit collection to only information that is relevant and necessary; or describe the sources of categories of records in the



Federal Register notice. The seven exemptions protect classified information; investigatory material compiled for a law enforcement purpose that does not meet the general exemption's requirements; records of the Secret Service related to protecting the president or others similarly protected; records required by statute to be maintained and used solely as statistical records; background investigation records; civil service examination records; and military promotion evaluations. In the case of the law enforcement, background investigation, and military evaluation records, the exemption only extends to information that would reveal the identity of a source who furnished information under a promise that his or her identity would be held in confidence.

Section 7 of the Privacy Act contains provisions regarding the collection of Social Security numbers. Section 7, unlike the rest of the act, applies to any federal, state, or local government agency. It prohibits such an agency from denying an individual any right, benefit, or privilege provided by law because that individual refuses to divulge his or her Social Security number. It also requires the agency to furnish notice each time it solicits a Social Security number, detailing whether the disclosure is mandatory or voluntary, by what authority the information is solicited, and what uses will be made of it.

There are two significant exceptions to the first provision. A government agency may deny an individual a right, benefit, or privilege for failure to divulge a Social Security number (1) if the disclosure is required by a federal statute or (2) if the disclosure was required by a statute or regulation adopted before passage of the Privacy Act, and the government entity was actually collecting and maintaining Social Security numbers before that date. Many federal statutes have been passed that permit governments to require Social Security numbers, including drivers' licensing, applying for federal loans and benefits, and tax administration.

[The views expressed in this article do not necessarily represent those of the Department of Health and Human Services or the United States.]

Suggested Reading : Bennett, Colin, and R. Grant (eds.). *Visions of Privacy*. Toronto: University of Toronto Press, 1999; Flaherty, David H. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill: University of North Carolina Press, 1992; Office of Management and Budget. "Privacy Act Implementation: Guidelines and Responsibilities," *Federal Register* 40 (1975): 28948–28978; Office of Management and Budget. *Privacy Guidance and Privacy Reference Materials*. <http://www.whitehouse.gov/omb/inforeg/infopoltech.html>. Online, March 2006; Regan, Priscilla. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press, 1995; U.S. Department of Health, Education and Welfare. Advisory Committee on Automated Personal Data Systems. *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*. Washington, DC: U.S. Government Printing Office, 1973; U.S. Department of Justice. Office of Information and Privacy. *Freedom of Information Act Guide and Privacy Act Overview*. Washington, DC: U.S. Government Printing Office, 2006.

Maya A. Bernstein

Privacy advocacy organizations

The 1980s marked the arrival of the information age with an explosion of information and **surveillance** technologies that would fundamentally reconfigure the social landscape. By the end of the decade, the convergence of **computer** and telecommunications systems had expanded the capacity to collect, process, and disseminate personal information at unprecedented rates. By 1990, a number of privacy advocacy organizations had formed in response to the purported threats to personal privacy these technologies had created. Organizations such as the Electronic Privacy Information Center (EPIC), Privacy International (PI), and the Electronic Frontier Foundation (EFF) have mobilized resources on a number of fronts to influence privacy policy at the state, federal, and international levels. Their efforts typically include lobbying for increased privacy protection, legal challenges, and the dissemination of information to the general public. As such, these organizations play an increasingly integral role in the development of privacy policy in the United States and in the international community.

One of the first privacy advocacy organizations formed in response to the growth of information technologies was the Electronic Frontier Foundation (EFF). The group was founded in 1990 by former Grateful Dead songwriter, John Barlow; Mitchell Kapor, the founder of the Lotus software company; and John Gilmore, who was also involved in the creation of Sun Microsystems. The group gained national attention because of the legal cases with which it became involved, including the case of Steve Jackson Games. In this case, the **Federal Bureau of Investigation (FBI)** seized computers and equipment from the gaming company while it was investigating one of the company's employees for hacking. The loss of equipment nearly caused the company to go bankrupt. EFF helped Steve Jackson sue the government, and it was ruled that the FBI had violated the **Privacy Act of 1974** and the **Electronic Communication Privacy Act of 1986**.

EFF focuses primarily on issues of digital rights, including free speech, privacy, innovation, and consumer rights. Although its efforts are primarily focused in the courts, it also advises policymakers, educates the media and the public, and funds the development of "freedom-enhancing" technologies. Its recent activities include litigation against AT&T for violating the law and its customers by collaborating with the **National Security Agency (NSA)** in its massive program to wiretap and data-mine the communications of Americans. It also has filed suit against Sony BMG for including undisclosed software on its CDs that reports customer listening habits and installs hidden files on users' computers that make them vulnerable to third-party attacks. EFF has also recently released a report analyzing the unintended ways that the Digital Millennium Copyright Act undermines free market competition and hinders scientific research and technological development.

The year 1990 also marked the founding of Privacy International. This organization was formed when over 100 privacy experts and human rights organizations joined together to form a worldwide network oriented toward privacy protection. Still one of the leading privacy advocacy groups in the world, PI is composed of a wide range of individuals, including lawyers, academics, journalists, jurists, computer scientists, and human rights activists. Primarily conceived as a watchdog over surveillance by governments and corporations, PI focuses on issues of cybercrime,



freedom of information, ID cards, digital money, outsourcing, **wiretapping** and encryption, and video surveillance.

PI differentiates itself from many other privacy advocacy organizations with its emphasis on an international approach to privacy policy. It has spearheaded public campaigns in a number of countries to push for privacy policy reform. PI worked closely with human rights groups in Thailand and the Philippines to campaign against the establishment of **national identity card** programs. It has also been active in lobbying former Communist countries in Central and Eastern Europe to become more accountable through the adoption of freedom of information policies. At the same time, PI monitors the activities of international organizations, such as the European Union (EU) and the United Nations in order to focus international attention on the policy initiatives of these organizations.

Another leading privacy advocacy organization is the Electronic Privacy Information Center (EPIC), which was founded in 1994 by lawyers Marc Rotenberg, David Banisar, and David Sobel. The trio first gained public attention through their successful public relations campaign against Lexis-Nexis, in which they were able to force the company to close down a database that contained the **Social Security numbers** of many individuals. Building on the success of this early effort, the three lawyers established EPIC in order to raise public awareness of the emergent civil liberties issues regarding privacy and freedom of expression associated with the onset of the information age. Through advocacy, litigation, policy research, publications, and public education, EPIC has continued to further its program to protect individual privacy rights. EPIC is currently involved in the national discussions on the privacy implications of Department of Homeland Security's activities regarding **electronic surveillance** and border monitoring, and the Department of Transportation's use of aviation passenger profiling, **data mining**, and **radio frequency identification (RFID)**. Additionally, it maintains two of the leading websites on privacy: epic.org and privacy.org (the latter of which is co-sponsored with Privacy International).

The Privacy Rights Clearinghouse (PRC) was founded by Beth Givens in 1992 in order to increase awareness of consumer privacy issues. PRC offers services tailored to the specific needs of consumers, members of the media, and legislators. PRC offers consumers fact sheets on 31 issues in order to provide practical advice and information about securing their privacy. Some of the issues included in these fact sheets are **telemarketing**, financial privacy, identity theft, and employment **background checks**. PRC also offers consumers a comprehensive listing of privacy laws and current legislation across the United States. It works closely with the media and legislators by providing readily available access to staff members, maintaining a listing of problems currently being experienced by consumers, and connecting journalists and legislators with consumers willing to be interviewed or testify. Additionally, PRC publishes research reports on privacy issues and actively lobbies for stronger privacy legislation.

In 1994 the Center for Democracy and Technology (CDT) was created by Jerry Berman in order to develop practical solutions to enhance free expression and privacy in global communications technology. Located in Washington, DC, CDT has become a powerhouse on Capitol Hill, partly because of its success in building coalitions between corporations and social activist groups (entities that are routinely at

odds with each other regarding issues of privacy). This emphasis on reaching compromises between competing groups has caused the CDT to be viewed poorly by some privacy advocates such as EPIC's Marc Rotenberg. Nevertheless, many lawmakers respect the members of CDT because they are not only strong advocates of privacy rights, but also because they actively engage in the political meetings in which legislative language is created. CDT is currently involved in protecting privacy rights in a number of areas, including efforts to quash the use of spyware, challenging the Department of Homeland Security for its disregard of the Privacy Act, and developing legislation aimed at punishing copyright infringement while still promoting innovation and protecting consumer rights.

Finally, the Privacy Foundation (PF) provides another model for privacy advocacy organizations. Unlike the other organizations discussed in this entry, PF is not a private organization but a policy research center associated with the Sturm School of Law at the University of Denver. The foundation focuses primarily on research, particularly on analyses of communications technologies and services that may pose a threat to personal privacy. It also conducts numerous public seminars and helps members of the business community and privacy advocates in policy development. PF's endeavors have included an expansive research project investigating employee monitoring in American workplaces and the analysis of the privacy implications of the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)**.

The above organizations are among the most prominent privacy advocacy organizations in the United States. There are, however, hundreds if not thousands of other advocacy groups that deal with privacy issues in the United States and throughout the world, ranging from local grassroots groups to large national and international privacy organizations. Furthermore, since the early 1990s, organizations such as the National Organization of Women (NOW) and the **American Civil Liberties Union (ACLU)** that focus on a wide range of social issues have increasingly engaged in the debates on privacy. Together, all these organizations play an important role in establishing and protecting individual privacy rights.

See also: **Cryptography; Identity fraud; Journalism**

Suggested Reading: Center for Democracy and Technology. www.cdt.org. Online, April 2006; Electronic Frontier Foundation. www.eff.org. Online, April 2006; Electronic Privacy Information Center. www.epic.org. Online, April 2006; Privacy.Org. www.privacy.org. Online, April 2006; Privacy Foundation. www.privacyfoundation.org. Online, April 2006; Privacy International. www.privacyinternational.org. Online, April 2006; Privacy Rights. www.privacyrights.org. Online, April 2006.

Brian L. Zirkle

Privacy and inequality

Privacy raises many social issues. One insufficiently considered issue involves implications for equality. The work of Karl Marx, Max Weber, and Michel Foucault on the development of the modern state suggests that inequality is one result of the use of technologies to collect personal information. This may involve monitoring workers or determining the characteristics of those processed by bureaucratic organizations, such as the military, schools, and hospitals.



The control over information—a defining characteristic of privacy—is a resource related to, but with varying degrees of independence from, other scarce social resources such as class, status, and power. Such resources are the basis for stratification in society. As **computers** become ever more important, questions about the extent and consequences of a “digital divide” appear. Is society becoming increasingly stratified on the basis of access to information? Privacy issues are strands of this much broader tapestry. The connection between knowledge and power is strong, even if, in spite of Enlightenment verities, there are times when the richness and dynamic nature of social reality weakens or reverses the link. Yet, on balance, differential access to information favors the privileged—whether individuals, groups, countries, or regions.

Rules regarding who can collect **personally identifiable information**, what is collected, the conditions under which it is gathered, and how it is used—and by whom—are very much connected to social stratification. Many contemporary concerns over privacy invasion involve large organizations and their employees and customers, police and suspects, guards and **prisoners**, and professionals and clients, as well as interpersonal relations such as those between parents and children. In these contexts the rules are relatively clear about who can ask or observe, and who is expected to reveal or is entitled to conceal. Consider also the extreme imbalance in caste and slave systems. Situations involving power differences with respect to gender and ethnicity may also reflect information inequality.

In these organizational patterns, stratification often exists within stratification. The irony of control agents themselves being under **surveillance** is strengthened by new technologies that indiscriminately record all in their path. Prison guards, for example, are watched and recorded by the same means they use on inmates. In the high-visibility conditions of wired shopping malls, guards never know when they are being watched, overheard, or secretly tested.

Rose Coser (1961) uses the felicitous phrase “insulation from observability” to describe the norms and resources that protect the actions of higher-status roles in bureaucratic organizations. Observability is also affected by the extent to which various kinds of personal information are aggregated or compartmentalized. One aspect of this central to contemporary controversy involves the ability to merge distinct databases by using a universal identifier, whether referring directly to the person’s identity or location, or through pseudonymous or anonymous means.

Beyond rules about who can ask or know and who must reveal, the literal availability of physical barriers to visibility needs to be considered. Contrast the enclosed office with soundproof walls that a manager may have with the open cubbies of office workers. The homeless are “in public” not only because they are on city streets, but because they often lack the insulation of walls or **automobiles** that prevent observation.

Issues of scale and the extent of geographical dispersion vs. concentration in the activities of daily life can also be noted. McCahill (2002) found significant differences in his study of two malls serving lower- and higher-status groups in England. The first mall was adjacent to a geographically isolated public housing project, in which the resources for daily living were highly concentrated. Shops, medical facilities, and government offices were in the mall. In their rootedness and with a lack of insulating resources, residents were under constant surveillance in their

daily rounds when they shopped, saw a doctor, used the post office, made a telephone call, or sat on a bench. In contrast, the more affluent and mobile patrons of the upscale mall had many more options and in some ways greater privacy as a result; for example, they had vehicles that made transportation to dispersed services easier, backyards for recreation, phones within their **homes**, and the ability to pay for deliveries.

The surveillance that crosses privacy borders can be analyzed with respect to whether it is nonreciprocal or reciprocal. The former is one-way, with personal data going from the watched to the watcher (e.g., to employers, merchants, doctors, teachers, parents) and tends to reflect power and resources differences. In contrast, reciprocal surveillance is bidirectional. But reciprocal need not mean equal. Thus in a democratic society citizens and government engage in reciprocal but distinct forms of mutual surveillance. Citizens can watch government through requirements for **open meetings**, freedom of information requests, and conflict of interest and other **disclosure** statements. However, unlike government, citizens can not legally wiretap, carry out Fourth Amendment searches, or see census or tax returns. Citizens can obtain some information from the public records that corporations must file. The corporation may require citizens to provide personal information in return for goods and services, but it does not offer equivalent information about those within its organization. Patients reveal a great deal to doctors, but beyond seeing framed symbolic diplomas and licenses, generally are not offered doctors' personal information.

In bounded settings such as a protest demonstration, there may be greater equivalence with respect to particular means; for instance, police and demonstrators may videotape each other—an example of symmetrical reciprocated surveillance. This is seen in many settings of organizational conflict in which the contending parties are roughly equivalent. Games such as poker involve this, as do some contractual agreements and treaties (e.g., the mutual deterrence of nuclear arms control sought through reciprocal watching).

Symmetrical forms may be present even in the absence of formal agreements. Spies or intelligence agents, whether working for countries, companies, or athletic teams are often mirror images of each other. They offensively seek to discover an opponent's information and defensively attempt to protect their own. Yet, on balance, asymmetry in formal surveillance and information rights within hierarchical organizations and other stratified settings remains. This asymmetry is not always easy to see because it can be embedded in the physical and cultural environment. Imaginative norm-breaching and bending experiments such as those conducted by Steve Mann (2003), who used a visible webcam to film employees in stores who themselves were using video cameras to watch customers, can help identify asymmetries. In Mann's research, the one-sidedness quickly became apparent when, with no appreciation for the humor or irony in the situation in evidence, he was told to leave the store.

The development and use of information-avaricious technologies tends to reflect differential access to resources. On the average, privacy-invasive technologies seem more likely to enhance the status quo and to extend inequality than the reverse. The more privileged have an advantage in the development, control, and use of technology. The uses of technologies for social sorting with respect to

opportunities for employment, consumption, health care, and the allocation of suspicion are profound.

The ability to control information is central to the borders of social groups. Privacy is a social as well as an individual value. For example, a legal oppositional political group, or indeed any group, needs to be able to control information about members, resources, and plans, and to feel that freedom of expression within the group is respected. To the extent that a group's borders are porous—punctured by informers and intensive surveillance—its ability to act is weakened and democratic ideals are undermined.

Consider the following thought experiment. What if those in developing nations—the colonized, workers, the poor, subordinate ethnic groups, the physically and mentally ill, social service agencies, and those in prison—had the same resources to develop and implement technologies to serve their needs that are available to developed nations, corporations, the military, police, and corrections? Would there be different technologies and uses? What if the information technology advances of the 1990s and later had been available during the more idealistic and social-reform focus of the early and mid-1960s?

Depending on the component, privacy can be either a right to which all citizens are entitled, or a commodity that must be paid for. Responding to demand, the market system increasingly offers technologies and services for protecting personal information—from shredders, to tools for finding hidden cameras, to home security systems, to various software and privacy-protection services. To the extent that privacy comes to be seen as a commodity for which how much you get depends on how much you can or are willing to pay, the more privileged are clearly in a better position to obtain it. They are also better situated to avoid being seduced by consumer rewards into voluntarily giving up, in a sense selling, their privacy.

George Orwell, the author of the novel *Nineteen Eighty-Four* and the idea of “**Big Brother**,” was once asked, “Isn’t technology neutral?” He is said to have replied, “Yes, and so is the jungle.” Yet as with the animals in another of Orwell’s novels, *Animal Farm*, surveillance is more neutral for some than for others. It is important to acknowledge the sense in which privacy-invasive technologies can be and are neutral. Yet the actual use of a technology needs to be considered apart from its potential use. Part of the neutrality or equality-of-technology argument is equivalent to Anatole France’s observation that the rich and the poor are both forbidden to sleep under bridges or steal a loaf of bread.

Certainly the camera, audio recorder, or motion detector will capture whatever is encountered independent of social factors, no matter the economic level, gender, or ethnicity of those being recorded. This can introduce fairness and help smooth out some of the rough edges of stratification. The populist arming of subordinates and the public at large with personal computers and recording devices may serve as a counterweight to the surveillance tools of the more powerful. Consider the video-cam documentations of police abuse seen on the evening news or the public figure being hoisted on his or her own petard, as in the case of President Nixon and the Watergate tapes.

But this egalitarian potential of the new technology does not mean that all persons and settings have an equivalent chance of being surveilled. Nor are the resources (whether cultural or physical) to defend, resist, and challenge equally

distributed in stratified settings and societies. When they are available, their use may be prohibited, as with company policies banning the use of **cellular telephone** cameras.

In the prison case noted above, in spite of the omnivorous potential of the lens, there is unlikely to be a camera or audio recording of what goes on in the warden's office or in the guards' recreational room, nor in the bathroom people in these positions use. The inmates' cells have no monitors that permit them to watch the guards, nor can they legally have cell phone cameras or even cell phones.

Yet there are some factors that qualify the familiar connection between privacy and stratification. Conceptions of privacy vary depending on the historical context. The Greeks, for example, placed the highest value on public life. One's sense of identity was found there. Privacy, being the realm of slaves, women, and children who were restricted to the home, was not valued. To be private meant to be deprived. Are there historical referents in the fact that privy is term for a toilet?

But beyond questions of cultural relativism, power is rarely a zero-sum game, and there are forces operating to weaken the link between privacy protection on the one hand, and invasion and stratification on the other. The ability to invade privacy as a reflection of power differences is often limited because it is rooted in conflicting values and interdependency, and is expressed on a broad and decentralized scale within a free market economy.

A number of factors limit the unleashing of the full potential of privacy-invading technology, even in contexts of inequality: legal and moral normative constraints on power holders; the logistical and economic limits on total monitoring; the interpretive, contextual, and indeterminate nature of many human situations; system complexity and interconnectedness; human inventiveness; and the vulnerability of those engaged in surveillance to be compromised or responded to in kind.

In spite of doomsday scenarios with respect to the death of privacy and liberty, in societies with liberal democratic economic and political systems, the advantages of technological and other strategic surveillance developments are sometimes short-lived and contain ironic vulnerabilities. In some ways technologies are neutral, and can help or even favor the less privileged. The design of automated and more-transparent systems that restrict or eliminate discretion may lessen the potential for official corruption and discrimination. The creation of documentary records of transactions that can be reviewed later (as with audio and video recordings) can offer evidence of what occurred in contested settings. Thus, the natural claim-making advantage of the more privileged may be somewhat offset.

The democratization of privacy-invading and privacy-protecting technologies as seen in their widespread availability and ease of application could increase equality. Through countersurveillance, we see an ironic turning of the tables. Thus, facing urine drug tests, employees can first experiment at home, testing themselves with a variety of readily available products like those used in the official test, or they may protect their private behavior through using products that mask drug residue.

Lower-status support persons such as maids, valets, butlers, chauffeurs, and personal assistants, often are required to know—or come to know—a great deal about the private lives of those they work for, and this tends not be reciprocated.

In modern societies where the mass media is so central, elite status comes with some new costs, and political leaders and celebrities lack the **anonymity** of



the average person. They both occupationally, and perhaps psychologically, need to be in the public eye, while they simultaneously place a high value on being left alone. The same mass media that is so central to their success also invades their privacy, as evidenced by the market for the goods produced by the **paparazzi**.

But other factors go far beyond public figures. Social life is dynamic. To be modern and successful in contemporary society increasingly means to be wired and plugged in to remotely mediated forms of communication and interaction. In one sense—excluding direct observation by police in public places—it is not homeless persons who are most subject to surveillance, but rather it is the more privileged. Indeed the very state of being “off the system,” which can partly define low or lumpen proletariat status, also brings with it a perverse kind of freedom to be left alone. Increasingly it is the more privileged within the system whose electronic transactions are subject to surveillance.

New styles of electronic living in some ways alter the traditional relationship between surveillance and stratification. For George Orwell, it was not the masses but the elites who were most closely watched. As life comes to imitate art, contemporary electronic lifestyles reverse some aspects of the traditional relationship between stratification and surveillance, at least with respect to documentary records of behavior. The deep immersion of the more privileged in new documentary record forms of communication and interaction comes with some ironic vulnerabilities.

Excluding their greater vulnerability to being observed in public places, in being unplugged the poor and transitory homeless are in some ways less subject to surveillance than the more privileged and located. Consider the latter’s telephone, fax, computer, bank, credit, employment, medical, and travel electronic trail- and tale-leaving behavior. Awareness of the above factors modifies, but does not overturn, the stratification-privacy invasion link. Such awareness reveals that indeed technology is a double-edged sword with respect to social stratification (and much else), even if its multiple blades are not of equivalent sharpness.

See also: **Constitutional protections; Electronic surveillance; Privacy, definition of; Privacy, philosophy of; Secrecy**

Suggested Reading: Brinn, David. *The Transparent Society*. New York: Perseus, 1999; Coser, Rose. “Insulation from Observability and Types of Social Conformity,” *American Sociological Review* 26 (1961): 28–39; Flaherty, David H. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill: University of North Carolina Press, 1992; Foucault, Michael. *Discipline and Punish: The Birth of the Prison*. New York: Pantheon, 1977; Gandy, Oscar. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press, 1993; Lyon, David (ed.). *Surveillance as Social Sorting*. London: Routledge, 2003; Mann, S., J. Nolan, and B. Wellman. “Surveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments,” *Surveillance and Society* 1 (2003): 331–355; Marx, Gary T. “Seeing Hazily (but not Darkly) through the Len(s): Some Recent Empirical Studies of Surveillance Technologies,” *Law and Social Inquiry* 30 (2005): 339–399; McCahill, M. *The Surveillance Web*. Devon, UK: Wilan, 2002; Orwell, George. *Animal Farm*. New York: Signet Classics, 1956;

Regan, Priscilla. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press, 1995.

Gary T. Marx

Privacy notices

Privacy notices, which are also called “privacy statements,” implement the notice principle of **fair information practices**. It is important to note that a privacy notice is not the same as a privacy policy, even though the terms are sometimes used interchangeably. A privacy notice communicates an organization’s information practices to the public while a privacy policy describes the organization’s standards for the collection of **personally identifiable information** and how the information is subsequently managed by the organization.

Privacy notices serve two purposes. First, they help people make informed choices among companies based on their information practices. Second, privacy notices help reduce the risks associated with disclosing personal information because they provide people with information about the organization’s information practices. This information can help people decide whether or not to disclose certain personal information, or whether or not to even engage with an organization at any level.

Privacy notices are particularly important for e-commerce because when business is conducted online, there are fewer signaling opportunities for companies than exist in the off-line world, thus the notice is a critical contact point with the individual. If the online environment is perceived as overly risky, people will be less motivated to conduct online transactions, particularly if the organization is not a well-known brand, or they have not done business with the organization previously.

At a minimum, privacy notices should include the basic elements of fair information practices: notice, choice, access, and security. A complete privacy notice typically describes what personal information is collected; how the information will be used; whether personal information will be shared and, if so, with whom; the options available to exercise control over how personal information is used, including the ability to **opt-in or opt-out** of unrelated uses; how to review one’s personal information and correct errors; and the general steps that the organization has taken to protect the information. The notice should also describe its scope, meaning which parts of an organization or a website are governed by the notice, and include information about how to contact the organization regarding privacy concerns.

Privacy notices became a public policy issue in the mid-1990s when privacy concerns threatened the growth of e-commerce. Privacy notices were viewed as one way to address these concerns. Between 1998 and 2000, the Federal Trade Commission (FTC) used web-based surveys to report to the U.S. Congress regarding online privacy. These surveys measured whether or not commercial websites collected personal information, whether or not the sites posted online privacy notices, and the extent to which these notices reflected fair information practices. In 1998 the FTC found that while the vast majority of websites collected personal information, only 14 percent provided any notice of their information practices, and only 2 percent provided notice by means of a comprehensive privacy notice. By 2000, the FTC reported that 88 percent of a random sample of websites had

posted some form of privacy **disclosure**. However, only 20 percent of those policies included all four basic elements of fair information practices: notice, choice, access, and security.

Subsequently, laws were enacted requiring privacy notices for three sectors: websites targeting children under 13 (**Children's Online Privacy Protection Act of 1999** (COPPA)), financial institutions (**Financial Services Modernization Act of 1999** or the Gramm-Leach-Bliley Act (GLBA)), and certain health organizations (**Health Information Portability and Accountability Act of 1996** (HIPAA)). These laws specified content, general format requirements, and delivery requirements for notices. While COPPA applied specifically to online privacy notices, GLB and HIPAA applied to both off-line and online privacy notices. Further, beginning in 1999, U.S. government agencies were required to post privacy policies on their websites. Industry self-regulatory programs for privacy, such as the BBBOnline and TRUSTe privacy seal programs, were also launched during this same time period.

While laws and self-regulatory programs define standards for the content of some privacy notices, there are no comprehensive rules that apply to all privacy notices, nor are all organizations required to post privacy notices. Congress declined to act on the FTC's 2000 recommendation to enact legislation mandating that commercial websites post baseline privacy notices. However, absent a requirement to post privacy notices, commercial websites or other organizations regulated by the FTC that voluntarily post or distribute privacy notices could nonetheless be subject to FTC enforcement action for engaging in an unfair or deceptive trade practice if their practices are at odds with their privacy notices. For example, in 2002 the FTC announced it had reached a settlement with two high-profile organizations, Eli Lilly and Microsoft, in response to complaints that these two organizations had violated their online privacy policies.

Current issues related to privacy notices include readability of notices, format standards for notice, and comprehension. For example, a 2004 Harris Interactive Survey conducted for *Privacy and American Business* found that 69 percent of those responding decided not to register at a website to get information or to shop because the site's privacy policy was perceived as too complicated or unclear. A 2001 Harris Interactive Survey found that a majority of those responding expressed a strong preference for short privacy notices and for companies to adopt a consistent summary or checklist format for their privacy policies.

In December 2001, the Gramm-Leach Bliley (GLB) regulatory agencies hosted a public workshop focusing on improving the readability of GLB notices, because the initial notices were widely perceived as unreadable. Approximately a year later, the FTC created a pamphlet summarizing the key communication tools and techniques presented at the workshop as a voluntary means for promoting the readability of GLB privacy notices.

Developing standards for notices is another way to promote readability. For example, privacy notices on websites displaying a privacy seal, while longer overall than privacy notices posted on other websites, are more readable than privacy notices posted on websites without a privacy seal. This may be the result of the fact that privacy policies submitted by prospective licensees are subject to review by the seal program and are revised to improve readability prior to being awarded a seal.

Nonetheless, readability remains an ongoing challenge as organizations attempt to balance legal compliance issues with effectively communicating complex information practices to consumers in a single document.

Alternative notice formats such as short or layered notices have the potential for improving the usefulness of notices to consumers. With the layered notice approach, organizations post or distribute short notices, modeled after nutrition or food labels, which are linked to the longer, complete privacy notices. The layered notice contains the highlights from the complete privacy notice. In January 2005 the FTC and the other GLB agencies issued requirements specifying language and format standards for prescreened offers for credit or insurance, including a requirement for a layered, short notice. In addition, alternative notice formats for wider use are under consideration by the government and industry groups in the U.S. and abroad. Major challenges in developing an effective layered notice include vocabulary and format issues as well as in determining what content should be included.

Finally, being able to read a notice does not mean that the reader comprehends the content of the notice. Privacy notices cannot help people make informed choices or reduce risk if an individual does not understand the meaning conveyed by the content of the notice. There has been little or no comprehension testing of privacy notices, so this is clearly an area for future work.

Privacy notices also cannot help address the risks of disclosing personal information if people are not motivated to read them. There is some evidence that people are unaware of the risks posed by disclosing personal information online, and the role privacy policies should play in helping them make informed decisions about disclosure. For example, a 2003 survey, *Americans and Online Privacy*, found that 57 percent of adults who access the Internet from home believe incorrectly that the existence of a privacy policy means the website will not share their personal information with third parties. A comprehensive program of consumer education is needed if privacy notices are to realize their potential as a tool for improved consumer decisionmaking and choice.

Suggested Reading: Federal Trade Commission. *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*. www.ftc.gov/reports/privacy2000/privacy2000.pdf. Online, May 2000; Milne, George R., and Mary J. Culnan. "Strategies for Reducing Online Privacy Risks: Why Consumers Read [or Don't Read] Online Privacy Notices," *Journal of Interactive Marketing* 18 (Summer 2004): 15–29; Milne, George R., Mary J. Culnan, and Henry Greene. "A Longitudinal Assessment of Online Privacy Notice Readability," *Journal of Public Policy and Marketing* 25 (Fall 2006): in press; Turow, Joseph. *Americans and Online Privacy: The System Is Broken*. Annenberg Public Policy Center, University of Pennsylvania, June 2003. www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf. Online, August 2006.

Mary J. Culnan

Privacy torts

The privacy torts are a group of legal causes of action under which an individual can sue another for invasion of privacy. There are four torts that are known collectively as the "privacy torts": (1) intrusion upon seclusion; (2) public **disclosure** of



private facts; (3) false light; and (4) appropriation of name or likeness. Today, most states recognize some or all of the privacy torts.

The privacy torts originated with an article by Samuel Warren and **Louis Brandeis**, “The Right to Privacy,” published in the *Harvard Law Review* in 1890. Warren and Brandeis were partners together in a law firm in Boston. Brandeis would later go on to become a U.S. Supreme Court justice. The article began by discussing the increasing sensationalism of newspapers. Warren and Brandeis wrote during a time when there was a rapid explosion in newspaper readership. This was the era of “yellow” **journalism**, where papers were inexpensive and where the focus of the media was on provocative headlines, tawdry human-interest stories, and other attention-grabbing matters. Warren and Brandeis were concerned by the press’s ability to invade the “sacred precincts of private and domestic life.” The authors were also concerned about new technologies in photography, namely a recently invented camera manufactured by the Eastman Kodak Company. This new camera, called the “snap camera,” was a lightweight, portable camera that was not very expensive. For the first time, Warren and Brandeis noted, people could take candid photographs of each other; previously, photos of people were taken by professional photographers, and people had to pose for their pictures to be taken. Warren and Brandeis feared that the new cameras in the hands of an increasingly sensationalistic media could pose a great threat to privacy.

The article argued that the law at the time did not adequately protect privacy. Warren and Brandeis observed, however, that the common-law cases did support a general “**right to be let alone**,” and from this general right, courts could derive specific protections for privacy. They suggested that courts create tort actions so that people who suffered an invasion of privacy could sue for damages.

Shortly after the twentieth century began, courts and legislatures responded to the Warren and Brandeis article by creating a number of torts to protect privacy.

In 1960 William Prosser, the foremost tort law expert in the country at the time, examined over 300 privacy cases, in reference to the Warren and Brandeis article. In an article titled “Privacy,” published in the *California Law Review*, Prosser noted that there were four distinct torts that had arisen from the Warren and Brandeis article, and these became known as the privacy torts.

Intrusion upon Seclusion

The tort of intrusion upon seclusion protects against the intentional intrusion into one’s “solicitude or seclusion” or “his private affairs or concerns” that “would be highly offensive to a reasonable person.” The tort deems it a legal wrong for people to snoop into others’ affairs by a variety of means. For example, in *Hamberger v. Eastman*, 206 A.2d 239 (N.H. 1964), a landlord was held liable for intrusion by using a hidden recording device to record his tenants’ conversations in their apartments. In *Nader v. General Motors Corp.*, 255 N.E.2d 765 (N.Y. Ct. App. 1970), the court concluded that General Motors could be liable for wiretapping Ralph Nader’s telephones and for having him placed under extensive surveillance in public. In *K-Mart Corp. v. Trott*, 677 S.W.2d 632 (Tex. App. 1984), an employer’s unauthorized search of employee’s personal locker constituted intrusion upon seclusion.

Other cases have found viable intrusion actions for peering into a person's **home** windows, such as *Pinkerton Nat'l Detective Agency, Inc. v. Stevens*, 132 S.E.2d 119 (Ga. App. 1963), or harassing a person by making repeated telephone calls, as in *Donnel v. Lara*, 703 S.W.2d 257 (Tex App. 1985). In another famous case, *Dietemann v. Time, Inc.*, 449 F.2d 245 (9th Cir. 1971), two reporters deceived a man in order to gain entry into his home, where they secretly recorded him performing his quack healing powers. The court concluded that the deceptive entry coupled with the hidden recording devices constituted a viable intrusion claim.

Public Disclosure

The tort of public disclosure of private facts creates a cause of action when one makes public "a matter concerning the private life of another" in a way that is "highly offensive to a reasonable person" and "not of legitimate concern to the public." In *Daily Times Democrat v. Graham*, 162 So. 2d 474 (Ala. 1964), a newspaper was liable for public disclosure when it printed a photograph of a woman whose dress was blown up by air jets. In *Barber v. Time, Inc.*, 159 S.W.2d 291 (Mo. 1942), the use of a woman's photograph in a story about the woman's rare disease was held to be a violation of the tort.

One of the most difficult elements of the tort to apply is the last element: that the disclosure not be of "legitimate concern to the public." This element is referred to as the "newsworthiness test." The purpose of the newsworthiness test is to protect free speech. Even if a disclosure violates somebody's privacy, it cannot give rise to liability if it is newsworthy. For example, in *Sipple v. Chronicle Publishing Co.*, 201 Cal. Rptr. 665 (Cal. App. 1984), a newspaper wrote a detailed account of the background of Oliver Sipple, the man who heroically saved President Ford from being shot by an assassin. In the story, the newspaper disclosed that Sipple was gay, a fact he had concealed from his family. One of the reasons why the court concluded that the article was newsworthy was because it questioned whether Ford's reluctance to publicly thank Sipple for saving his life was because Sipple was gay.

Courts have found the newsworthiness element very difficult to apply. A number of approaches have arisen. Sometimes courts defer to the media, concluding that they should not be second guessing the judgments made by journalists. The problem with this approach, however, is that it lets the media win all of the time. Other courts look to the "customs and conventions of the community" and conclude that information is not of legitimate concern to the public if it consists of "morbid and sensational prying into private lives for its own sake." In one very controversial case, *Diaz v. Oakland Tribune*, 188 Cal. Rptr. 762 (Ct. App. 1983), the *Oakland Tribune* published an article indicating that the first woman student-body president elected at a local community college was a transsexual. The court concluded that there was "little if any connection between the information disclosed" and the plaintiff's "fitness for office." Another famous case, *Shulman v. Group W. Productions, Inc.*, 955 P.2d 469 (Cal. 1998), involved a television show chronicling real emergency rescues that filmed the rescue of a woman who had been severely injured in a car accident. The court concluded that the television show was newsworthy.

The public disclosure tort raises potential First Amendment concerns, as the tort involves free speech. Law professor Eugene Volokh criticizes the tort for allowing



people to stop others from speaking about them. The Supreme Court has never squarely addressed whether the tort is constitutional under the First Amendment. In a series of cases, the Supreme Court has concluded that when the government makes information publicly available in a public record, the press cannot be held liable for publishing it (see *Cox Broadcasting v. Cohn*, 420 U.S. 469 (1975); *Smith v. Daily Mail*, 443 U.S. 97 (1979)). In *Florida Star v. B. J. F.*, 491 U.S. 524 (1989), the Supreme Court held that this rule applies when a rape victim's name, revealed in a public police report, is published in a newspaper article. In each case, the Supreme Court explicitly refrained from more broadly holding that the tort was unconstitutional.

False Light

A third privacy tort, false light, protects against the giving of “publicity to a matter concerning another that places the other before the public in a false light” that is “highly offensive to a reasonable person.” The tort deals with falsehoods and fostering misimpressions. False light bears many similarities to the defamation torts of libel and slander. A primary difference, however, is that whereas libel and slander require that the falsehood be damaging to a person's reputation, false light does not. Under false light, even a flattering yet false statement about a person can give rise to liability so long as it causes emotional distress to the person.

Many false light cases involve instances where people's photographs are used out of context. For example, in *Thompson v. Close-up, Inc.*, 98 N.Y.S.2d 300 (1950), the court held that a plaintiff could bring a false light action when his photo was used in an article about drug dealing. In another case, *Holmes v. Curtis Publishing Co.*, 303 F. Supp. 522 (D.S.C. 1969), the court found a false light action occurred when a plaintiff's photo was used with the caption indicating he was a high-stakes gambler.

Appropriation

The tort of appropriation occurs when “one who appropriates to his own use or benefit the name or likeness of another.” The tort protects the individual's right to “the exclusive use of his own identity, in so far as it is represented by his name or likeness.”

What constitutes a person's name or likeness has been interpreted broadly. The use of a famous football player's nickname, for example, can constitute an appropriation of his name or likeness (see, for example, *Hirsch v. S. C. Johnson & Son, Inc.*, 280 N.W.2d 129 (Wis. 1979)). In *Ali v. Playgirl, Inc.*, 447 F. Supp. 723 (S.D.N.Y. 1978), the famous boxer Muhammad Ali sued *Playgirl* magazine for publishing a drawing of a man in a boxing ring with the identification “The Greatest.” This was an appropriation because “The Greatest” was Ali's nickname. In *Midler v. Ford Motor Co.*, 849 F.2d 460 (9th Cir. 1988), the court held that singer Bette Midler could sue for appropriation when a commercial used a singer who imitated her voice.

Appropriation protects against the commercial exploitation of one's name or likeness, not the use of one's name or likeness for news, art, literature, parody, satire, history, or biography. Using a person's photograph to illustrate a news article,

for example, is not appropriation; nor is writing a biography about a person. A sculpture of a person constitutes a work of art, and is therefore not an appropriation of that person's name or likeness. The key to the tort is whether the person's identity is being used to endorse a product, or whether the value of the person's identity is being exploited for the benefit of another.

In a series of cases, courts have held that newspapers can use people's photographs to illustrate stories even when the people in the photographs are not the actual people involved in the story. For example, in *Finger v. Omni Publications International, Ltd.*, 566 N.E.2d 141 (N.Y. Ct. App. 1990), the court held that a newspaper could print the photo of a large family in an article about in vitro fertilization even though the children had not been conceived using in vitro fertilization. In *Arrington v. New York Times*, 434 N.E.2d 1319 (N.Y. Ct. App. 1982), a photograph of the plaintiff was used in connection with an article about the black middle class. Since the photo illustrated the story, it was not an appropriation of the plaintiff's name or likeness. In *Messenger v. Gruner + Jahr Printing and Publishing*, 208 F.3d 122 (2d Cir. 2000), a young woman's photos were used to illustrate a story in *Young and Modern* magazine about a 14-year-old girl who, while drunk, had sex with three older men. The woman whose photos were used had nothing to do with the story, but the court concluded that the images illustrated the themes of the story.

Other Torts

The privacy torts are not the only torts that protect privacy. In some cases, a general tort action for negligence has been used. For example, in *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001 (N.H. 2003), a man bought data about a woman from a database company. He used the information about her work address to confront her at her place of employment and kill her. The court held that the company could be liable if it did not act with "reasonable care in disclosing a third person's personal information to a client."

The tort of breach of confidentiality is another tort that protects privacy (see *McCormick v. England*, 494 S.E.2d 431 (S.C. Ct. App. 1997)). The tort applies when certain professionals (doctors, lawyers, bankers, and teachers, among others) disclose information that their patients or clients disclose to them in confidence. Unlike the tort of public disclosure, the breach of confidentiality tort does not require that the disclosure be highly offensive to a reasonable person. There is no newsworthiness test.

See also: **Constitutional protections; Privacy, definition of; Privacy, philosophical foundations of**

Suggested Reading: Kalven, Harry, Jr. "Privacy in Tort Law—Were Warren and Brandeis Wrong?" *Law and Contemporary Problems* 31 (1966): 326; Post, Robert C. "The Social Foundations of Privacy: Community and Self in the Common Law Tort," *California Law Review* 77 (1989): 957; Prosser, William. "Privacy," *California Law Review* 48 (1960): 383; Solove, Daniel J. "The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure," *Duke Law Journal* 53 (2003): 1018; Solove, Daniel J., Marc Rotenberg, and Paul M. Schwartz. *Information Privacy Law*. New York: Aspen, 2006; Volokh, Eugene. "Freedom of Speech and



Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You,” *Stanford Law Review* 52 (2000): 1049–1090; Warren, Samuel D., and Louis D. Brandeis. “The Right to Privacy,” *Harvard Law Review* 4 (1890): 193; Zimmerman, Diane L. “Requiem for a Heavyweight: A Farewell to Warren and Brandeis’s Privacy Tort,” *Cornell Law Review* 68 (1983): 291.

Daniel J. Solove

Private investigators

Private investigators (or “PIs”) are professional, nongovernmental individuals who seek out information about groups or individuals for private clients. PIs are employed by lawyers, legal firms, corporations, nonprofit organizations, private citizens, and celebrities. Private investigating work typically operates at the limits of the laws governing **surveillance** and privacy. Lawyers and legal firms hire PIs to interview witnesses, investigate their backgrounds, or get information to make a case for a client. Corporations often hire PIs in order to decrease and investigate theft as well as **industrial espionage**. Most PI work done for average private citizens concerns issues of infidelity, divorce, and/or premarital **background checks**. The fees for PIs are usually expensive, and are billed and calculated in a similar fashion to that of lawyers: the charges are per hour, plus expenses. This means that the services of PIs are typically engaged by wealthy individuals or well-funded organizations.

PIs use various forms of surveillance and research in order to gather information for their clients. Direct fieldwork for PIs includes physically watching a target’s house, calling the target’s place of employment under false pretenses, and observing the target’s activities. This type of work often involves irregular hours. PIs use inconspicuous locations or vehicles to observe the activities of the target, using such tools as binoculars, video surveillance cameras, still photo cameras, **cellular telephones**, one-way listening devices, and microphones. Other aspects of private investigators’ work involve researching the **public records** that contain much information on individuals’ personal lives.

Some types of PI work may border on the illegal. PIs are often aware of legal boundaries and may push their investigations to these limits. PIs are generally required to hold PI licenses in the states in which they operate. Some states such as Alaska and Alabama do not require licenses, yet some other states, such as California, require PIs not only to have licenses but to complete an official investigating course. If a PI is found guilty of infractions relating to the legal boundaries, it could lead to the loss of his or her license.

Contrary to popular fiction, PIs rarely engage in direct confrontations with those they are investigating or do work involving guns. Many PIs do not have concealed weapon licenses, since firing a weapon in a noncontrolled situation may require suspension of a PI’s license during the legal investigation of the shooting. Unlike a police officer, during the time a license is suspended, a PI cannot earn a living as a private investigator. PIs, therefore, avoid confrontation whenever possible and are likely to reject contracts that would threaten the status of their licenses.

The exception to this is a different aspect of private investigators: the security specialist. Some private investigators specialize in maintaining security for individuals

or organizations. The investigation aspect of this specialty involves researching and adjusting the security protocols of clients as well as investigating potential threats.

Allan Pinkerton (1819–1884) was an early and high-profile private investigator. His firm started with a few investigators who were generally hired to investigate bank thefts, unexplained corporate losses, and other types of fraud. Later, Pinkerton became infamous for employing mercenaries who engaged in violent confrontations with striking workers and for hiring people to infiltrate labor organizations as spies. Pinkerton was hired by the government on many occasions until Congress passed the Pinkerton Law, forbidding the federal government from hiring Pinkerton's and similar agencies.

The future of private investigating will be shaped by technological developments. More sophisticated, higher-quality, and less-expensive surveillance equipment will mean more thorough—and potentially more invasive—investigations. Moreover, as more and more “public” information is put online, access to the **Internet** will mean it will be easier to find, analyze, and compile information for background checks and other investigations. Finally, some PI agencies are employing **computer** hackers for the purpose of breaking in to a target's equipment and accessing other information. It seems likely that computer PIs will come to occupy their own niche as companies monitor and potentially punish copyright infringements on the Internet.

See also: **Electronic surveillance**

Suggested Reading: Bruno, Bob. *Serious Surveillance for the Private Investigator*. Boulder, CO: Paladin Press, 1992; Travers, Joseph. *Introduction to Private Investigation: Essential Knowledge and Procedures for the Private Investigator*, 2nd ed. Springfield, IL: Charles C. Thomas, 2005.

Shaun Parkman

Private parts

The term “private parts” is a euphemism for areas of the human body that are associated with sexual excitement, reproduction, and elimination. Distinguishing between private and public parts of the physical body has varied across time and cultures, and some cultures adhere to a narrow interpretation of private parts (genitalia are private) and other societies abide by a broader interpretation (any exposed skin is considered private or erotic). In the United States, private parts of the body are associated with both pleasure and danger. The power associated with bodily pleasure is intoxicating and thus considered potentially dangerous. The Judeo-Christian culture maintains a considerable separation between private and public parts of the body. When this **private/public dichotomy** or distinction is maintained, private parts are more often associated with immorality and degenerate behavior. The association of private parts with morality and sexuality increases anxieties regarding the human body.

Private and public divisions are not only applied to the physical human body, but the same distinctions are carried throughout our political and social body. A central tenant of the theory of liberalism is an interest in freedom from governmental interference. This interest is expressed by the difference between public and private realms of social life. In modern and classical political theory, the public arena is the realm of life regarding politics, and the private arena refers to issues of **family** life,



areas beyond governmental intervention. Second-wave feminists exposed the ambiguity of private and public boundaries of social and political life in their analysis of work. One of the many issues behind the feminist slogan “the personal is political” was the fact that the private life of the family bolsters public life. That is, the public sphere is dependent on the private sphere, including the initial, unpaid, and unrecognized work women perform in the private familial household. However, many actors in the public sphere, primarily men, refused to recognize women’s unpaid work in the household. Thus feminists questioned and criticized the demarcations between private and public spheres. Female exploitation could be reduced, they argued, by eradicating the distinction between public and private spheres.

Private and public manifestations of the physical as well as the social and political body begin to merge when examining legislative agendas. Obscenity is the term most often associated with representation of the private parts of the human body. The legal definition of obscenity has historically been used to describe language, images, and behavior that are offensive to the mainstream population. The definition of obscenity has variety across cultures and time. Representations deemed offensive to the general population vary according to the standards of the dominant ruling group. Behavior and images associated with obscenity became political tools to be used or abused by those in power, often those in control of the definition itself. As a result, issues regarding obscenity have to do with civil liberties. The U.S. Supreme Court originally defined obscenity as material that was “sexually explicit.” This proved problematic as the very groups who attempted to apply obscenity regulations, radical feminists and conservative policymakers in particular, were charged with obscenity when they simply described the offensive images in question. The Supreme Court further clarified the definition of obscenity with *Miller vs. California*, *Miller vs. California*, 413 U.S. 15 (1973) decision. Here the Court established a three-part test for a judge or jury to determine whether the material in question would be considered obscene. If the material was deemed “patently offensive” to “the prevailing community standards” or was equated with “prurient interests,” then the representations were deemed offensive. Once public officials applied the *Miller* standards, however, certain groups’ practices became the gauge of obscenity. That is, European male behavior became defined as normative, and all other behaviors (particularly that associated with lesbian or gay sex as well as with other sexual behaviors such as sadomasochism or bondage) were deemed obscene. As a result, deviant and minority groups rather than images and representations became targets of social control.

A number of laws currently regulate behavior associated with private parts of the human body. The U.S. Supreme Court, under Chief Justice Earl Warren, rendered the most far-reaching decisions with respect to privacy and the human body. In *Griswold v. Connecticut*, 381 U.S. 479 (1965), the Court established that every individual was protected by a right to privacy based on interpretations of the First, Fourth and Fourteenth Amendments. The *Griswold* case determined that the use of contraception was a right for married couples. Privacy was further expanded with subsequent decisions, among them *Roe v. Wade*, 410 U.S. 113 (1973), which granted privacy rights to women seeking abortions. However, the Court appeared to restrict privacy protections in *Bowers v. Hardwick*, 478 U.S. 186 (1986), when justices refused to recognize sexual relations between two consenting adults of the

same sex as a basic right. The Court determined that privacy rights did not extend to previously criminalized behavior. In the *Griswold* case, the Court imposed limitations on states' abilities to regulate private behavior, but the Court also ruled that states did have the right to override individual privacy if a persuasive rationale could be established. In the *Bowers* case, that persuasive rationale was invoked with the act of **sodomy**. Here the implications were devastating for gay, lesbian, and bisexual groups as their behavior became the definitive criteria upon which states rights governed private behavior. The *Webster v. Reproductive Health Services*, **492 U.S. 490 (1989)**, case further restricted women's bodily privacy as it established that the state could impose restrictions on a woman's right to an abortion. These later Supreme Court cases appeared to restrict, or even reverse, some privacy rights initially established in earlier courts. But the *Lawrence v. Texas*, **539 U.S. 558 (2003)**, decision that decriminalized all sodomy statutes reversed the *Bowers* decision. The Court ruled that the right to engage in private consenting adult sexual activity was a constitutional right of privacy. Initially the Court's decision seemed to eliminate the stigma that had applied to minority-group behaviors targeted in former sodomy laws. However, post-*Lawrence v. Texas* decisions have not eliminated the stigma entirely. For example, in Virginia, publicly engaging in sodomy is a felony under the "Crimes Against Nature" statute, while publicly engaging in heterosexual intercourse is simply a misdemeanor. Consequently, minority group behaviors continue to be targeted for additional social control.

As cultural critics, feminist performance artists like Annie Sprinkle openly question boundaries not only between public and private parts of the body, but boundaries involving many other Western-defined notions of duality: sacred and profane, art and pornography, Madonna and whore. Deconstructing and exposing ambiguity is a focal point of some performance artists. Performance artists practice art by using their bodies as the centerpieces of their presentations. Characterized as deviant and pornographic (as opposed to artistic) for her sexually explicit dramas, Sprinkle seeks to educate the public about the private arena of sex, sexuality, and the human body. Sprinkle considers herself a sexual healer, encouraging people to celebrate sexuality, sloughing off the shame associated with this privatized realm of life. Sprinkle demystifies sex and exposes some of people's deepest anxieties about private parts of the human body with her stage shows, some of which have included masturbating, urinating, sucking dildos, exhibiting her dirty underwear, resting her breasts upon the heads of willing audience members, and most notoriously, inserting a speculum in her vagina and inviting audience members to gaze at and photograph her cervix. In a typical performance where she portrays a prostitute, Sprinkle deconstructs the binary oppositions of client and whore. She illustrates and discusses the customer's desire, then takes the audience through versions and images of her own private desire. She does not characterize the client's desire as misogynist (the argument associated with radical feminists), nor does she elevate her own desire above the client's (the argument associated with pro-pornography feminists). An advocate of postmodernism, Sprinkle embraces and expands on binary positioning, rendering all categories authentic and continual. She advances agency and power to both representations.

Sprinkle's art poses the question of why it is important to draw distinctions between binary categories, particularly between private and public categories of the



human body. The separation between private and public parts of the human body, as well as between the same parts of the social and political body, is not only artificial and tenuous; in addition, Sprinkle illustrates that binary distinctions create identities by coercing individuals to navigate between them. She deconstructs and exposes the ambiguity of boundaries with a keen eye on how the categories are used in the service of the powerful, to the detriment of the less powerful. While dichotomous private and public categories function well as analytic devices, they are often more consequential in the lives of many individuals. Binary categories are never equal; they always force hierarchy and inequality.

See also: **Gender; Home; Privacy and inequality; Restrooms and dressing rooms; Voyeurism; Women and privacy**

Suggested Reading: Curry, Lynne. *The Human Body on Trial: A Handbook with Cases, Laws, and Documents*. Santa Barbara, CA: ABC-CLIO, 2002; Gibson, Pamela Church, and Roma Gibson. *Dirty Looks: Women, Pornography and Power*. London: British Film Institute, 1993; Robinson, Christine M. "Manifest and Latent Functions of Legal Social Control: Sodomy Statutes Post-Lawrence v. Texas." Paper presented at the Annual Midwest Sociological Society Meeting, Kansas City, MO, 2004.

Sue E. Spivey

Privilege

Generally, when the needs or interests of society in protecting the privacy of communications trump the need for evidence, the law protects the right to keep communications between two persons confidential. The protection is called privilege. It prevents the **disclosure** of certain types of private information, including the substance of confidential conversations between two people. The privilege must be properly asserted and can be waived. Generally, however, the privilege belongs to the speaker and cannot be waived by the listener.

In order for communication to be privileged, it must truly be a confidential communication. Thus, conversations among groups are generally not afforded protection. Further, if the conversation is made in a public place or otherwise overheard, it will not be considered truly confidential, and thus will not be subject to protection. Privilege can attach to any communication, whether spoken, written, or otherwise.

Use of privilege defeats the goals of the judicial process, that is, of determining the truth about what was said in any particular context. Courts, therefore, recognize privilege in limited circumstances and construe privileges very narrowly. Rarely are new privileges created; instead, the courts rely on privileges that have long legal histories.

In some jurisdictions, there is a presumption that privilege exists in certain circumstances (i.e., conversations between attorney and client, wife and husband, minister and penitent, therapist and patient, doctor and patient). In other words, the intent that a communication be privileged is assumed by the court. In other jurisdictions, those relying on privilege must prove that the conversations at issue were intended to be confidential and were in fact not overheard by a third party.

There is frequently a two-step test applied to determine if a privilege will be attached to a specific conversation or communication. The first question is whether the speaker intended the message to be confidential. If a confessor tells a priest,

“Please tell my brother I never intended to kill his wife,” the communication will not be afforded protection. The intent that the message be relayed to a third person will defeat the first requirement of **confidentiality**. The second prong of the test is whether the communication was indeed confidential. In other words, did (or sometimes could) another hear the conversation? If, in the confines of the confessional, the penitent party told the priest, “I killed my brother’s wife,” the confession would be protected. If, however, the penitent and priest had been riding on a crowded train and the penitent had made the same confession, no such privilege could be claimed.

Exceptions to the second prong of the test do exist. For example, if a patient makes statements to his or her doctor’s nurse, the doctor-patient privilege would ordinarily still apply. This conclusion, however, depends on the assumption that the patient intended the communication to be confidential and that it was made in circumstances where it was reasonable to believe the communication was confidential. There are also circumstances where communications that would ordinarily qualify as privileged will not be afforded that protection. Those circumstances are generally those where the speaker announces plans to commit a crime or harm a person, or uses the communication to commit fraud or further a criminal endeavor.

In order to waive a privilege, the party waiving it must actually hold the privilege. Thus, a doctor cannot waive a patient’s privilege and testify about what the patient told him or her. The patient, however, is always free to waive confidentiality and testify about the substance of the previously confidential communication.

Since privileges block the goals of the judicial process, they can be easily waived by explicit or implicit action. For example, if the victim of an auto accident sues seeking payment for medical bills and pain and suffering, the victim implicitly waives the doctor-patient privilege by making the very nature of doctor-patient communications the subject matter of the lawsuit. If the person relying on the privilege has, voluntarily or involuntarily, disclosed the content of the conversation to any third party, privilege is waived. Privilege can also be waived by simply failing to assert it.

A distinction does need to be made between the content of a conversation and the subject matter of the conversation. If a penitent tells a friend that he or she went to confession and confessed committing a prior crime to the priest, the penitent has disclosed the nature of the conversation but not the content. There has been no waiver of the privilege. If the penitent, however, tells the friend, “I told Father Smith I murdered my sister-in-law,” the privilege has been waived.

I. Attorney-Client Privilege

Communications between clients and attorneys in the course of the professional relationship are privileged if they are confidential. There need be no established relationship between the attorney and the client before the communication. Nor is there any requirement that the client hires or retains the attorney before the communication. Generally, all that is required is that the person talking with the attorney intends that the communication be confidential.

As discussed above, communications by a client with an attorney’s employees or agents are generally privileged as well. Privilege generally lasts long as the attorney’s employees or agents are assisting the attorney and the communication involves a subject within the scope of that representation.



The communications of independent experts hired to assist an attorney in evaluating a case or examining a client are also generally kept confidential. Exceptions to this are numerous. For example, reports prepared by those experts will frequently be subject to discovery. Likewise, if a client should discuss circumstances involving child abuse with a mandated reporter of child abuse, the communications regarding that issue will not be kept confidential.

A client may also expect that when he or she uses agents to communicate with a lawyer, the communication carried by the agent to the lawyer will be kept confidential. In that circumstance, neither the agent nor the attorney could reveal the confidential information. The protection would depend on the client's intent that the communication be confidential, the instructions given to the agent about confidentiality, and the agent's actions in protecting the confidentiality as the message is relayed to the attorney.

Attorney-client privilege is also a privilege for corporate clients. Corporations are treated as persons under the law, so privilege in this case is not all that different in concept. Questions arise, however, in terms of who can claim privilege. In *Upjohn Co. v. United States*, 449 U.S. 383 (1981), the Supreme Court held that when an employee is speaking on behalf of the corporation, communications between that employee and corporate counsel are privileged if the communication concerns corporate, not personal, matters. It is generally held that privilege can be successfully asserted by corporate managers, management-level corporate agents, in-house counsel, and outside attorneys. Specific corporate approval may be required to qualify communications between lower-level employees and counsel as confidential. In the corporate context, attorney-client privilege can be waived by the board of directors, executives authorized to act for the corporation, or in certain circumstances, by the corporation's attorney. Communications must be treated as confidential within the corporation to be considered as confidential by the courts.

The attorney-client privilege will generally not apply to physical evidence. Further, if an attorney represents two persons in one legal matter and a subsequent dispute between clients occurs, there is no privilege if the dispute is about the matter in which the attorney assisted the clients. The attorney-client privilege will also not survive if the client sues the attorney for actions taken by the attorney during the attorney's representation of the client.

There is an important distinction between attorney-client privilege and what has become known as the attorney's "work product doctrine." An attorney's work product, defined as the lawyer's written documents prepared in anticipation of litigation, has a qualified immunity from discovery in judicial proceedings even though there is no "communication" necessarily involved. The protection in this case is not a privilege in the historic sense. Protections for an attorney's work product are not absolute. Discovery of materials prepared in anticipation of litigation is permitted if the opposing party can show there is a substantial need of the materials in preparation of its case, and that the requesting party has been unable to obtain the information contained in the attorney's papers.

II. Marital Privilege

Generally, courts cannot force one spouse to testify about confidential communications received from the other spouse. The goal is to protect and promote honesty between spouses. The privilege is held to extend to verbal communications, communicative acts, and information obtained as a result of the marital relationship. While it can be difficult to define, marital privilege will not protect ordinary acts and conduct occurring in the spouse's presence.

For this kind of privilege to be claimed, the parties involved must be married to each other. Thus, it is frequently said the privilege does not survive divorce or death. Divorce or death, however, does not free either spouse to reveal the confidential communications that occurred during the marriage. It only frees each party to reveal communications made either before or after marriage. Conversations between members of an engaged couple are not protected, nor are conversations between persons living in a marriage-like relationship. If the parties are married, the privilege will generally survive even if they no longer live together or have been legally separated for years. Many states require that the act or communication have a relationship to the marriage or not be directly deleterious to the marriage in order to qualify for marital privilege. In a minority of states, a spouse cannot be forced to testify about any communication, even as drastic a communication as a threat to kill the other. Thus, victims of domestic battery can sometimes be prevented from testifying about their abuse by the spouse who was responsible for the attack.

It is important to remember that the rules of confidentiality apply. If a spousal communication has been reported to a third party, the protection afforded by privilege is lost. Police can interview one spouse to gain evidence against another, and the evidence obtained can be admitted at trial. And any third party can testify about what one spouse may have said about another.

III. Religious Privilege

Generally, a person has a privilege to refuse to disclose and to prevent another from disclosing confidential communication between the person and a member of the clergy when the clergy member is acting as a spiritual advisor. The privilege covers formal confessions as well as informal but confidential communications seeking spiritual guidance. The privilege can be claimed by the speaker, or on a speaker's behalf, by a guardian, conservator, or executor.

Most states have statutory definitions of clergy for the purposes of identifying those to whom the term applies. For example, Kentucky requires that a member of the clergy "is a minister, priest, rabbi, accredited Christian Science practitioner, or other similar functionary of a religious organization, or an individual reasonably believed to be so by the person" seeking consultation (Kentucky Revised Statutes, KRS Chapter 421).

This privilege is not without limits. At least one court has required that the communication involve a "confession" to qualify for the privilege. In that case, the court held that ministers must produce notes about conversations with victims of sexual abuse to be used by the defense in a criminal trial. Some courts have rejected claims of privilege for comments made in quasi-religious circumstances



like Alcoholics Anonymous meetings, while others have endorsed the privilege under those circumstances.

IV. Reporter's Privilege

A reporter's privilege, often established under "shield laws," twists the traditional notion of the privilege as belonging to the speaker and not to the listener. As interpreted by the courts and set forth in various state statutes, a reporter's privilege is to refuse to reveal the unpublished contents of his or her notes or to reveal the identities of confidential sources. This privilege is far from absolute.

Perhaps one of the most misunderstood privileges of all, the reporter's privilege would seem to find its basis in the First Amendment press protections. Nevertheless, a sharply divided U.S. Supreme Court ruled in *Branzburg v. Hayes*, 408 U.S. 665 (1972), that the constitution affords no such protection. That ruling still stands.

Even under some of the more than 30 state statutes that set forth a privilege for the press, the privilege is not absolute and may be overridden by applying a balancing test as encouraged by Justice Powell's concurrence in *Branzburg*. The actual tests suggested include considering whether the information sought is relevant or material; whether there is a compelling and overriding interest in obtaining the information; and whether the information is available from any other source. Courts use a variety of sources to recognize what might constitute a reporter's privilege including court decisions, common law, state statutes, and the court's own procedural rules.

If the confusion about the existence of any protection for journalists is not enough, the simple question of who is entitled to claim the privilege adds yet another layer. Some states require that to qualify for the privilege, the reporter must be a full-time newspaper or broadcast station employee. Arguably, that definition excludes all website, blog, or e-zine authors, freelance reporters, writers of non-fiction books, and documentary producers. In effect, the unsettled nature of this privilege from state to state, and even from federal court to federal court, leaves reporters and sources on uncertain ground.

V. Doctor-Patient Privilege

Communications from a patient to a doctor while the patient is seeking the doctor's opinion or treatment are privileged. The protection includes statements by the patient as well as details learned by the doctor as a result of medical examination or testing. Typically, the protection will cover the person's entire medical file. Generally, information obtained by or comments made to technicians and nurses working under the supervision or at the direction of a physician are also privileged. The privilege is not automatic. A staff person, nurse, or other person must work under the doctor's direct supervision for the doctor's privilege to apply. Hospital staff persons, or health care clinic employees who have no direct connection to the patient's doctor, may not be covered by the doctor-patient privilege (but may be covered by privileges of their own). Also, for the doctor-patient privilege to apply when a patient has communicated to someone other than the doctor, the communication must be made in the course of seeking a doctor's opinion or treatment.

When a patient sues a physician for malpractice, or sues a third party claiming an injury or medical condition was caused by that third party, the privilege is waived. Indeed, in these circumstances, patients are frequently deemed to have waived their rights to all their medical records, whether directly related to the condition for which they were treated or not. Requests for payment of medical bills by an insurance company are considered waivers of privilege. Applications for health or life insurance usually include explicit waivers of the privilege as well.

Many states have by statute created a kind of healthcare professional privilege. Similar to the doctor-patient privilege, in order for the privilege to apply, the two-prong test of intent and circumstances must be met. Some of the privileges created by various state laws include registered nurse-patient, nurse practitioner-patient, chiropractor-patient, psychologist-patient, social worker-patient, marriage and **family** therapist-patient, and professional counselor-patient privileges.

VI. Accountant-Client Privilege

Historically, only lawyers could promise clients confidentiality regarding communications about financial affairs. Thus, when business people or individuals discussed tax and other concerns with accountants, or released financial documents to those accountants, all that information could be obtained through discovery by the **Internal Revenue Service (IRS)** or any other litigant. As a result, there was a chilling effect on clients' desires to confide in accountants, who were also the best persons to provide the financial advice the clients needed.

Today, in most states, confidential communications made to an accountant in the course of a professional relationship are privileged. The privilege usually covers information provided to an accountant and anything learned by an accountant during an audit. The privilege will also cover any documents created by the accountant in the course of working for the client. In most instances, however, the privilege will not cover papers and documents given to the accountant.

VIII. Executive Privilege

When a president of the United States wants to avoid making confidential records or communications public, the president claims executive privilege. The privilege is also claimed by other executive branch employees. The privilege is almost always claimed to keep other governmental agencies from gaining access to the confidential materials. The privilege is based on the concept of separation of powers contained in the Constitution.

This privilege is actually not mentioned in the Constitution. There is also no statute protecting it. The Supreme Court basically acknowledged the privilege in *United States v. Nixon*, 418 U.S. 683 (1971), also known as the Pentagon Papers case, when it acknowledged the "valid need for protection of communications between high Government officials and those who advise and assist them in the performance of their manifold duties." Unfortunately for Richard Nixon, the Court did not adopt his effort to claim the privilege, and it ordered that he release the documents because, under the circumstances, the need for truth trumped the president's need for **secrecy**.

See also: **Journalism**



Suggested Reading: Allen, Ronald J., Mark F. Grady, Daniel D. Polsby, and Michael S. Yashko; “A Positive Theory of the Attorney-Client Privilege and the Work Product Doctrine,” *Journal of Legal Studies* 19 (1990): 359–397; Imwinkelried, Edward J., and Richard D. Friedman. *The New Wigmore: A Treatise on Evidence: Evidentiary Privileges*. New York: Aspen Law & Business, 2002; Newbold, Lorraine E. “The Crime/Fraud Exception to Legal Professional Privilege,” *Modern Law Review* 53 (1990): 472–484; Reynolds, Mildred M. “Privacy and Privilege: Patients’, Professionals’, and the Public’s Rights,” *Clinical Social Work Journal* 5 (1977): 29–42; Rice, Paul R. “Attorney-Client Privilege: The Eroding Concept of Confidentiality Should Be Abolished,” *Duke Law Journal* 47 (1998): 853–898; Spielberg, Alissa R. “Online without a Net: Physician-Patient Communication by Electronic Mail,” *American Journal of Law & Medicine* 25 (1999): 267–296; Weinstock, Robert, Gregory B. Leong, and Arturo Silva. “Potential Erosion of Psychotherapist-Patient Privilege beyond California: Dangers of ‘Criminalizing’ *Tarassoff*,” *Behavioral Sciences & the Law* 19 (2002): 437–449.

David J. Brown

Probable cause. *See* Search warrant

Proprietary privacy. *See* Privacy, definition of

Public health and safety

Public health and safety are often defined as those societal activities that seek to ensure the conditions necessary for people to be healthy. Underlying many of the activities to protect and promote the health of populations are vast acquisitions of identifiable health data by governmental public health authorities—and their private-sector partners—from health care providers, insurance companies, and others. The extensive collection and use of identifiable health data to protect the public’s health within increasingly national and international electronic health information systems raise significant concerns among individuals about the privacy of their health information. Balancing individual privacy concerns with the laudable goal of protecting communal health is a central component of historic and modern privacy laws, ethics, and policies.

In many ways, protecting the privacy of individually identifiable health data and promoting the public’s health seem contrary. Public health proponents want access to large amounts of health data; privacy advocates want to limit access to similar data. Individually identifiable health information has traditionally been used by or disclosed to an array of public- and private-sector entities (e.g., health care workers, pharmacies, researchers, insurance companies, and employers) for a variety of reasons (both legitimate and dubious), and with or without an individual’s knowledge or consent. Varied policies for sharing health data reflect the fragmented nature of legal and ethical protections of health information privacy. Fearing potential misuses or wrongful **disclosures** of sensitive health data that could lead to individual discrimination and stigmatization, privacy advocates consistently seek to limit the acquisition, use, and disclosure of identifiable health information in governmental and private-sector settings. Their concerns, often highlighted in well-publicized breaches of privacy norms or standards by governmental and private-sector data holders, seemingly justify more restrictive privacy practices.

Conversely, public health practitioners need consistent, routine access to and use of individually identifiable health information to accomplish important public health objectives. The collection and use of identifiable health data by federal, tribal, state, and local health authorities support nearly all public health functions and goals. Aggregated health data are needed to monitor the incidence, patterns, and trends of injuries and diseases in populations. Health data are acquired by public health authorities through legally authorized testing, screening, and treatment programs. Carefully planned **surveillance** programs and epidemiological investigations at the state and local levels gather individual health information on multiple conditions and factors, including (1) communicable (e.g., tuberculosis, SARS, avian flu) or sexually transmitted (e.g., HIV/AIDS, syphilis, gonorrhea) infections or diseases; (2) clusters or outbreaks of bacterial or viral infection (e.g., hantavirus, *E. coli*) from naturally occurring sources or bioterrorism; (3) risk behaviors in subpopulations (e.g., smoking among adolescents or ethnic minorities); and (4) other harmful conditions (e.g., diabetes, child or spousal abuse, lead poisoning, or iatrogenic injuries). Collecting this information helps public health authorities develop and implement meaningful programs and interventions to improve public health outcomes.

Privacy and public health proponents may disagree whether public health needs for health data override the legitimate privacy interests of individuals. In order to resolve conflicting demands, modern law- and policymakers try to balance individual privacy rights against the public's interest in promoting public health outcomes. When properly balanced, identifiable health data can be shared responsibly with public health authorities while still respecting individual privacy. This balance, for example, is seen in the HIPAA Privacy Rule, promulgated by the U.S. Department of Health and Human Services (DHHS) under the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**. Prior to the implementation of the Privacy Rule, an array of federal and state laws attempted to safeguard health information privacy. The effect was to create a patchwork of privacy protections that protected health data in differing ways, depending on the type, holder, and purpose of the data. When the Privacy Rule took effect on April 14, 2003, it presented for the first time a national U.S. standard of health information privacy and security protections (similar to data protection acts that proliferate among member countries of the European Union).

The Privacy Rule applies to covered entities (i.e., health plans, health insurance companies, specifically named government health programs, health care clearinghouses, and most health care providers) and their business associates through contractual mechanisms. It protects individually identifiable health information ("protected health information," or PHI) created or received in any form by covered entities. These entities responsible for establishing and adhering to a host of privacy protections, including (1) providing notice to individuals regarding their privacy rights and how their PHI is used or disclosed; (2) adopting and implementing internal privacy policies and procedures; (3) training employees to understand privacy policies and procedures; (4) establishing appropriate administrative, technical, and physical safeguards to protect the privacy of PHI; and (5) assisting health consumers to exercise their rights to inspect and request corrections or amendments to their PHI.



The Privacy Rule specifically addresses how and under what circumstances covered entities may disclose PHI outside their organizations. In general, a covered entity may not disclose PHI without individual written authorization, subject to several exceptions. Among these exceptions are disclosures from covered entities to public health authorities for legitimate public health purposes. In this way, the Privacy Rule—and most other comprehensive privacy laws—reflects an appropriate balance between individual privacy interests and public health. However, this balance is still compromised through misinterpretations and misapplications of privacy principles that can present barriers to public health activities. Some covered entities may mistakenly refuse to share PHI with public health authorities because they perceive that the Privacy Rule prohibits these disclosures. The entities incorrectly use privacy laws like the Privacy Rule almost like a shield to reject reasonable public health data requests.

Alternatively, public health authorities may misperceive that the Privacy Rule affects how they utilize PHI once it has been received from covered entities. This is not the case. Public health authorities doing public health functions are not covered by the Privacy Rule. Rather, public health authorities may have to adhere to a host of federal, state, and local privacy laws and policies that, taken together, are inconsistent, fragmented, and inadequate. These laws differ as to the degree of privacy protections afforded, assign varying rights to access identifiable data, and allow multiple exceptions to disclosure prohibitions outside public health agencies. Some states' laws declare that public health records are private but do not spell out the degree of privacy protections afforded. They may fail to narrowly define who may have access to such data or require persons to demonstrate why they need access. Public health information privacy laws may lack specificity about when disclosures may be made, permissively allow disclosures to persons or for purposes that are inconsistent with public health (e.g., disclosure in court settings), or fail to address secondary disclosures of information beyond those used to justify the original collection. Some states' disclosure provisions are too strict, interfering with legitimate public health exchanges of identifiable data among public health agencies.

In response to the myriad of public health information privacy laws and policies, Lawrence O. Gostin and James G. Hodge, Jr., scholars at Georgetown and Johns Hopkins universities, convened a multidisciplinary team of privacy, public health, and legislative experts under the auspices of the federal Centers for Disease Control and Prevention (CDC) to create a “gold standard” for the legally responsible use of identifiable data in public health settings. They developed the Model State Public Health Privacy Act of 1999 (MSPHPA), which provided, for the first time, a model set of provisions that addressed strong and consistent privacy safeguards for public health data. The MSPHPA authorizes public health agencies to acquire, use, and store identifiable health data for public health purposes while simultaneously requiring them to respect individual privacy and imposing penalties for noncompliance. Individuals are also empowered with various privacy rights and remedies.

Notwithstanding the observation that some privacy laws present some barriers to effective data use practices by public health authorities, in reality privacy and public health are synergistic. This is a core theme of the MSPHPA. Protecting the privacy of identifiable health data is critical to accomplishing public health goals. People will not stand for unwarranted privacy abuses by government or by the

private sector. Failing to respect the sensitivity and privacy of a person's health information predictably leads individuals to avoid or limit their participation in public health programs. When measured across populations, these collective decisions can skew the accuracy of public health information, ultimately affecting public health programs and outcomes. Protecting privacy is thus essential to protecting the public's health.

Conversely, everyone needs public health. No single person can ensure conditions in which he or she, or others, can be healthy. Protecting the public's health is more than a community aspiration; it requires the active cooperation and participation by each individual as a member of society. For everyone to benefit from communal health goals, people must be willing to confidentially share their health data for public health purposes. Each person experiences some diminution in informational privacy expectations in the interests of public health. Protecting the privacy of health information is thus not absolute. There are always legitimate uses of health data for public health purposes that should not necessarily be viewed as infringements of individual privacy interests.

In summary, protecting individual privacy and the public's health are indispensable objectives within a national health infrastructure that increasingly exchanges health data through electronic means. Neither goal can be neglected for the sake of the other because privacy and public health are synergistic. Individuals rely on public health authorities to protect the health of communities. Public health officials rely on individuals to provide timely and accurate health data through covered entities, which requires privacy protections. The HIPAA Privacy Rule recognizes this synergy. It reflects an essential feature of national privacy policy: disclosures of health data are made for public health purposes without individual written authorization. Still the Privacy Rule and other laws present some barriers to public health practice. These barriers may reshape the practice of public health in years ahead absent better societal understanding of the critical objectives of protecting communal health.

See also: **European Union Data Directive; Fair information practices; Health privacy; Personally identifiable information; Privacy Act of 1974**

Suggested Reading: Centers for Disease Control and Prevention. "HIPAA Privacy Rule and Public Health: Guidance from the Centers for Disease Control and the Department of Health and Human Services," *MMWR* 52 (Supp. 2003): 1–20; Etzioni, Amitai. *The Limits of Privacy*. New York: Basic Books, 1999; Gostin, L., and J. Hodge, Jr. "Personal Privacy and Common Goods: A Framework for Balancing under the National Health Information Privacy Rule," *Minnesota Law Review*, 86 (2002): 1439–1480; Gostin, L., J. Hodge, Jr., and R. Valdiserri. "Informational Privacy and the Public's Health: The Model State Public Health Privacy Act," *American Journal of Public Health* 91 (2001): 1388–1392; Hodge, J. G. "Health Information Privacy and Public Health," *Journal of Law, Medicine, and Ethics* 31, no. 4 (2004): 663–671.

James G. Hodge, Jr.

Public/private dichotomy

The terms "public" and "private," and their underlying concepts, have been used for thousands of years, often as opposites to form the public/private dichotomy. For Aristotle, male citizens were expected to govern themselves. Separate



from the governing sphere, male citizens ruled their own households. Other male citizens could not interfere with a male's household unless a male citizen violated the expectations for his roles as husband, father, or slave owner. Open to many interpretations, Jesus said, "Render unto Caesar the things which are Caesar's, and unto God the things that are God's," a statement perhaps serving as a basis for the separation of church and state. Today, the public/private dichotomy is widely used as a tool to delineate the powers of government and market actors, devise boundaries around family **homes**, and define responsibilities of community members. Public often concerns government, but sometimes includes areas where individuals can communicate. Private frequently refers to markets, but just as often to people and spaces where individuals, **families**, nonprofit organizations, and others live and cooperate. Public is characterized by access and openness. Private is characterized by efficiency, innovation, and promotion of self-interest. Although public and private have different meanings, what is meant by the public/private dichotomy?

A dichotomy is typically conceptualized as having four components. The first component is a division. A dichotomy divides phenomena. The second component is having two parts. *Di-* means "two" ; a dichotomy has two parts. The third component is exclusion. The division creates a boundary that excludes overlap of the two parts. The fourth component is exhaustion. The dichotomy exhaustively includes all potential phenomena, and all phenomena belong on one side or the other of the dichotomy. Applying these four components to a consideration of the public/private dichotomy will further understanding of whether the public/private dichotomy truly is a dichotomy, and if it is not, whether the notion of a public/private dichotomy is still useful.

The first component of a dichotomy is that phenomena can be divided. The boundary is drawn on the basis of a difference, such as one phenomenon possesses a characteristic the other phenomenon does not. In the public/private dichotomy, this boundary divides public and private. An important boundary separating public and private is eligibility. In the case of eligibility, public often implies accessibility: a public good is available to everyone. Private means restriction: the good is available to some, such as people who can pay for access. A similar boundary is a physical boundary. A public space, such as a public park, is available to everyone. A private space is restricted; for instance, a family can lock their home and take steps to prevent individuals from entering their property. Another important boundary is obligations. For obligations, public often denotes a legal requirement: individuals and families are obligated to pay taxes to governments. Private implies absence of legal coercion: individuals enjoy freedoms to act or not act as they see fit. Private examples range from whether to try to adopt children to whether to consume alcoholic beverages. The public/private dichotomy divides these phenomena into two spheres of activity.

The second component is that the dichotomy consists of two parts. Quite simply, the public/private dichotomy is based on two parts, the public and the private. Yet both public and private have multiple meanings, and each meaning of public is related to each meaning of private. For instance, in discussing social policies, public sector usually refers to government and private sector refers to the market. Public can refer to the public sphere and private to the private sphere when discussing areas of sociopolitical action. In each instance, public refers to one kind of phenomenon and private refers to a second kind of phenomenon.

A key component is the ability to use the dichotomy to exclude one phenomenon from another, to designate a phenomenon as one kind or the other. This component clarifies that all phenomena can be divided into two parts. For the public/private dichotomy to exist, all phenomena must be able to be divided into either public or private. An example is social policy. We designate health insurance plans as either public or private. In the United States, the largest public health insurance plan is Medicare. The private system of employment-based health insurance plans insures most Americans. Further, the public/private dichotomy is used to distinguish private property on which a home is built from public property on the same property, such as a sidewalk or a public utility mechanism. Finally, some activities are designated public and others private. Participating as a citizen in meetings of local government bodies, such as schools or city councils, is a public activity. The decision to have sexual intercourse is considered one of the most private activities.

A closer look reveals, however, that the boundaries separating the public and the private, essential to the existence of the public/private dichotomy, are regularly crossed. One instance of violating this boundary is determining who pays. The federal government does not directly finance Medicare. Employers and employees pay for Medicare, the U.S. public health insurance plan with the broadest coverage. In contrast, employment-based health insurance plans enjoy preferential tax treatment. Potential tax revenue is foregone, which must be paid for by all income taxpayers, including taxpayers who do not enjoy health insurance coverage. In another example, a government may rationalize that a decision is for the public good and use eminent domain powers to force a family to sell its private property. The private sphere is often subject to intervention by public-sphere actors. Decisions to marry and become parents are considered private prerogatives in many countries, but in some places, intense public debates are taking place as to whether gays and lesbians possess the same rights.

Do private efforts ever cross the public/private boundary to shape public efforts? An important example can be found in the welfare state. Many governments rely on pay-as-you-go approaches, by which currently employed workers support current recipients. These pay-as-you-go public systems are disrupted by reductions in tax revenues, which occur when the numbers of employers and employees and the amount of wages are reduced. Market-based relationships and events affect public policies. Health of the public sphere is significantly affected by individuals' decisions to engage intellectually and become involved in social and political debates. For a public sphere to maintain its essential contributions to a sustainable society, individuals must make efforts to stay informed, debate ideas, cooperate in decision-making, and communicate with each other.

Exhaustion is the idea that all phenomena can fit into the two categories making up the dichotomy. If a universe of phenomena exists, the dichotomy is based on this universe consisting of two parts. As suggested above, however, many phenomena cannot easily be characterized as public or private. These phenomena may represent a third sector, which is neither purely public nor purely private, but rather a hybrid. The idea of exhaustion depends on what kinds of public and private actors and institutions are contrasted. Public and private qualities of welfare policies usually contrast government-employment and government-individual efforts. Important efforts are undertaken, however, by social groups whose identifying characteristic is not employment

based but rather characterized by collective action that seeks to provide welfare to its members, such as through the work of mutual aid societies. Often designated as the social sector, in contrast to the public and private sectors, efforts of these groups may be essential to a functioning public sphere. Here it is not possible to decide whether the public/private dichotomy does or does not incorporate the social sector, but it is important to indicate that some experts approach the social sector as neither public nor private.

Is the public/private dichotomy a false dichotomy? A false dichotomy occurs when a dichotomous construct's boundary fails to produce exclusive or exhaustive categories, or both. The public/private dichotomy for social policies often violates the requirement of exclusion. Government and private entities frequently collaborate to sponsor social policy initiatives, including providing pensions, health insurance, education, and social services such as addiction treatment programs. In some instances, collaboration is less voluntary when government coerces provision by private entities. The public/private dichotomy for privacy often violates the requirement of exclusion. Governments try to shape individuals' health behaviors, for example, especially reproductive and parenting decisions. Governments also seek to monitor individuals' decisions to join organizations and form relationships with others.

The public/private dichotomy for public and private spheres often violates the requirement of exclusion. Necessary to the public sphere, libraries, television and radio broadcasts, and religious organizations also require the interest of and support from private-sphere members. The public/private dichotomy may not exhaust all possibilities. Voluntary organizations, which belong in the social sector, are often considered necessary for a healthy society, but their membership does not easily belong in either the public or private sphere. The frequency and importance of public/private collaborations raises the question of exhaustion: do the frequency and importance of public/private collaborations suggest a third type of phenomena the concept of a public/private dichotomy does not encapsulate?

What are potential harms of relying on the idea of a public/private dichotomy? Potential harms include false assumptions, hidden involvement, and inequities. Advantages are supposed to characterize the efforts of public- and private-sector actors and institutions. After recognizing the numerous violations of the exclusion component, however, these distinct advantages become fuzzy and perhaps disappear. If tax benefits are removed, will individuals be less likely to act in their own interests and save for retirement? Governments financially support and intervene in many private activities. Some private actors may not provide goods and services without government involvement, and government may provide goods and services as a result of private behaviors. Public/private collaborations can hinder democratic accountability. When we ignore public involvement and label an activity as private, government officials and their constituents may be discouraged from gathering information about how government resources are used to support such private undertakings. Labeling an activity as public may overstate the degrees of access to a good, program, or service that government provides. Inequities arise from how public and private efforts are funded and regulated. All taxpayers may foot the bill for private retirement pensions and health insurance plans, especially when these plans go bankrupt. All governments regulate and some conduct **surveillance**, but many governments regulate and observe private behaviors of some social groups more

than others. Inequalities in access to information and education can result in inequities in public-sphere participation, thereby producing public-sphere weaknesses.

Despite these dangers, why should we continue to use the concept of the public/private dichotomy? The public/private dichotomy can function as a tool and shield. It can be used to place responsibilities on the shoulders of government or non-governmental institutions. The public/private dichotomy can be employed to distinguish between public and private spheres, highlighting the importance of the public sphere in keeping governments and markets under control. The public/private dichotomy can be drawn on to describe change. It is a valuable tool for analyzing privatization and new assumptions of responsibilities and powers by private and public actors. The public/private dichotomy is useful for describing declines in public spheres. The public/private dichotomy can be effective as a shield. It can be wielded to prevent government intrusion into private decisions and other government surveillance. Social groups can deploy the public/private dichotomy to draw attention to hypocritical stances taken by governments. These social groups can point out that the same sort of behavior is considered private for some, but that government actors seek to make the behavior an issue of government regulation for other social groups.

Dichotomies are characterized as consisting of four components: division, two parts, exclusion, and exhaustion. Using this conceptualization, it is difficult to characterize the public/private dichotomy as exclusive or exhaustive. Consequently, this difficulty raises questions of whether the public/private dichotomy is a false dichotomy. It remains an open question as to whether the benefits of relying on the concept of a public/private dichotomy outweigh its costs.

See also: **Privacy, definition of; Privacy, philosophical foundation of**

Suggested Reading: Aristotle. *Politics*, trans. Peter L. Phillips Simpson. Chapel Hill: University of North Carolina Press, 1997; Fraser, Nancy. *Unruly Practices: Power, Discourse, and Gender in Contemporary Social Theory*. Minneapolis: University of Minnesota Press, 1989; Gobetti, Daniela. "Humankind as a System: Private and Public Agency at the Origins of Modern Liberalism." In Jeff Weintraub and Krishan Kumar (eds.), *Public and Private in Thought and Practice*, pp. 103–132. Chicago: University of Chicago Press, 1997; Habermas, Jürgen. *The Structural Transformation of the Public Sphere*. Cambridge, MA: MIT Press, 1991; Minow, Martha. *Partners, Not Rivals: Privatization and the Public Good*. New York: Beacon Press, 2002.

Brian Gran

Public records

Public records laws require the federal government, state governments, and many local and county governments to disclose government documents and records. Disclosures, however, can threaten personal privacy. For this reason, many of these laws permit the withholding of documents when disclosure invades personal privacy.

In the United States, such public records laws reflect the importance of the public's right to know about the operations of government. Several states enacted public records law prior to the enactment of the federal **Freedom of Information Act** (FOIA) in 1966, a statute that has become the model for many subsequent laws.



The federal FOIA exemplifies the scope of these laws. The federal law assumes that government documents and records are available to the public and that “any person” may obtain them without giving a reason for a request. The federal FOIA and other public records laws, however, permit or require government officials to withhold documents affecting interests that are protected by exemptions to these statutes.

Among the most important of these exemptions are ones designed to protect personal privacy. The federal FOIA contains two such exemptions that illustrate the character of privacy protections contained within other public records laws. One of these exemptions, the privacy exemption, allows a government agency to withhold requested documents, the disclosure of which would “constitute a clearly unwarranted invasion of personal privacy.” Another exemption applies to law enforcement records the release of which could reasonably be expected to “constitute an unwarranted invasion of personal privacy.”

The privacy exemption applies to “personnel, medical and similar files” but has been broadly defined to include any documents that implicate personal privacy interests. The language of the exemption articulates a balancing test that weighs privacy interest against the interests in disclosure. Because the exemption requires a balancing of interests, it directs that the reasons for disclosure sought by a requester be considered. The “clearly unwarranted” language indicates that balance must be strongly in favor of the protection of personal privacy for the exemption to apply.

The U.S. Supreme Court, however, has made the exemption more broadly applicable than the language of FOIA might suggest. According to the Supreme Court, only the “core purpose” of FOIA may be balanced against any possible invasion of privacy. That core purpose is to understand the operations of government. Even if the disclosure serves other laudable interests, such as improved labor-management relations, consumer understanding of the risks of products, or the commercial interests of a requester, these interests may not be balanced against any invasion of the right of privacy. Thus, even a minimal invasion of the right of privacy, such as the release of names and addresses of individuals, would constitute a “clearly unwarranted” invasion of personal privacy unless the interest served by the release falls within the “core purpose” of FOIA.

In addition, the Supreme Court has stated that a mere suspicion of government wrongdoing is insufficient to invoke the core purpose of the Act. Rather, a requester must produce evidence that would allow a reasonable person to believe that some impropriety by government officials might have occurred.

Although generally the exemptions permit but do not require the withholding of documents covered by them, the privacy exemption may limit the discretion of government officials to release documents falling under the exemption. This limitation results from the interaction of the exemption with the prohibitions against the release of certain documents under the **Privacy Act of 1974**.

The law enforcement exemption applicable to law enforcement records adopts a similar balancing test regarding the risk to personal privacy. The omission of the word “clearly” from the balancing test for this exemption provides a somewhat broader protection of personal privacy. As with the privacy exemption, only the “core purpose” of FOIA is balanced against the reasonably likely invasion of personal privacy.

In 1996 Congress enacted the Electronic Freedom of Information Act Amendments (EFOIA). That act adjusted standards and procedures to address the electronic storage of government documents. EFOIA also stressed the obligations of government to disseminate information to the public rather than to wait for requests. Some scholars feared that this emphasis on dissemination combined with the easier access to documents provided by electronic access could pose new threats to privacy. However, by increasing the likelihood that citizens might discover invasions of privacy by government agencies, EFOIA and public records laws may increase the protection of privacy by deterring such government conduct.

See also: **Disclosures; Open meetings laws**

Suggested Reading: O'Reilly, James. *Federal Information Disclosure*, 3rd ed. St. Paul, MN: West, 2000; U.S. Department of Justice. Office of Information and Privacy. *Freedom of Information Act Guide and Privacy Act Overview*. Washington, DC: U.S. Department of Justice, 2004; U.S. Department of Justice. *Freedom of Information Act Reference Guide*. http://www.usdoj.gov/04foia/04_3.html. Online, February 2006.

Robert G. Vaughn

R



Radio Frequency Identification (RFID)

Radio frequency identification (RFID) systems signal a shift toward nonvisual (or post-optic) forms of **surveillance**. Essentially, RFID systems work as unique electronic identifiers placed on items (in the form of stickers embedded with RFID chips or “tags”) or on people or animals (in the form of bracelets, badges, or implants embedded with RFID chips). Once “tagged,” humans and nonhuman objects can be identified, tracked, and managed through electronic databases. There are two main types of RFIDs: active and passive. Active RFIDs contain a miniature battery and actively emit radio frequencies to any nearby system readers. Passive RFIDs contain no battery source but instead draw the necessary power to emit a frequency through secondary “reader” devices such as mounted detectors or handheld wands, which are often called “interrogators” by industry vendors. Both types of RFIDs are “transponders” with built-in antennas for communicating with tag readers or “transceivers.” To date, these systems have been deployed by factory, shipping, retail, and entertainment industries; by hospitals, schools, and other organizations monitoring people; by public transportation departments and private transportation companies; and—of course—by the military. While the stated goal of using RFIDs is to track and manage products and resources more efficiently, the potential of RFIDs for surveillance and social control of people has caused vocal alarm among privacy advocates, technology critics, and religious groups.

Privacy advocates and others are concerned that RFIDs will enable ubiquitous identification and tracking of individuals, primarily through their products (clothes, books, ID cards, **automobiles**, food, etc.). For instance, a scheme by Gillette and UK supermarket chain Tesco to tag boxes of razors and coordinate those RFIDs with storewide surveillance systems illustrates the advanced regulation of social relations made possible by these systems. In this case, covert pictures are taken of individuals who remove boxes of razors from the “smart shelf,” and these images are then beamed to the Personal Data Assistant (PDA) devices of store security personnel. The RFIDs allow real-time tracking of those individuals throughout the store and, potentially, beyond. This development sparked significant public outcry, including online campaigns to “boycott Gillette.” What is



interesting from a surveillance studies perspective is that RFIDs integrate with older forms of visual surveillance (via closed-circuit TV), which were focused on monitoring, to provide enhanced databased surveillance predicated upon active prediction, identification, and tracking. A significant critique of RFIDs has also emerged from Christian fundamentalist groups in the United States, which interpret these technologies as “the mark of the beast” and, therefore, harbingers of the apocalypse. These groups, which are found mostly in online settings, base their interpretation on the Book of Revelation, which states, “[The beast] causes all, both small and great, both rich and poor, both free and slave, to be marked on the right hand or the forehead, so that no one can buy or sell unless he has the mark.” From this perspective, implanting RFIDs into humans (for which the company Verichip received FDA approval in 2004) represents an advanced form of “the mark,” and thus cause for personal intervention (to avoid taking the mark, perhaps unwittingly) and collective mobilization (to warn others). Interestingly, privacy advocates and Christian fundamentalists agree that societies must critically investigate the social ramifications of RFID technologies, but they come to this shared conclusion from radically divergent political orientations—leftist-progressive and ultra-conservative, respectively.

See also: **Video cameras**

Suggested Reading: Cameron, Heather. “CCTV and (In)dividuation,” *Surveillance & Society* 2: 2/3 (2004): 136–144. [http://www.surveillance-and-society.org/articles2\(2\)/individuation.pdf](http://www.surveillance-and-society.org/articles2(2)/individuation.pdf); Fisher, Jill A. “Indoor Positioning and Digital Management: Emerging Surveillance Regimes in Hospitals.” In Torin Monahan, (ed.), *Surveillance and Security: Technological Politics and Power in Everyday Life*, pp. 77–88. New York: Routledge, 2006; Weis, Stephen August. “Security and Privacy in Radio-Frequency Identification Devices.” M.S. thesis, Massachusetts Institute of Technology, 2003. <http://theory.lcs.mit.edu/~cis/theses/weis-masters.pdf>.

Torin Monahan

Real ID Act of 2005. *See* National identity cards

Reasonable expectation of privacy

The “reasonable expectation of privacy” test is applied to determine whether the Fourth Amendment to the U.S. Constitution will protect against certain searches and seizures by government officials. The test was first formulated by the U.S. Supreme Court in *Katz v. United States*, 389 U.S. 347 (1967). The test actually appeared in a concurring opinion by Justice Harlan, who stated the Fourth Amendment covers a search or seizure if (1) a person exhibits an “actual or subjective expectation of privacy” and (2) “the expectation [is] one that society is prepared to recognize as ‘reasonable.’”

What constitutes a reasonable expectation of privacy? The answer is rather difficult because it involves understanding a litany of Supreme Court decisions in particular cases. There is no particular formula for determining when a reasonable expectation of privacy exists. Therefore, one must look at the specific circumstances of each case in which the Supreme Court rendered a decision and make generalizations and analogies. In *Katz*, the Supreme Court famously stated,

For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.

In practice, however, the Court has not always adhered to this approach. In several cases, the Supreme Court has concluded that people lack a reasonable expectation of privacy when they are observed in public. In what is known as the **plain view doctrine**, the Supreme Court has held that “it has long been settled that objects falling in the plain view of an officer who has a right to be in the position to have that view are subject to seizure and may be introduced in evidence” (*Harris v. United States*, 390 U.S. 234, 236 (1968)). In *Florida v. Riley*, 488 U.S. 445 (1989), for example, the Supreme Court held that a person lacked a reasonable expectation of privacy in his greenhouse where the roof was partially open to a view from above and where the police flew over it in a helicopter to peer inside.

People also lack a reasonable expectation of privacy in being overheard when speaking in a public place. In private places, however, if people cannot be seen or heard by others, then generally they will be deemed to have a reasonable expectation of privacy.

Consistent with the view that people lack a reasonable expectation of privacy in public, the Supreme Court has held that a person lacked a reasonable expectation of privacy when law enforcement officials installed a physical-tracking device that monitored where he drove in his car. According to the Court, a “person traveling in an **automobile** on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another” (*United States v. Knotts*, 460 U.S. 276 (1983)). In contrast, a tracking device that monitored a person's movements in his home did infringe upon his reasonable expectation of privacy (*United States v. Karo*, 468 U.S. 705 (1984)). Whereas the movements in *Knotts* were in public, the movements within the residence were not, and this amounted to an impermissible search of the residence.

The police can apply sensory enhancement technology to what they see or hear with the naked senses. In *Texas v. Brown*, 460 U.S. 730 (1983), the Supreme Court held that using a flashlight to “illuminate a darkened area” did not implicate a reasonable expectation of privacy. In *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986), government officials flew over the defendant's property and used a high-tech aerial-mapping camera to take photographs, which could then be magnified to reveal very small objects. The Supreme Court concluded that there was no reasonable expectation of privacy because the “mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems.”

There are instances, however, when using sensory enhancement technology can implicate a person's reasonable expectation of privacy. In *United States v. Kyllo*, **533 U.S. 27 (2001)**, the police used a **thermal sensor** imaging device to detect heat patterns coming from a person's home. Although the police did not enter the residence, the device measured the heat emanating from the residence. The Supreme Court nevertheless concluded that the defendant had a reasonable expectation of privacy because the device could be used to detect activities within his home.



The Supreme Court also has concluded that people lack a reasonable expectation of privacy in information exposed to third parties. This has become known as the “third-party doctrine.” For example, in *United States v. Miller*, 425 U.S. 435 (1976), the Court held that people lack a reasonable expectation of privacy in their bank records because “[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.” Employing analogous reasoning in *Smith v. Maryland*, 442 U.S. 735 (1979), the Court held that people lack a reasonable expectation of privacy in **pen register** information (the phone numbers they dial) because they “know that they must convey numerical information to the phone company,” and therefore they cannot “harbor any general expectation that the numbers they dial will remain secret.” Similarly, in *California v. Greenwood*, 486 U.S. 35 (1988), the Supreme Court concluded that people cannot have a reasonable expectation of privacy in trash left for collection on the curb because they “exposed their **garbage** to the public” and “placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector.”

The third-party doctrine is difficult to square with other Fourth Amendment doctrines. If a person is talking on the phone to another person, this does not negate either person's reasonable expectation of privacy, even though the two are sharing information with each other. One of the parties to the conversation can betray the other, and people do not have a reasonable expectation that their confidants will not communicate their secrets to the police. However, so long as both parties to the conversation have resolved to keep the conversation private, they have a reasonable expectation of privacy if they did not speak in public or where audible to others. Nevertheless, if a person provides information to a bank or a company, then the person has been deemed to have relinquished his reasonable expectation of privacy—even if the bank or company desires that the information be kept private. The Court has not explained why exposing information to a bank or company is different from exposing it to another conversant over the telephone.

The third-party doctrine also gives rise to some difficult issues because of life in the information age. Countless companies maintain detailed records of people's personal information: **Internet** service providers, merchants, bookstores, phone companies, cable companies, and many more. According to the third-party doctrine, a person lacks a reasonable expectation of privacy in this information because third parties possess it.

Taken together, the cases suggest that the Supreme Court believes that people lack a reasonable expectation of privacy whenever something is exposed to the public or to third parties. In other words, if a person keeps something a total secret, then he can reasonably expect it to be private. However, once something is revealed in public or to others, then he can no longer reasonably expect privacy.

Methodologically, how does the Supreme Court determine whether there is a reasonable expectation of privacy? At first glance, the reasonable expectation test appears to be empirical: a reasonable expectation of privacy is an expectation that a majority of members in society deem reasonable. However, in applying the test, the Supreme Court has rarely looked to empirical evidence or to polls. Instead, the Court has typically applied its own notions of privacy. In at least one instance, the

Court acknowledged that the “reasonable expectation of privacy” test has a normative dimension:

For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such circumstances, where an individual's subjective expectations had been “conditioned” by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a “legitimate expectation of privacy” existed in such cases, a normative inquiry would be proper (*Smith v. Maryland*, 442 U.S. 735, 741 n.5 (1979)).

A broader conclusion might be drawn from the preceding statement. Perhaps the “reasonable expectation of privacy” test should measure whether privacy in a particular matter is normatively desirable, as expectations can erode over time as technology advances. On the other hand, under such an approach, who determines what is normatively desirable? Some critics are skeptical as to whether it is appropriate for judges to be making such normative judgments for society.

Other critics have charged that the “reasonable expectation of privacy” test has, in practice, led to a curtailment of Fourth Amendment privacy protection. Many cases applying the test have concluded that there is no reasonable expectation of privacy, and hence no Fourth Amendment protection. Despite much criticism and controversy, the “reasonable expectation of privacy” test remains the central criterion courts use to determine the scope of Fourth Amendment protection.

See also: Constitutional protections

Suggested Reading: Amsterdam, Anthony G. “Perspectives on the Fourth Amendment,” *Minnesota Law Review* 58 (1974): 349–367; Slobogin, Christopher, and Joseph E. Schumacher. “Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at ‘Understandings Recognized and Permitted by Society,’” *Duke Law Journal* 42 (1993): 727; Solove, Daniel J. “Digital Dossiers and the Dissipation,” *Southern California Law Review* 75 (2002): 1083; Stuntz, William J. “Privacy’s Problem and the Law of Criminal Procedure,” *Michigan Law Review* 93 (1995): 1016; Sundby, Scott E. “‘Everyman’s’ Fourth Amendment: Privacy or Mutual Trust between Government and Citizen?” *Columbia Law Review* 94 (1994): 1751.

Daniel J. Solove

Red & Black Publishing Co. v. Board of Regents, 262 GA. 848 (1993)

In the case of *Red & Black Publishing Co. v. Board of Regents*, the staff of the student newspaper at the University of Georgia, *The Red and Black*, believed that it should be granted access to the records and proceedings of the university’s student organization court. Specifically, in this instance it desired access to the records and proceedings dealing with hazing charges brought against two fraternities. *The Red*



and *Black* filed suit against the university's Board of Regents, including university president Charles Knapp and others, under Georgia's Open Records Act and **Open Meetings Act** after its request for access to the records was denied.

The Supreme Court, in accordance with the trial court, ruled that the newspaper was entitled to the organization court's records; however, unlike the trial court, it also deemed the proceedings to be accessible. The Supreme Court based its ruling, in part, on the definition of the term "open records" under Georgia's Open Records Act, as any material processed in a public agency or office. It noted that the act's purpose is to promote the openness of such material so that the public may monitor its institutions as well as maintain trust in them. The organization court was formed as part of a public institution, the University of Georgia, which is governed by a public agency, the Board of Regents. Thus, the Court concluded that the organization court's records were public and therefore accessible to the student newspaper. Although the defendants argued that the **Family Educational Rights and Privacy Act (FERPA)**, otherwise known as the Buckley Amendment, did not require them to disclose the records, the Supreme Court considered this impertinent since the purpose of the Buckley Amendment was not to protect individuals' privacy, but to prevent institutions from carelessly releasing education records. Furthermore, it did not consider the organization court's records to be of the same nature as the education records protected under this amendment.

The Supreme Court noted that the purpose of Georgia's Open Meetings Act is similar to that of the Open Records Act in that it protects the public by allowing it to monitor the governmental proceedings of public agencies at which official business and policies are discussed. While the organization court is not a governmental agency or body in the same sense as the Board of Regents, the Court held that it was equivalent under the Open Meetings Act. The organization court was created by the university; holds its sessions on the campus; and, has the job of discussing, enacting, and deciding on policies and regulations dealing with the university's social organizations.

To determine a verdict in this case, the Supreme Court based its decision on the implications of certain prior acts and amendments as well as on the definitions of significant terms that arose in the proceedings. In addition, it noted that the state required such business to be open to the public under the two acts discussed. Although decisions on the issue of privacy are difficult to make, perhaps future courts will find the reasoning in this specific incident useful for their own justifications.

See also: Associated Press v. Walker, 388 U.S. 130 (1967); *Bauer v. Kincaid* 759 F. Supp. 575 (1991); *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975); **Open meetings laws; Public records; Time, Inc. v. Hill**, 385 U.S. 374; *United States v. Caldwell*, 408 U.S. 665 (1972)

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Hall, Kermit L. *Conscience, Expression, and Privacy: The Supreme Court in American Society*. New York: Garland, 2000; Smith, Robert Ellis. *Compilation of State and Federal Pri-*

vacy *Laws*. Providence, RI: Privacy Journal, 1992; Sullivan, Kathleen M., and Gerald Gunther. *First Amendment Law*. St. Paul, MN: West, 1998.

Sean M. Peek

Red-light and speeding cameras

Red-light and speeding camera systems automate some of the traffic enforcement functions of police. The technologies can include radar or laser detection devices, electromagnetic loops embedded in the road, pole-mounted or portable cameras, microprocessors, and networking devices. Most of the older systems rely on 35 mm film, which must be routinely extracted from the units; newer systems employ digital and video cameras and send the information over data networks. In theory, when an **automobile** trips an electronic sensor after a traffic light changes to red, or when a vehicle's speed exceeds the posted limit by a certain amount (usually 10 mph in the United States), photographs are taken of the front and rear of the vehicle (i.e., of the driver and the license plate, respectively). The owner of the vehicle may then be sent a citation or a notice to "nominate" the actual driver of the vehicle at the time of the alleged violation. Currently, 45 countries use such systems; in the United States, the systems are active in 19 states and the District of Columbia.

Privacy advocates and others have vocally opposed such systems. The key concerns involve the potential for **surveillance** creep, the attenuation of constitutionally guaranteed due process and equal protection, and the apparent conflicts of interest and lack of transparency entailed by the outsourcing of police functions to private industries. First, surveillance creep is a serious concern with technological systems such as these, because they allow the indefinite retention of data, making it possible—and likely attractive—for law enforcement agencies and others to access the data for purposes beyond the intended functions of the systems. It is also possible that unintentional breaches of privacy can occur, such as in a well-documented case in Hawthorne, California, where a picture of a woman and her lover was sent, in the form of a citation, to the woman's husband. Second, the Due Process and Equal Protection clauses of the U.S. Constitution may be conveniently ignored by police departments and the courts that perceive the technological systems as somehow "neutral" and therefore fairer than individual law enforcement agents in targeting traffic crimes. However, compelling cases have been made that significant threats to **constitutional protections** are occurring. Not everyone is being photographed. Punishments can vary depending on whether one is cited by an officer or by the automated system. Data unrelated to the violation are being collected and stored; and, those being accused of breaking the law have no recourse to challenge their accusers in court—meaning, in effect, that they are guilty until proven innocent. Finally, the privatization of police functions has introduced a host of secondary concerns about the profit interests and **secrecy** of the companies operating these systems. Notably, a judge in San Diego, California, found that the evidence generated by these systems was unreliable because the private company operating them received a percentage of the fines and evidently "rigged" the system to increase its profits. What this example demonstrates is that, far from being neutral, the technologies are embedded with the values and interests of their designers, who in most cases are private companies with no obligations of public accountability.



As might be expected, individuals have developed vibrant “countersurveillance” techniques to neutralize the effectiveness of red-light and speeding camera systems. These include extreme measures such as destroying cameras; using various sprays, shields, or automated camera flash guns to make license plates illegible; or using **Global Positioning System (GPS)** devices, radar or laser detectors, or maps of camera locations to facilitate avoidance of, or behavior modification around, known cameras.

Suggested Reading: Association of British Drivers. *Speed Camera Map of Great Britain*. <http://www.abd.org.uk/cameras/map.htm>. Online, April 2006; Delaney, Amanda, Heather Ward, and Max Cameron. *The History and Development of Speed Camera Use*. Victoria, Australia: Monash University Accident Research Centre, 2005. <http://www.monash.edu.au/muarc/reports/muarc242.pdf>. Online, April 2006; HighwayRobbery.net. *Illegal Red Light Cameras*. <http://www.highwayrobbery.net/>. Online, April 2006; Nieto, Marcus, Kimberly Johnston-Dodds, and Charlene Wear Simmons. *Public and Private Applications of Video Surveillance and Biometric Technologies*. Sacramento: California Research Bureau, 2002. <http://www.library.ca.gov/crb/02/06/02-006.pdf>. Online, April 2006.

Torin Monahan

Reproductive rights

Reproductive rights refers to a compilation of issues related primarily to women’s rights to bear and raise children as well as their rights not to do so. Matters such as **birth control**, emergency contraception, **abortion**, **sterilization**, **assisted reproductive technologies**, and fetal rights are included in the moral and legal debates surrounding reproductive rights. While questions surrounding the control of reproductive capacities have a long history, the term “reproductive rights” came into popular usage in the 1960s, during a time of technological advancement, sexual revolution, and a general “rights explosion.” Currently, women’s reproductive rights are guaranteed as individual rights to privacy rather than rights of **gender** equality. Public and political debates over reproductive control are not woman-centered; rather, they are aimed at addressing large-scale social or economic problems.

There is an intricate connection between reproductive rights and privacy. Although the word “privacy” does not actually appear in the U.S. Constitution, an underlying notion of individual autonomy and privacy are evident in the Fourth Amendment’s guarantee against unlawful search and seizure and the Fifth Amendment’s shield against self-incrimination. While these **constitutional protections** have been extended to reproductive rights, a woman’s right to privacy in such matters is rooted in the Fourteenth Amendment’s assurance of individual liberty. Before his appointment to the Supreme Court, then lawyer **Louis Brandeis** argued that this embedded right to privacy would lead to a judicial “**right to be let alone**.” This notion became salient in the case of *Griswold v Connecticut*, **381 U.S. 479 (1965)**, which overturned the illegality of birth control by married couples. In this case, the marital bedroom was designated as “**a zone of privacy**.”

While *Griswold* laid the foundation for reproductive rights as a privacy issue, the landmark abortion case of *Roe v. Wade*, **410 U.S. 113 (1973)**, further established this right. Although the Court argued that abortion was foremost a medical

issue, Justice Henry Blackmun's opinion that the Due Process Clause of the Fourteenth Amendment guarantees a woman's right to privacy prevailed as a victory for reproductive rights activism. However, this right to privacy, like First Amendment rights, may be reduced if the state has a compelling interest in the issue. This is evident in *Roe*'s creation of a trimester system, with women granted some level of autonomy and bodily integrity during the first three months of pregnancy. During this time, the individual woman, in consultation with her doctor, remained free to make decisions regarding the progression of her pregnancy. A woman's right to privacy decreased in the second trimester, when her health is defined by the state as more vulnerable. Finally, in the third trimester, the state's right to protect a viable fetus (one that could potentially live outside the womb) usurps a woman's right to privacy and justifies state intervention to prevent an abortion, unless it is necessary for preserving the mother's life or health. This trimester system has had contradictory effects, expanding women's reproductive control on one hand while legalizing state intervention on the other. Ultimately, the ruling in *Roe* placed the control of pregnant bodies in the hands of physicians.

Roe faced a potential overturn in the 1992 case of *Planned Parenthood of Pennsylvania v Casey*. This case addressed the limitations and regulations of abortion even in the first trimester, including: provisions for a 24-hour waiting period; spousal consent; parental consent; informed consent on the part of the pregnant woman; and, reporting regulations. The Court fractured into three blocs, but *Roe* was not overturned. Instead, the trimester system was replaced with a framework of "undue burden," and all of the abortion restrictions, with the exception of spousal consent, were upheld. The Court indicated that the public had come to rely on the right to abortion put forth in *Roe*, but now states could limit access as long as they did not place "a substantial obstacle in the path of a woman seeking an abortion of a nonviable fetus." Reproductive rights advocates argue that the legal restrictions to abortion approved under the *Casey* ruling challenge women's right to privacy and limit control of their own bodies.

Social policies such as the Hyde Amendment, which allows federal money for abortions only in instances where the woman's life is threatened, limit the reproductive rights of many women. In 2000 federal policies were expanded to permit funds for abortions in cases of rape or incest as well. Currently, 20 states allow the use of their funds for abortions, while 30 have no public assistance for such acts. The right to choose whether or not to continue a pregnancy relates directly to a woman's financial capability to be a properly legitimate mother. At the same time, those women who do not meet middle-class standards of legitimate motherhood are not provided with the social and financial support to end their pregnancies. Opponents to reproductive rights place the interests of the unborn over an individual woman's right to privacy by prohibiting federal funding for abortion. By limiting funds for abortions, social policies refute the idea that limiting family size has benefits for society as a whole. Because poverty does not demand special consideration under the Constitution, the right to privacy in procreative matters is not universal.

In the decades since *Roe*, fetal personhood has stood at the center of anti-abortion campaigns. Proponents of fetal personhood argue that the fetus has rights—like living, breathing people—and those rights can be distinguished from those of the pregnant woman. Advocates of fetal protection maintain that the state has an



obligation to secure the interests of the unborn. Several protectionist policies developed in the last decades of the twentieth century placed fetal rights above women's individual rights. These policies resulted in the prosecution of women for dispensing drugs to minors via the umbilical cord, and the banning or restriction of fertile (although not necessarily pregnant) women from hazardous workplaces. Some pregnant women have been ordered to undergo medical treatment, including cesarean sections, against their will, and others have lost custody of their children as a result of behaviors during pregnancy that the state deemed threatening to the potential life of the unborn fetus. Reproductive rights activists challenge these policies as an invasion of the pregnant woman's privacy. Unlike other conflicts of individual rights, the issue of fetal rights is complicated by the physicality of pregnancy. Fetal protection demands that the pregnant woman's individual rights be violated to protect those of the fetus. The social pressure to protect the fetus is likely to further challenge women's control of their own bodies, especially since the possibilities for additional restrictions on pregnant women's conduct are unlimited. The current debate could lead to the prosecution of women who fail to follow physicians' advice to exercise during pregnancy, to limit alcohol intake, or to take prenatal vitamins. As long as moral and legal motivations underlie support for fetal rights, women's rights are in jeopardy. The status of the fetus, desired or not, determines whether fetal rights or women's right to privacy prevail.

Race and social class play an important role in reproductive rights and result in social policies that assign differing social importance to groups of babies based on these characteristics. Because society values the reproduction capacity of some women while disregarding that of others, white women and other women of **privilege** have historically fought for reproductive autonomy to liberate themselves from the notion of motherhood as biological destiny. Women of color, on the other hand, have challenged governmental policies that have alternately compelled or restricted their reproductive capacity depending on social demands and attitudes. During slavery, black women, viewed as capital, were forced to procreate to further their owners' holdings. Eugenics in the 1920s resulted in forced sterilization for those deemed socially unfit. During the early 1970s, federally funded experimental trials of Depo-Provera resulted in the sterilization of more than 100,000 poor women, nearly half of whom were black. Currently, poor and minority women are more likely to be subjected to forced medical treatment during pregnancy. The fear of forced treatment could deter women from seeking any prenatal care, further endangering their health and the health of the fetus. Public authorities overwhelmingly associate poor women and women of color with social problems, such as drug-addicted newborns, "welfare queens," and teenage pregnancy. Ultimately, women of color and poor women are faced with different realities when reproduction is considered a privacy issue.

Reproductive rights straddle the **public/private dichotomy** of American society. Women's private decisions about whether to have children do not exist in a vacuum. Laws and policies shape women's rights to privacy and place women's reproductive control in the public context. Society's desire to grant women rights of bodily integrity has a relatively short history in the United States, gaining legal recognition with *Roe* and *Casey* only late in the twentieth century. Thus, women's

reproductive rights face a tenuous future as an individual woman's rights compete with those of the unborn and the best interest of the state.

See also: **Constitutional protections; Gender; Privacy, definition of; Women and privacy**

Suggested Reading: Daniels, Cynthia R. *At Woman's Expense: State Power and the Politics of Fetal Rights*. Cambridge: Harvard University Press, 1993; Gordon, Linda. *Woman's Body, Woman's Right: Birth Control in America*. Revised and updated. New York: Penguin Books, 1990 [1976]; Solinger, Rickie (ed.). *Abortion Wars: A Half Century of Struggle, 1950–2000*. Berkeley: University of California Press, 1998; Solinger, Rickie. *Pregnancy and Power: A Short History of Reproductive Politics in America*. New York: New York University Press, 2005.

Tori Barnes-Brus

Restrooms and dressing rooms

Restrooms are rooms or areas that are often equipped with a toilet, shower, and sink in which an individual typically would wash, shower, urinate, or defecate. Dressing rooms are rooms or areas that are designated for changing clothes, applying makeup, or other, similar conduct. These types of activities are traditionally performed within an enclosed or secluded setting because they innately invoke a sense of privacy.

Although there is no uniform definition of privacy, it is generally accepted that privacy includes a desire to shield one's body, including genitalia or "**private parts**," as well as certain activities, ranging from defecating to bathing and trying on clothing in a retail dressing room, from the **plain view** of other individuals. In fact, public display of some of these activities is often considered taboo.

Restrooms and dressing rooms furnish a measure of privacy protection to an individual who is engaging in activities such as bathing by limiting the access available to others, and thus limiting the opportunity of exposure to others. As a general matter, the level of protection afforded depends upon whether society considers the individual to have a **reasonable expectation of privacy**. Typically, by going behind the closed doors of a bathroom or dressing room, an individual may reasonably expect not to be observed by others.

"Peeping Toms," however, often commit acts of **voyeurism** by targeting restrooms and dressing rooms for the purpose of spying on an individual in various states of undress. Because of the innate privacy concerns involved, this is often illegal.

Public restrooms and retail dressing rooms, however, may be legitimately subject to limited **surveillance** under certain circumstances. For example, privacy interests may be weighed against the interests in law enforcement and the prevention of shoplifting. Therefore, where a property owner posts a conspicuous warning of surveillance, or where the restroom or dressing room reasonably does not suggest that it offers privacy protection, an individual engaging in private activities therein may not be considered to have acted reasonably by expecting to remain private. As a general matter, however, nonconsensual observation or image recording of occupants of restrooms and dressing rooms is prohibited by law.

See also: **Privacy, definition of**



Suggested Reading: Alderman, Ellen, and Caroline Kennedy. *The Right to Privacy*. New York: Alfred A. Knopf, 1995; Aries, Philippe, and Georges Duby. *A History of Private Life, Vols. I–V*. Cambridge, MA: Belknap Press, 1992; McClurg, Andrew. “Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places,” *North Carolina Law Review* 73 (1995): 989.

Lance E. Rothenberg

Right to be let alone

The origin of a legal remedy for invasion of privacy is most often traced to the writings of former Harvard Law School roommates Samuel D. Warren and **Louis D. Brandeis** (class of 1877). Later in his career, Brandeis served on the United States Supreme Court from 1916 to 1939. Warren founded a prominent Boston law firm that still exists today. In 1890, after Warren had wooed Brandeis to his firm, the upstart lawyers convinced the *Harvard Law Review* to publish their article “The Right to Privacy.” There they defined an expansive concept of privacy and the steps private individuals could take to protect those privacy rights. However, the “right to be let alone” was first described in the writings of a lesser-known Michigan jurist.

Thomas M. Cooley began his professional life as city clerk, then newspaper editor, and later circuit court commissioner. Once he turned his attention to the practice of law, he began to amass what has been called “the most distinguished legal record of any man whose name has been associated with the jurisprudence of Michigan.” He became a state court justice in 1864.

When the University of Michigan Law School began operations in 1859, Cooley was one of the first professors hired. At the school he taught constitutional law, real property, trust, estates, and domestic property. In addition to teaching, he wrote numerous legal articles on varied subjects, including constitutional limitations, Blackstone’s Commentaries, Story’s Commentaries, and torts. His 1888 treatise on the law of torts included the “right to be let alone.” As Cooley described the right, it was a right to be free from assault or threats of violence. As he characterized it, “The right to one’s person may be said to be a right of complete immunity: to be let alone.”

Brandeis and Warren modified that “right” to accomplish their own purposes. According to popular legend, Warren was appalled by newspaper reports about his daughter’s wedding. Although this story is refuted by some scholars, it is clear that Brandeis and Warren felt that individuals should be free from fear that newspapers would scrutinize their private lives and publish details that constituted little more than idle **gossip**. They explained, “Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’” The authors ranted against the press’s “overstepping . . . the obvious bounds of propriety” in an effort to satisfy the “prurient taste” of readers.

To explain their proposed cause of action, the authors traced the development of common law and actions to protect individuals from threats to their bodies as well as to their reputations, concluding that the time was ripe for the application of those principles as a remedy for the “evils” of the press. They suggested that the right to privacy would not proscribe all publications, but rather would protect “those per-

sons with whose affairs the community has not legitimate interest.” They also proposed that all persons should have the right to prevent publication of “matters which they may properly prefer to keep private.” Their goal was “to protect the privacy of private life.”

Brandeis and Warren acknowledged that publication of matters of **public record**, court actions, and the like would not be covered under their right of privacy. Their right also would not allow an action for its violation unless there was “a special damage,” nor would there be any right to claim an invasion of privacy if the publication was made by or with the consent of the subject of the publication. When there was an “invasion,” however, truth would provide no defense for the publisher, nor would the absence of malice. They suggested that remedies for those wronged should include damages for “injury to feelings,” as well as an injunction in limited cases.

Today the federal courts, most states, and the District of Columbia recognize a right of privacy, and the limits of the tort of public **disclosure** of private facts are well established: (1) private facts must be publicly disclosed; (2) the “private” facts must not be matters of which the public has a right to know, and cannot be “news-worthy,” lest the legal protections come in direct conflict with the freedom of the press; and (3) the matters made public must violate the public’s sense of decency or be offensive and objectionable to a reasonable person of ordinary sensibilities.

See also: **Privacy, definition of; Privacy torts**

Suggested Reading: Purcell, Edward A., Jr. *Brandeis and the Progressive Constitution*. New Haven, CT: Yale University Press, 2000; Solove, Daniel, Marc Rotenberg, and Paul Schwartz. *Information Privacy Law: Cases and Materials*. New York: Aspen, 2005; Strum, Philippa. *Brandeis: Beyond Progressivism*. Lawrence: University Press of Kansas, 1993.

David J. Brown

Right to die

The right to die is a relatively recent development in society, brought about by dramatic advances in medical technology beginning in the 1960s. The legal case that launched the societal discussion involved a 21-year-old woman from New Jersey who collapsed and ended up in a New Jersey hospital emergency room on April 15, 1975. The whole country soon knew her name: Karen Ann Quinlan. Doctors did not know the cause of Quinlan’s collapse, but she apparently experienced a significant period without oxygen before being resuscitated. The technique that the “rescue squad” used to revive her in her house, called cardiopulmonary resuscitation or CPR, had originated a little more than 10 years earlier. In the hospital she could not breathe on her own, and doctors cut a hole in her throat (a tracheotomy) and inserted a tube that was connected to another fairly recent invention, a large respirator that did the breathing for Quinlan.

After Quinlan spent a short period in a coma, her eyes opened. However, doctors told her family that she had not regained consciousness. They called her condition “the persistent vegetative state,” a diagnosis named only three years earlier, in 1972, by Drs. Fred Plum and Bryan Jennett in the prestigious medical journal *The Lancet*. This condition was the by-product of increasingly sophisticated lifesaving



techniques at accident sites and better-equipped emergency rooms. Patients who previously would have died were brought back from the brink of death, but not all the way back. In the early 1970s doctors were seeing more and more patients in this condition, necessitating a diagnosis and a name. Quinlan's parents faced a question that was new to society: If this medical technology could do no more than keep Karen Ann Quinlan suspended in a state of permanent unconsciousness, would it be best to turn off the respirator and allow her to die naturally? Ultimately, the question came before the New Jersey Supreme Court, which concluded that Quinlan, though unconscious, retained a right to privacy that allowed her to refuse unwanted medical treatment. The court stated that her parents could exercise this right on her behalf. Once the doctors turned off the respirator, however, Quinlan was able to breathe on her own. She lived, unconscious in a persistent vegetative state, for 10 more years, succumbing to pneumonia on June 11, 1985.

In the wake of the *Quinlan* case, the federal government convened the President's Commission for the Study of Ethical Problems in Medicine and Biomedical and Behavioral Research, which issued several reports analyzing the difficult legal and ethical issues raised by advancing technology, such as those in the circumstance of Karen Ann Quinlan. The commission issued a separate report on another amazing topic created by medical technology: the definition of death itself. For most of human history, a person who was dead, was dead; one's heart, lungs, and brain all stopped at roughly the same time. Technology changed that equation, and the President's Commission wrestled with the question of defining a person as dead by law, even though that person's heart and lungs continued to function with the support of technology. The term "brain death" was born. In addition to the President's Commission, many state legislatures, medical and legal groups, and others investigated ways to address these new issues. Most states passed laws authorizing citizens to complete a document called a "living will." Through such documents, people could attempt to make their wishes about medical treatment known ahead of time, in case they found themselves unable to communicate, like Karen Ann Quinlan.

In 1990 the American public tackled its second national right-to-die situation, involving a young woman from southern Missouri named Nancy Cruzan. Cruzan suffered significant oxygen deprivation to the brain because of a car accident on January 11, 1983. Like Karen Ann Quinlan, she lapsed into the eyes-open unconsciousness of the persistent vegetative state. Unlike Quinlan, however, Nancy Cruzan's parents sought court approval to remove artificial nutrition and hydration, or a feeding tube, rather than a respirator. Also with Cruzan, the public saw for the first time still photos and videotape footage of exactly what the persistent vegetative state looked like (Quinlan's parents only released her black-and-white high school yearbook photo). Ultimately, the Cruzan case ended up before the U.S. Supreme Court. The 1990 decision in *Cruzan v. Director, Missouri Dep't of Health*, 497 U.S. 261 (1990), established the constitutional right of all Americans to refuse unwanted medical treatment. The Court also reasoned that a feeding tube was medical technology, like a respirator or dialysis, and a device that had taken the place of a natural function lost due to accident or illness. In the wake of *Cruzan*, Congress passed a law called the Patient Self Determination Act, which provides that all patients entering a hospital in the United States must be counseled about living wills and other types of health care planning.

In the spring of 2005, the third major right-to-die circumstance came into the public spotlight, involving a young Florida woman named Terri Schiavo. Like Cruzan and Quinlan, Schiavo was in a persistent vegetative state, and like Cruzan, Schiavo's case involved a feeding tube. Unlike the two earlier cases, however, the Schiavo case pitted the husband, Michael Schiavo, against Terri Schiavo's parents, Bob and Mary Schindler, in a bitter public court battle over her fate. Her husband sought the removal of her feeding tube, and her parents opposed that effort. Ultimately, the dispute went through a series of trials and appeals over 10 years, with different interest groups becoming involved on both sides. During this skirmish, Terri Schiavo's tube feeding was stopped and restarted twice. The second time, the tube was reinserted when the Florida legislature passed a law, soon known as Terri's Law, which ordered that the tube be reinserted. The court battle continued, and near the end even the federal government and the president attempted to weigh in. The courts eventually ruled in favor of the husband, and Terri Schiavo died on March 31, 2005, 13 days after the removal of her feeding tube.

At the start of the twenty-first century, American society is in many ways only beginning to tackle the hard questions raised by relentlessly advancing medical technology. In a little more than 40 years, that technology has moved from the invention of the respirator to the capability of doctors in New York to perform surgery on a woman in France using a robot and images transmitted over a cable at the bottom of the Atlantic Ocean. Changes are coming at a breathtaking pace to a population that is aging rapidly. The huge demographic bulge consisting of people popularly known as Baby Boomers is poised to enter "old age." The U.S. Census Bureau estimates that the population of those 85 years and older will more than quadruple between the years 2000 and 2050, from 4 million to 18 million. In the year 2000, only Florida had a population at least 17 percent of which was age 65 or older. By the year 2030, the Census Bureau estimates that 44 states will look like Florida does now. Hard questions about the goal of medicine and what rights people have in demanding or refusing medical treatment are only going to grow more difficult, and more frequent. American society will be debating and shaping the framework of those rights, including the right to die, for years to come.

See also: **Privacy, philosophical foundations of**

Suggested Reading: Caring Connections. www.caringinfo.org. Online, December 2005; Colby, William. *Long Goodbye: The Deaths of Nancy Cruzan*. Carlsbad, CA: Hay House, 2002; Colby, William. *Unplugged: Reclaiming Our Right to Die in America*. New York: AMACOM Books, 2006; Webb, Marilyn. *The Good Death: The American Search to Reshape the End of Life*. New York: Bantam Books, 1997.

William H. Colby

Right to Financial Privacy Act. *See* **Banking and financial records**

Roe v. Wade, 410 U.S. 113 (1973)

This landmark decision of the U.S. Supreme Court remains at the center of national debates over whether terminating pregnancies should be legal. The opinion contains a lengthy survey of the history of **abortion**, which illustrates that restrictive criminal abortion laws are relatively modern in origin. In *Roe v. Wade*,



the Supreme Court held a woman's right to an abortion to fall within the right to privacy and therefore to be protected by the Fourteenth Amendment of the U.S. Constitution. This right was found to be not absolute, however, and laws regulating abortion practices could be upheld if they were narrowly tailored to satisfy a compelling state interest. The decision in *Roe* is significant because it held that a woman's right to choose is a fundamental constitutional right of privacy and also because the decision represents the first steps by the judiciary to determine just how far this right should extend.

The Texas statutes at issue in the case made it a crime to procure an abortion, or to attempt one, except for the purpose of saving the life of the mother. Texas first enacted a criminal abortion statute in 1854. "Jane Roe," a single woman residing in Dallas County, brought this cause of action in March 1970 against the district attorney of the county. The case requested a declaratory judgment that the Texas criminal abortion statutes were unconstitutional and that the state should be restrained from enforcing statutes that criminalize abortion.

In her initial federal action, "Jane Roe" alleged that she was unmarried and pregnant and that she wished to terminate her pregnancy by an abortion performed by a licensed physician. Since her life was not threatened, she was unable to get a legal abortion in Texas, and she could not afford to travel outside the state to have the procedure. She claimed that the Texas statutes were unconstitutionally vague and that they abridged her right of personal privacy as protected by various U.S. constitutional amendments. After the initial case was filed, the suit was expanded to include several other parties, such as James Hubert Hallford, a physician who had been arrested for violations of the Texas abortion statutes, and "John and May Doe," a married couple whose doctor had advised them against pregnancy. Finding that the other parties were not appropriate plaintiffs in the litigation, the Supreme Court decided the case based solely on the complaint brought by "Jane Roe."

The central issue decided in *Roe v. Wade* was whether the Texas statutes that criminalized abortion, except in instances where the mother's life was threatened, improperly invaded a women's right to choose to terminate her pregnancy. The first question the Court addressed was whether there exists a private right to an abortion guaranteed in the U.S. Constitution. While the Constitution does not explicitly mention any right of privacy, in decisions dating as far back as 1891 the Supreme Court has recognized that a right of personal privacy, or a guarantee of certain areas or **zones of privacy**, does exist pursuant to the several constitutional amendments.

The decision in *Roe* found that while the roots of the privacy rights at issue in the case were contained in several constitutional amendments, they lay chiefly in the Fourteenth Amendment and the guarantee that no state shall deprive any person of life, liberty, or property without due process of law. The Due Process Clause, which was adopted in 1868, is said to guarantee both procedural rights, such as basic due process of the law, and also more substantive rights, such as those holding that a person's life, liberty, and property cannot be subject to state regulation without an appropriate compelling state interest to justify the limitation. In addition, the Court held that only personal rights that can be deemed fundamental, or "implicit in the concept of ordered liberty," should be properly included in the constitutional guarantee of personal privacy.

In prior cases, the right to privacy had been extended to activities relating to marriage, procreation, contraception, family relationships, child rearing, and education. In *Roe v. Wade*, the Supreme Court explained that the concept of privacy guaranteed in the Constitution was broad enough to encompass a woman's decision concerning whether to terminate her pregnancy. Specifically, the Court found that state criminal abortion statutes like those promulgated in Texas, which exempted from criminality only a lifesaving procedure on behalf of the mother without regard to pregnancy stage and without recognition of the other interests involved, violated the due process clause of the Fourteenth Amendment. Since the right to choose whether to terminate a pregnancy was part of the liberty guaranteed in the amendment, the right could not be limited or restricted without due process of law.

Although the *Roe* Court did not explain the value of a right to privacy, the opinion goes into some detail concerning the consequences of statutes that criminalize abortion. The detriment that the state would impose upon the pregnant woman by denying this choice altogether was apparent to the Court, and the decision cites the specific and direct harm of denying this right. This discussion is important to the decision in *Roe* because it holds that all factors—medical, psychological, economic, and otherwise—were to be weighed by the woman privately or with her physician during consultation, and not based on broad state interests.

An important element in the decision that a woman's right to choose whether to terminate her pregnancy is part of a fundamental right of privacy based on **constitutional protections** was the Court's holding that the unborn do not possess the rights of a person guaranteed in the U.S. Constitution, and particularly those rights guaranteed in the Fourteenth Amendment's Due Process Clause. The *Roe* Court surveyed a broad sweep of previous laws and decisions that had been reluctant to endorse any theory that life begins before birth. Most legal rights, including those relating to inheritance or other devolution of property, have generally been contingent on being born. Similarly, in the case at issue, the fundamental guarantee to privacy takes supremacy over life not yet realized. This part of the opinion, and precisely when life begins, remains central to debates today concerning a whole range of privacy issues.

With the centrality of privacy guaranteed in the Fourteenth Amendment determined, the second question the Court answered was whether the woman's right is absolute such that she is entitled to terminate her pregnancy at whatever time, in whatever way, and for whatever reason she alone chooses. On this point, the Court diverged from "Jane Roe" and held that a right of privacy must also acknowledge that some state regulation in areas protected by that right is appropriate. While the state may generally regulate activities through legislation and other enactments, when a fundamental constitutional right is at issue, only regulation that is necessary to a compelling state interest will be upheld. On this issue, the Court held that the privacy right involved in whether to terminate a pregnancy cannot be said to be absolute and must be subject to some limitations. For example, the state may properly assert an interest in safeguarding health, in maintaining medical standards, and in protecting potential life; and in the case at issue, there will be some point in a pregnancy where these respective interests will become sufficiently compelling to sustain regulation of some factors that govern the abortion decision.

With respect to state limitations governing the right to privacy in the termination of a pregnancy, following *Roe*, any such regulations must be supported by a compelling state interest and must also be narrowly drawn to express only the legitimate state interests at stake in regulating the activity. The Court found two state interests that could properly limit the woman's right to choose whether to terminate her pregnancy. Protecting life and potential health could not justify broad limitations without more narrowly tailored state interests. According to the *Roe* Court, it is reasonable and appropriate for a state to determine at some point that another interest—for example, the health of the mother or that of the potential human life—becomes significantly involved and thus appropriately limiting of the woman's right to privacy.

Rejecting the state of Texas' argument that life begins at conception, the Court in deciding *Roe* blazed a difficult trail in its discussion of when exactly the state should have an important and legitimate interest in preserving and protecting the health of the pregnant woman and still another important and legitimate interest in protecting the potentiality of human life. Following the opinion, these interests were to be understood as separate and distinct, each growing in substantiality as the woman approaches term, and each with the possibility of becoming "compelling."

Drawing on modern medical advances and with the expressed need to limit the circumstances under which the state could invade the woman's constitutional right to privacy, the Supreme Court drew several lines limiting the right to choose. The issue of whether and when the state may regulate this right was laid out by the *Roe* Court in three parts. The first holding was that during the first trimester, the abortion decision and its effectuation must be left to the medical judgment of the pregnant woman's attending physician. Second, following the first trimester, the state may regulate the abortion procedure in ways that are reasonably related to maternal health. Finally, for the stage of pregnancy subsequent to viability, the state may regulate or proscribe the procedure except where it is necessary for the preservation of the life or health of the mother. Importantly, the *Roe* opinion holds that an exception should always exist in the law to protect the mother's life, no matter what stage the pregnancy is in upon termination.

The Supreme Court's "trimester" analysis has never been overturned, but in cases following *Roe*, the Court seemed to use a reasonableness test to determine the validity of laws regulating abortion. The requirement that state regulation be both compelling and narrowly tailored remains the law today. Whether laws regulating a woman's right to choose are a reasonable means to protect health or are simply enacted to deter abortion procedures, and when the state's interest is compelling enough to regulate a fundamental constitutional right, are lines of inquiry that have been central to the Court's wrestling with one of the most controversial issues in the United States.

See also: Eisenstadt v. Baird, 405 U.S. 438 (1972); *Gender*; *Griswold v. Connecticut*, 381 U.S. 479 (1965); *Privacy, definition of*; *Reproductive rights*; *Webster v. Reproductive Health Services*, 492 U.S. 490 (1989); *Women and privacy*

Suggested Reading: Allen, Anita, and Erin Mack. "How Privacy Got Its Gender," *Northern Illinois University Law Review* 10 (1990): 441–454; Allen, Anita, and Erin Mack. *Uneasy Access: Privacy for Women in a Free Society*. Totowa, NJ: Rowman & Littlefield, 1988; Garrow, David J. *Liberty and Sexuality: The Right to*

Privacy and the Making of Roe v. Wade. Berkeley: University of California Press, 1998; Hull, N.E.H., and Peter Charles Hoffer. *Roe v. Wade: The Abortion Rights Controversy in American History (Landmark Law Cases and American Society)*. Lawrence: University of Kansas Press, 2001; Kersch, Ken I. *Constructing Civil Liberties: Discontinuities in the Development of American Constitutional Law*. Cambridge, UK: Cambridge University Press, 2004; O'Connor, Karen. *No Neutral Ground? Abortion Politics in an Age of Absolutes*. Boulder, CO: Westview Press, 1996.

Ann Marie Neir

S



Safe Harbor Principles

The Safe Harbor Principles are a voluntary, self-regulatory, privacy policy framework for U.S. companies wishing to do business with European Union (EU) member states. The principles were developed by the International Trade Administration of the U.S. Department of Commerce in response to the **European Data Protection Directive**, which prohibits the flow of personal data from European Union member countries to non-EU countries whose data protection measures are not considered adequate by European Union standards. After two years of negotiations with EU data protection officials, the EU approved the Safe Harbor Principles, while retaining the right to review its decision at a later time. After receiving this approval, the principles were implemented in November 2000.

The Safe Harbor Principles are important to the negotiation of privacy policy in a global arena because they reflect different approaches to privacy protection between the European Union and the United States. While the EU provides comprehensive data protection legislation for all sectors of society in all member states, the United States has traditionally preferred a mixed approach of limited state and federal legislation in isolated cases (e.g., the privacy of video rental records) and industry self-regulation. Of the stakeholders in personal information, the United States has thus emphasized the rights of businesses to use personal data for business purposes and to treat such data as subject to market principles.

Designed to bridge these differences in approach to privacy protection, the Safe Harbor Principles protect U.S. companies from interruptions in their data flow from European Union member countries and from prosecution under European data protection laws. For this purpose, U.S. businesses wishing to join the Safe Harbor program self-certify and publicly state their compliance with the Safe Harbor Principles annually on the U.S. Department of Commerce website. As a result, these companies can be subject to prosecution under U.S. laws addressing fraud and misrepresentation such as the False Statements Act (18 U.S.C. 1001) if they fail to follow the principles. According to the U.S. Department of Commerce, participation in the Safe Harbor Principles provides companies with a number of benefits, including recognition by all 25 EU member countries as adhering to adequate privacy practices and the increased likelihood that complaints about



privacy violations against the companies by EU citizens will be heard in the United States and will be subject to U.S. law.

For this purpose, the Safe Harbor Principles provide a compromise between EU standards for data protection and the U.S. tradition of mixed approaches and business self-regulation. Most notably, under the Safe Harbor framework, businesses must obtain “**opt-in**” consent from individuals only if sensitive personal data are to be passed on to a third party or to be used for purposes not specified during data collection. The principles also allow for less stringent requirements for individuals to access their personal data to make corrections or deletions, specifying that such access does not need to be provided if the costs of providing access are “disproportionate to the risks to the individual’s privacy.” Finally, the Safe Harbor Principles do not require data protection authorities as recourse mechanisms; rather, they allow for a range of mechanisms, including voluntary, corporate-sponsored privacy seal programs such as TRUSTe or BBOnline.

Nevertheless, the Safe Harbor Principles have received a mix response. Businesses have sometimes found them onerous and confusing, and have also noted the cost of maintaining two different sets of privacy practices—one for their European and one for their North American operations. Accordingly, participation has been limited. As of October 2005, only 811 businesses were listed on the Safe Harbor compliance list, a number of whom had not renewed participation and were listed as “not current.” In contrast, **privacy advocacy organizations** in the United States, such as Privacy International, the Electronic Privacy Information Center (EPIC), and the **American Civil Liberties Union (ACLU)** have argued that the principles do not go far enough to protect the privacy of European citizens and that the principles, by design, fail to offer any privacy protection to U.S. citizens.

See also: **Privacy notices**

Suggested Reading: Bennett, Colin J., and Raab, Charles D. “The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response,” *Information Society* 13 (1997): 245-263; Regan, Pricilla. “Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows,” *Journal of Social Issues* 59 (2003): 263-282; Starke-Meyerring, D., D. Burk, and L. Gurak. “Americans and Internet Privacy: A *Safe Harbor* of Their Own?” In P. E. N. Howard and S. Jones (eds.). *Society Online: The Internet in Context*, pp. 275-293. Thousand Oaks, CA: Sage, 2004; Swire, Peter, and Robert E. Litan. *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*. Washington, DC: Brookings Institution, 1998; U.S. Department of Commerce. *Safe Harbor*. www.export.gov/safeharbor. Online, October 2005.

Doreen Starke-Meyerring

Same-sex marriage. *See* **Family**

Schmerber v. California, 384 U.S. 757 (1966)

On November 12, 1964, Mr. Schmerber and a friend were drinking in a tavern and bowling alley until around midnight. After deciding to go **home**, they both got into Schmerber’s **automobile**. While driving under the influence of alcohol, Schmerber lost control of his vehicle, skidded across the road, and collided with a

tree. When the ambulance arrived, the paramedics determined that both individuals had sustained injuries and needed to be taken to the hospital for treatment. It was apparent that Schmerber had been drinking and was intoxicated at the time of the accident; consequently, he was arrested and later convicted of violating the California Vehicle Code. In order to secure the evidence needed to prove intoxication, a police officer had told the overseeing physician to draw blood and conduct a chemical analysis. Subsequently, the test revealed that Schmerber's blood alcohol level was over the legal limit, and the results of this test were later admitted into evidence.

Schmerber objected to evidence revealed by the **blood test** analysis on the grounds that it violated his right to silence under the Fifth Amendment. He also argued that his right to security from an unreasonable search and seizure of his blood was a violation of his enumerated Fourth Amendment **privilege**. The trial court did not believe that drawing blood was a violation of Schmerber's constitutionally protected rights. When the Supreme Court of the United States heard the constitutional arguments under a writ of certiorari, they affirmed the trial court's decision that there was no constitutional violation.

The Fifth Amendment argument was dismissed because the nature of the evidence under its protection must be testimonial or communicative. The privilege to remain silent when asked to provide information pertaining to one's guilt is enumerated in the Fifth Amendment and is extended only to information that can be withheld or provided by the choice of that individual. According to the court, a blood test is no different than a **fingerprint** or a photograph. The physical nature of a blood test is not communicated and therefore does not have an ability to remain silent when used to determine the guilt of an individual. There is no testimony that is offered by a blood sample beyond the actual physical characteristics of the blood. The Court reasoned its action to dismiss this argument through a long history of jurisprudence that had defined the specific limitations of the Fifth Amendment.

The Fourth Amendment argument was likewise rejected by the Supreme Court on the grounds that the amendment's purpose is not to protect against all intrusions, but rather to protect against ones that were unjustifiable or unreasonable under the circumstances in which they were conducted. In a perfect world, the legality of a search or seizure of a person or property often hinges upon a court-issued warrant. However, it is necessary to permit officers of the law to arrest or seize an individual when it is apparent that the individual is either guilty of or is planning to commit an illegal act. This probable cause of action justifies society's intrusion into the Fourth Amendment protections, and, therefore, a court-issued warrant is not always required.

In this case, the officer had probable cause to conduct a lawful arrest without a warrant because of the combination of the apparent smell of alcohol on Schmerber as well as his visibly bloodshot and glassy eyes. Even though the arrest was made lawfully, the search and seizure of the respondent's blood still became an issue under the Fourth Amendment. Typically, after the lawful arrest of a suspect, the courts have held that it is lawful to search and seize any evidence reasonably corresponding to the accused person at the time of arrest. The issue in this case is whether the circumstances surrounding Schmerber's arrest had created a reasonable



environment within the legal realm of the Fourth Amendment that would justify drawing his blood without his consent. Simply because the arrest was lawful did not necessarily substantiate the intrusion of a needle into Schmerber's body for the purpose of drawing his blood.

In order to preserve the human dignity and privacy that the Fourth Amendment seeks to protect, the Court imposed two caveats that must be met before a warrantless search and seizure can be justifiable following the arrest of a suspect. First, the Court required that there must be clear indication that the intrusion will produce the evidence it seeks to obtain. Second, there must be exigent circumstances to justify the need to act in order to preserve any evidence that will obviously be lost if the search or seizure is delayed because of the requirement to get a warrant. Since it is a fact that blood contains any alcohol that has been consumed by a person and that the alcohol will dissipate over time, the officer was justified in his action to obtain the evidence that was certainly in the respondent's blood. It was certain that the blood analysis would produce the evidence, and that, if the officer had waited for a warrant, the evidence would likely have been metabolized out of Schmerber's system. The Court decided that both caveats were satisfied, justifying the deviation from the Fourth Amendment.

The invasiveness of the intrusion into Schmerber's body was weighed against the specific circumstances surrounding the search and seizure of his blood. The taking of his blood was done by a physician in a hospital setting and was performed according to standard medical practices. Since the blood was obtained in a customary manner, the Court decided that it had been reasonable. Because there was an exigent need to retrieve the respondent's blood combined with the certainty of procuring the evidence, the Court decided that the invasiveness of the blood test had been acceptable, as long as the manner in which the blood had been taken was in accordance with standard medical practice. Ultimately, the Court ruled that Schmerber's Fourth Amendment argument was not applicable to the circumstances surrounding this case.

The dissenting opinion of the Court disagreed with the majority's decision regarding the Fifth Amendment. The minority suggested that the blood test was of a testimonial or communicative nature and therefore should be protected under the Fifth Amendment. Previous cases had held that it was unlawful for the government to compel individuals to produce papers or documents that could incriminate them. The dissent illustrated the disparity between the protection of an individual's incriminating documents and the refusal to protect an individual from the puncturing of his skin to retrieve his blood in order to secure the same incriminating evidence. The dissent argued this was a strange hierarchy of importance, where the protection of a person's blood was less valued than were documents and papers.

The decision in *Schmerber v. California* was made under the specific circumstances that surrounded the search and seizure of Schmerber's blood. The Court was clear to point out that it continued to balance human integrity and dignity protected under the Fourth and Fifth Amendments against the need for society to obtain evidence and preserve the lawfulness and protection of its citizens. The decision in this specific case was reached only on the presented facts and did not create a precedent that would be applicable to all intrusions into a person's body.

See also: **Automobile search**; *Carroll v. United States*, 267 U.S. 132 (1925); **Constitutional protections**; **Search warrant**; **Sobriety checkpoint**; *South Dakota v. Opperman*, 428 U.S. 364 (1976); *Terry v. Ohio*, 392 U.S. 1 (1968)

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul: West, 1999; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hubbard, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

Sean M. Peek

Search warrant

A search warrant is a written order issued by a judge (or other officer of a court) authorizing a law enforcement or other government official to search a person or location, usually for illegal material (contraband) or for evidence of a crime. Warrants may include special criteria, such as “no knock” provisions that allow police to execute them without warning. Since searches are likely to be intrusive and disruptive of privacy, the requirement of a search warrant based on probable cause is one of the most important constitutional safeguards of privacy. Indeed, the Fourth Amendment’s guarantee against unreasonable searches and seizures was one of the provisions of the Bill of Rights that Supreme Court Justice **William O. Douglas** cited in his majority opinion in *Griswold v. Connecticut*, 381 U.S. 479 (1965), the decision that made explicit a constitutional right to privacy.

Over the years, the meaning of the warrant clause and other aspects of the Fourth Amendment have been the subject of much interpretation by the courts. These interpretations have dealt with questions such as what constitutes a search, what defines an unreasonable search, when searches may be conducted without warrants, and what satisfies the requirement of probable cause. Interpretation has usually taken place in a context characterized by tension between impatience with those portions of the law that constrain the police and a concern that the privacy of the individual be respected

The **constitutional protection** of privacy against unreasonable searches and seizures is grounded in the Fourth Amendment, which states that “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated,” and further provides that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized.” The requirement of specificity was especially important to the framers of the Bill of Rights. The events leading up to the American Revolution had seen widespread objections to British use of open-ended “general warrants,” both in America where customs officials used them (in the form of writs of assistance) to search for unnamed smuggled goods and in Britain where the government had used general



warrants as a means of suppressing opposition journalist John Wilkes. Opposition to such searches had frequently cited the common law right to be left alone, another of the legal bases of the right to privacy.

As with the rest of the Bill of Rights, the Fourth Amendment was originally held to protect Americans from abuse by the federal government but not to apply to the states. During the course of the twentieth century, most of the protections of the Bill of Rights were gradually “incorporated” into the Fourteenth Amendment’s Due Process Clause and held to apply also to the states. The Supreme Court held the “core” of the Fourth Amendment to be applicable to the states in *Wolf v. Colorado* (1948).

A search originally was taken to mean a physical intrusion by an agent of government, particularly into lodging. The definition expanded dramatically during the last third of the twentieth century. In the case of *Katz v. United States*, 389 U.S. 347 (1967), the Supreme Court reversed earlier precedents to include **wiretapping** of conversations within the meaning of search, opening up a field in which the courts would struggle to stay abreast of proliferating eavesdropping technology. Also considered searches are physical intrusions into the person, such as those necessary to obtain blood, breath, and **DNA** samples. However, the action of a police officer who performs a “**stop and frisk**” or a “pat down” of a person deemed to act in a suspicious manner is not considered an unreasonable search within the meaning of the Fourth Amendment.

One of the difficulties of interpreting the Fourth Amendment is that it has something of split personality. The first part emphasizes the need to protect the individual from “unreasonable” searches and seizures, while the second stresses that warrants should be issued only for probable cause. Some might argue that any search without a warrant issued for probable cause is unreasonable, but the amendment does not actually say this, and the courts have not interpreted it in this fashion. The courts have long recognized that some types of searches do not require warrants. The crucial question thus becomes whether those searches are reasonable. Typically, twentieth-century courts relied on the standard of probable cause (see below) to define reasonableness. Since the 1980s, though, the standard has increasingly become whether an action violates the standard of a “**reasonable expectation of privacy**.” The phrase first occurred in the aforementioned *Katz* case in 1967, where it was used to extend the definition of search to include electronic eavesdropping. It has since been used more often to narrow the definition of what might be judged an unreasonable search. In effect, the Court evaluates the balance between the weight of the government’s interest in the search and the extent to which the individual’s privacy interest is affected. In general, the courts tend to look most critically at actions that intrude on the interior of people’s **homes**, while showing greater tolerance for government activities elsewhere. A farmer’s fields or even a fenced backyard, for example, have been held not to be entitled to an expectation of privacy.

There is a long list of exceptions to the rule that searches should be based on warrants. In daily practice, many more searches are conducted without warrants than with them. These warrantless searches include (but are not necessarily limited to) a search incident to an arrest, a search of a motor vehicle, an inventory of the personal effects of persons who are arrested, a search of abandoned property

(including garbage), evidence in plain view, consensual searches, searches at borders and airports, and searches in “exigent circumstances” (i.e., those where the delay in obtaining a warrant would make it impossible to conduct the search). All of these exceptions have been defined and elaborated by judicial interpretation.

Probable cause is important both to the issuing of search warrants and to the justifications for warrantless searches. Since many warrants are based on information supplied by police informants, establishing the credibility of the source of that information became a major concern. During the 1960s, there was a decided tendency toward tightening requirements for warrants and invoking rules of evidence similar to those used in trials. Police requesting warrants were expected to make clear both the circumstances in which the informant was likely to have gained useful information and the officer’s reasons for believing it was true. In 1983, however, the Supreme Court decided in *Illinois v. Gates* that a more holistic judgment of the totality of circumstances was more practical. The Court has also held that “administrative searches” in workplaces and schools do not have to have warrants or meet the probable cause standard.

The tension between the needs of government and privacy concerns continues to provoke controversies. One of the most controversial aspects of the prohibition of unreasonable searches and seizures has been the exclusionary rule. This excludes from consideration evidence gathered in violation of the Fourth Amendment. The exclusionary rule was first adopted by the federal courts in *Weeks v. United States*, **232 U.S. 383 (1914)**, and subsequently applied to the states in *Mapp v. Ohio* (1961). The Court, however, has allowed some use of unconstitutionally obtained evidence, for example in challenging the testimony of witnesses.

While most controversies in this area of privacy have grown out of the criminal justice system, an additional site of controversy has been the area of national security, particularly in the area of **electronic surveillance**. For example, in the aftermath of the September 11, 2001, attacks, President George W. Bush ordered intercepts of telephone conversations of American citizens with foreigners suspected of terrorist connections on his authority as commander in chief. Not only did this involve the **National Security Agency** in spying on American citizens, but it also bypassed the procedure set up by the **Foreign Intelligence Surveillance Act of 1978 (FISA)** for seeking warrants for national security wiretaps. In such cases, the government argued that national security requirements outweighed the privacy interests of individuals.

Search warrants are only intended to protect individual privacy from abuse by public authorities. Employers, for example, have broad powers to search in the workplace or to make **drug testing** a condition of employment.

See also: **Automobile search; Blood testing; Plain view doctrine; Silver platter doctrine; Strip search**

Suggested Reading: Barton, Robert R. *Texas Search and Seizure*. Huntington, NY: Juris, 2002; Black, Henry C. *Black’s Law Dictionary*, 7th ed. St. Paul: West, 1999; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*,



3rd ed., 5 vols. St. Paul: West, 1996; Oyez. *U.S. Supreme Court Multimedia*. www.oyez.org. Online, December 2006.

William C. Lowe

Secrecy

Secrecy is the concealment of that which, if known, would bring negative consequences; privacy is the concealment of that which is positive or intimate. Secrecy has negative connotations, irrespective of the content of the secret, while privacy, irrespective of what goes on in private, has positive ones. In American society, secrecy is the provenance of at least six social groups: the government, the workplace, the stigmatized, the institutionalized, the young and old, and those engaged in secret societies or rituals.

Governmental secrecy has been studied extensively by social scientists. Although openness has supposedly been one of the hallmarks of American democracy in its judicial, executive, and legislative branches, there have always been areas where that light has been darkened: secret “security risk” lists kept by the **Federal Bureau of Investigation (FBI)**, secret **surveillance** of right- or left-wing threats to national security or safety, secret meetings of local government agencies, and the like. Although nations may be wary of internal secrecy, governments justify it to varying degrees and under various circumstances. Governmental secrecy is also commonplace in international relations, including wars, where nations attempt to keep secret from other nations everything from the details of satellite surveillance to the number of spies on foreign territory. International secrecy, especially in wartime, is generally more palatable to populations than is internal secrecy.

Both public- and private-sector workplaces may have secrets, either from outsiders or from their own employees. Industrial secrets protect new pharmaceutical discoveries or **automobile** designs from **industrial espionage** or “poaching” by other companies. The protection of workplace secrets is one reason given by employers for overt or secret surveillance of their employees; other reasons include social control related to inventory protection or how time is spent on the job. Workplace surveillance is controversial in itself, but even more so when the surveillance is secret; indeed, the workplace, like government, epitomizes the ethical and legal conflicts over the right to individual privacy vs. collective or corporate protection.

Secrecy has historically been the provenance of the stigmatized or misbehaving: gays and lesbians, former mental patients, ex-convicts, philandering spouses. The stigmatized conceal identities, past histories, or present activities for many reasons: the homosexual or philanderer may fear losing his or her spouse and children, the ex-convict may fear being denied employment, the drug user may fear losing his or her job. **Private investigators** may be hired to penetrate these individual secrecies.

Both individual and more collective types of secrecy are found among institutionalized populations such as mental patients and **prisoners**, who are not entitled to many resources or to much, if any, privacy. Inmates or patients are forbidden to engage in certain activities—for example, sexual acts with others—and are deprived of certain goods—generally alcohol, cigarettes, and drugs. They are also limited in the amount of legitimate goods and services they may acquire, from food to haircuts.

Therefore, forbidden and limited activities, goods, and services are engaged in and acquired in secret, often resulting in entire secret institutional economies.

In American society, the old and the young are protected by law from behaviors and relationships that are permitted to adults but forbidden to the young or old. These behaviors are culturally defined either as valuable or as tolerable for adults—marital sexuality, responsible drinking, access to pornography—but as negative and damaging when engaged in by minors or the elderly. Sexual activity is forbidden by law to unmarried minors, and sometimes to the institutionalized elderly. Preadolescents and adolescents are not permitted to partake of certain adult privileges and substances, from having sex to driving automobiles to cigarette smoking, and when they do these things, they do them in secret. Age-related and institution-related secrecy are similar in that concealment is resorted to when the privacies and privileges permitted to adults are denied or taken away.

As noted above, what is common to these several arenas of secrecy is the concealment of what the audience—not necessarily the secret-bearer—might define as negative: a secret government decision, the stigma of homosexuality, staff finding cigarettes in a mental patient's room, or a parent finding out that a teenager has been drinking. Those who keep secrets, however, may or may not share the audience's negative view of what they are concealing: the secretly gay person who scorns heterosexuals, the teenager who likes to drink, the mental patient who wants a cigarette. It is only in the arena of governmental secrecy that both the audience and the secret-keepers are likely to view what is concealed as negative: for example, the threat of a potential terrorist attack on Los Angeles.

Another arena of secrecy in America includes the secret society, code, and/or ritual. Both children and adults may engage in temporary or more enduring secret activities or societies, from secret handshakes or phrases to rituals and spaces, to which only the secret-sharers have access. The existence of secret societies may be known about, but not their membership or location; indeed, efforts may be made by governments or religious bodies threatened by secret societies to acquire lists of members in order to stamp them out. Since secrecy itself is negative (although, again, the content of the secret will likely seem positive to its keepers), secret codes, rituals, or societies are generally suspect. The secrecy inherent in secret societies intersects with privacy at the point where the individual's privacy is violated in order to determine whether she or he is a member of such a society. Such investigative tactics have been used by governments and religious bodies in cases of illicit or illegal secret societies.

As the above examples illustrate, secrecy and privacy have a number of similarities and differences. Like secrecy, privacy is a concealment strategy, but what is being concealed may be positive (to the self and to audience) rather than negative. Marital sexual relations, a handwritten diary, or the hard drive of a **computer**, are among the positive cultural values protected by privacy. Conversely, illegal sexual activities, a handwritten diary detailing armed robberies, or pedophilic pornography must be concealed as secrets.

Privacy also conceals necessary intimacies; paramount among these are the washing and toileting functions of **private parts**. The necessary intimacy of private parts and their handling is common to all members of society, thus there is no

secrecy equivalent as such. In the arena of necessary intimacies, privacy is enforced by laws forbidding public defecation, urination, or sexual intercourse.

The relationship between privacy and secrecy is structured by economic and power relations: the more privacy entitlement or acquisition that a social group, **family**, or individual has, the less secrecy seeking is necessary. The more upper-class and wealthy the family or (non-stigmatized) individual is, the more that family or person can acquire spaces and times for privacy; conversely, there is little privacy for lower-class individuals crowded into tenements. The staff and administrators of an institution can escape from its walls into their private **homes**, whereas the inmates cannot.

This is not to say that social status, wealth, and power always confer privacy and obviate the need for secrecy. Although the right to privacy is clustered at the top of a hierarchy and the resort to privacy resides at the bottom, this relationship may be inverted in some contexts. A politician who smokes may keep this fact secret from his constituency, while the politician's office janitor would not bother. The janitor is likely to be able to protect his or her privacy from the media more effectively than can the politician—although the politician's household may afford more privacy.

Secrecy and privacy are also social definitions subject to negotiation and conflict, in political/religious, family, and institutional contexts. For example, the Church of Scientology, variously regarded as a religion, cult, sect, or illegal organization, has been accused by various governments of posing a danger to citizens. Attempts to subpoena "secret" documents have been met with attempts to redefine such documents as private "religious, sacred knowledge" protected by the First Amendment. Power relations in a given society determine the success or failure of these tactics.

Power relations are also relevant to the conflict of definitions in families and in institutions. In a family vignette, a teenage girl is talking on the phone and her mother comes into the room. The teen turns her head down and starts mumbling into the phone. Her mother says, "Oh, don't be so secretive," and the teen responds, "I just want some privacy!" This scene could be repeated in other places where authorities and subordinates coexist, such as between the staff and patients in a mental hospital or between the teachers and pupils in a boarding school. What the miscreant defines as privacy and its entitlements the authority defines as secrecy and its illicit concealments.

While privacy is vulnerable to invasion, secrecy is vulnerable to revelation: privacy's invasion is by the public or the unwanted; secrecy's revelation may be by anyone. The best-kept secret is an unshared one: a person with secret homosexual desires who does not share them with anybody (and thus, of course, cannot fulfill them). The truth is, the more people who share a secret, the more the possibility of its violation.

There is secrecy and there is privacy; there is a secret but no equivalent such as "a private"—the closest our language comes to that is private parts. The term "private parts" conjures up the origins of privacy in the body, extending over the centuries to a plethora of extra-bodily rights. Privacy is essentially individual, at most dyadic. Secrecy may be individual—the unshared secret—but it is also collective. The sociological essence of the relationship between privacy and secrecy lies in this: the balance of power, rights, and responsibilities between the individual and the collective.

See also: **Manners; Open meetings laws; Privacy, definition of; Privacy and inequality; Public/private dichotomy; Public records; Workplace privacy**

Suggested Reading: Allen, Anita. *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability*. Lanham, MD: Rowman & Littlefield, 2003; Bellman, Beryl. "The Paradox of Secrecy," *Human Studies* 4 (1981): 1–24; Bok, Sissela. *Secrets: On the Ethics of Concealment and Revelation*. New York: Pantheon Books, 1983; Warren, Carol A. B., and Barbara Laslett. "Privacy and Secrecy: A Conceptual Comparison," *Journal of Social Issues* 33 (1977): 43–51.

Carol A. B. Warren

Secure Socket Layer (SSL)

Secure Socket Layer (SSL) is a handshake protocol that enables secure communication between two programs or machines. It is used primarily to secure **Internet** transmissions. SSL protects data that are in transit from eavesdroppers and other active attackers on the network. The first version of SSL was designed in 1994 by a group of engineers at Netscape Communications, and since then, the protocol has undergone several revisions and modifications, culminating in its adoption as the Transport Layer Security (TLS) standard by the Internet Engineering Task Force (IETF) in 1999.

SSL provides generic security features for the communication channel on top of Transmission Control Protocol (TCP). Therefore, any protocol that can be carried over TCP, such as HTTP (Hypertext Transfer Protocol) and FTP (File Transfer Protocol) can be secured using the SSL protocol. In order to enable secure communication, SSL provides data **confidentiality** by encrypting the data that are being transferred between two communicating machines. Encrypting the data being sent on the wire renders that data unintelligible to third-party attackers. Thus, SSL has made it safe for users to send their **credit card** numbers, passwords, and other confidential information to authorized remote servers. Another important security feature provided by SSL is server **authentication**. Server authentication makes it possible for a client machine to corroborate the identity of a remote server before it reveals or sends sensitive information such as password or credit card information to the remote server. Thus the client machine or, more specifically, the web browser acting on behalf of the client machine can be sure that the sensitive information is revealed only to intended servers. Although it is not strictly required for the server to carry out client authentication, since the password or the credit card information provides inherent proof of the client's identity to the server, the SSL protocol does support client authentication as well. Authentication in SSL is carried out using a certificate-based mechanism. The client machine verifies the X.509 public-key certificate of the server in order to corroborate its identity. Further, SSL also provides data integrity by making use of message authentication codes. Thus, it is possible to detect any unauthorized attempts to tamper with the data.

The SSL handshake protocol consists of two phases. The first phase involves server authentication. During this phase, the server sends its certificate in response to a client's connection request. The client generates a random master key, encrypts the master key with the server's public key, and then transmits the encrypted master key to the server. The server recovers the master key and authenticates itself to the



client using this master key. Subsequent communication is encrypted and authenticated with keys derived from this master key. In the optional second phase, the server sends a challenge to the client. Upon receiving the challenge, the client authenticates itself to the server by generating a digital signature on the challenge and returning the signed challenge along with its public-key certificate. Upon successful authentication, the server and client can communicate securely using the shared keys.

See also: **Cryptography; Password protection**

Suggested Reading: Agre, Phil, and Marc Rotenberg (eds.). *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT Press, 1998; George, Joey F. (ed.). *Computers in Society: Privacy, Ethics and the Internet*. Upper Saddle River, NJ: Pearson Prentice Hall, 2004; Gurak, Laura. *Cyberliteracy: Navigating the Internet with Awareness*. New Haven, CT: Yale University Press, 2001.

Maithili Narasimha

Sell v. United States, 539 U.S. 166 (2003)

Charles Sell, once a practicing dentist, had a long history of mental illness. In September 1982, after telling doctors that the gold he used for fillings had been contaminated by Communists, Sell was hospitalized, treated with antipsychotic medication, and subsequently discharged. In June 1984, Sell called the police to say that a leopard was outside his office boarding a bus, and he then asked the police to shoot the leopard. Sell was again hospitalized and subsequently released. On various occasions he complained that public officials were trying to kill him. In April 1997 he told law enforcement personnel that he “spoke to God last night,” and that “God told me every [Federal Bureau of Investigation (FBI)] person I kill, a soul will be saved.”

In 1997 the federal government charged Charles Sell with submitting fictitious insurance claims for payment. A federal magistrate, after ordering a psychiatric examination, found Sell “currently competent” but noted that Sell might experience “a psychotic episode” in the future. The magistrate released Sell on bail. A grand jury later produced a superseding indictment charging Sell and his wife with 56 counts of mail fraud, 6 counts of Medicaid fraud, and 1 count of money laundering.

In early 1998 the government claimed that Sell had sought to intimidate a witness. The magistrate held a bail revocation hearing. Sell’s behavior at his initial appearance was, in the judge’s words, “totally out of control,” involving “screaming and shouting,” the use of “personal insults” and “racial epithets,” and spitting “in the judge’s face.” A psychiatrist reported that Sell could not sleep because he expected the FBI to come busting through the door. The judge then revoked Sell’s bail.

In April 1998 a grand jury issued a new indictment charging Sell with attempting to murder the FBI agent who had arrested him and a former employee who planned to testify against him in the fraud case. The attempted murder and fraud cases were joined for trial. In early 1999 Sell asked the magistrate to reconsider his competence to stand trial. The magistrate sent Sell to the United States Medical Center for Federal Prisoners at Springfield, Missouri, for

examination. Subsequently the magistrate found that Sell was “mentally incompetent to stand trial.” He ordered Sell to be hospitalized for treatment at the medical center for up to four months, to determine whether there was a substantial probability the Sell would attain the capacity to allow his trial to proceed.

Two months later, medical center staff recommended that Sell take antipsychotic medication. Sell refused to do so, and the staff sought permission to administer the medication against Sell’s will. One new incident that was introduced at the next trial was that Sell had approached one of the medical center’s nurses, suggested that he was in love with her, criticized her for having nothing to do with him, and, when told that his behavior was inappropriate, added that he couldn’t help it. The medical center doctors testified that, given Sell’s prior behavior, diagnosis, and current beliefs, boundary-breaching incidents of this sort were not harmless and, when coupled with Sell’s inability or unwillingness to desist, indicated that he was a safety risk even within the institution. They even had him moved to a locked cell.

The magistrate authorized forced administration of antipsychotic drugs. In affirming that decision, the district court concluded that medication was the only viable way of rendering Sell competent to stand trial and was necessary to serve the federal government’s interest in determining his guilt or innocence on the fraud charges. The court of appeals also affirmed the earlier decisions. On the fraud charges, the appellate court found that the federal government had an essential interest in bringing Sell to trial, that the treatment was medically appropriate, and that the medical evidence indicated that Sell would be able to participate fairly in his trial.

The privacy question involved was as follows: may the federal government administer antipsychotic drugs involuntarily to a mentally ill criminal defendant in order to render that defendant competent to stand trial for a serious, but nonviolent, crimes? Justice Stephen G. Breyer delivered the opinion for the Supreme Court. The Court held that the Constitution allows the federal government to administer antipsychotic drugs, even against the defendant’s will, in limited circumstances. The Court reasoned that such conditions include if the treatment is medically appropriate, is substantially unlikely to have side effects that may undermine the trial’s fairness, and taking account of less intrusive alternatives, is necessary significantly to further important governmental trial-related interests. After determining that the district court and appeals court findings did not satisfy these conditions, the Court vacated the appellate court’s judgment. Justice Antonin Scalia, joined by Justice Clarence Thomas, dissented, arguing that the Court did not have jurisdiction to decide the case.

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black’s Law Dictionary*, 7th ed. St. Paul: West, 1999; Freckleton, Ian. “Coercing Fitness for Trial: Mandating Efficacious Pharmacotherapy: *Sell v. United States*, 539 U.S. 166 (2003); 123 S. Ct. 2174; 156 L. Ed. 2d 197 (2003),” *Psychiatry, Psychology and Law* 11 (2004): 174–179; Liokis, Michelle Garriga, and Paul B. Herbert. “Competence to Stand Trial,” *Journal of the American Academy of Psychiatry Law* 33 (2005): 554–555.

Tod J. Beavers



Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities

In the mid-1970s, this committee, chaired by Frank Church (D-ID), was organized to investigate illegal governmental spying and **surveillance** activity in the wake of the Watergate break-in by members of Richard Nixon's reelection campaign. "The Church Committee," as it became known, took public and private testimony from hundreds of people and collected huge volumes of files from the **Federal Bureau of Investigation (FBI)**, the **Central Intelligence Agency (CIA)**, the **National Security Agency**, and the **Internal Revenue Service (IRS)**, as well as many other federal agencies during testimony in 1974–1975. This information gathering culminated in 14 reports completed in 1975 and 1976, which remain the most extensive review of governmental intelligence activities to date. Recommendations from the committee for reform of intelligence activities were debated in Congress and in some cases were carried out.

The interim report documents the Church Committee's findings on United States involvement in attempts to assassinate foreign leaders, particularly Fidel Castro of Cuba, Patrice Lumumba of the Congo, and Ngo Din Diem of South Vietnam. Although the CIA did not succeed in assassinating these foreign leaders, the agency provided arms to insurgents and spent millions of dollars in public propaganda, attempted to influence democratic elections (as in the case of Allende in Chile), and funded opposition political campaigns. Based on the recommendations in this report, President Gerald Ford issued an executive order (11905) to ban U.S.-sanctioned assassinations of foreign leaders, which was subsequently replaced in 1981 by President Reagan's Executive Order 12333.

The remaining reports include seven volumes of public hearing records and exhibits, and six books that document the committee's writings on the various topics investigated. In regard to privacy, Book II, titled *Intelligence Activities and the Rights of Americans*, details the abuses of domestic intelligence agencies. The conclusion states, "Domestic intelligence activity has threatened and undermined the constitutional rights of Americans to free speech, association and privacy. It has done so primarily because the constitutional system for checking abuse of power has not been applied."

The committee found that the government had collected huge amounts of information about the lives of private citizens, including political beliefs and personal associations, through the use of illegal or uncontrolled intrusive techniques, including theft and **electronic surveillance**. Included in these activities were a CIA program to open mail to or from selected American citizens that led to 1.5 million names being stored in the Agency's **computer** database; efforts by intelligence units within the FBI that created files on over one million Americans; burglaries carried out by intelligence agencies in the **homes** and offices of suspected "subversives;" and, actions by intelligence agency agents to infiltrate religious, media, and academic organizations.

The report charged that the checks and balances that protected privacy had been compromised by three main departures from the constitutional plan for controlling the abuse of power: excessive executive power, excessive **secrecy**, and avoidance of the rule of law. The document produced three recommendations to protect privacy in the wake of these abuses of power. First, all governmental action that directly

infringes on First Amendment rights must be prohibited. Second, any governmental action that has an indirect impact upon the rights of speech and assembly is permissible only if it is undertaken to fulfill a compelling governmental need, and the government must use the least restrictive means to meet that need. Third, procedural safeguards should be adopted along with substantive restraints, such as that of obtaining a judicial warrant from a neutral magistrate once probable cause has been determined.

Suggested Reading: Assassination Archive and Research Center. *Assassination Transcripts of the Church Committee*, 1992. www.aarclibrary.org. Online, December 2005; U.S. Senate. *Hearings before the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*. Washington, DC: U.S. Government Printing Office, 1976.

Shelley L. Koch

Sense-enhancing technologies

The term “sense-enhancing technologies” refers to all types of equipment or machines that increase the perceptual ability of the user. In practical terms, this means a device that allows the user to see or hear things that could not be detected by the use of the normal human eyes or ears: for example, infrared goggles, parabolic microphones, or **thermal sensors**. This entry will survey the different types of sense-enhancing technologies and provide an overview of the law governing their use.

Sense-enhancing technologies have been around for centuries. The first and most basic example of a sense-enhancing technology is artificial illumination, such as a torch or, in more modern usage, a flashlight. Another example is a visual magnifier, such as a telescope or binoculars, which have been used for centuries by scientists, law enforcement officers, and lay people in order to see things that would otherwise be undetectable by the naked eye. Hearing-enhancing devices can be traced back almost 200 years to devices like the stethoscope, used originally by doctors but also adapted for use by individuals conducting **surveillance** through walls.

As the twentieth century progressed, however, sense-enhancing devices became more powerful and more potentially intrusive in two ways. First, the potential magnitude of amplification increased dramatically: modern-day binoculars can magnify an image between 30 and 80 times its actual size, while an individual can use a parabolic microphone to listen in on a conversations over 400 feet away. Second, and more significantly, new devices have been created that can detect inputs that are beyond our five senses, such as **x-ray devices**, infrared light, and radiation. Sometimes termed “sense-replacing devices” rather than sense-enhancing devices, these surveillance tools have become ubiquitous in our society: metal detectors (which detect disturbances in a magnetic field) are a standard fixture in airports or any other “secure” location, while night-vision goggles and thermal imagers (which detect infrared light waves) are readily available on the open market and frequently used by law enforcement and military personnel. Other forms of sense-replacing devices, such as x-ray machines, are less widespread but commonplace in specific fields such as medicine. And still others have been used almost exclusively by law enforcement to great effect. Radar guns have been used by police for over



50 years to detect the speed of passing cars; today there are over 125,000 radar guns in this country, and an average motorist can expect to be monitored by a radar gun over 1000 times in his or her lifetime. Similarly, law enforcement officers use thousands of trained dogs throughout the country to detect the smell of narcotics or explosives; although technically these animals are not a type of “technology,” they are tools used to detect otherwise imperceptible sensory inputs during a search of an individual or an **automobile**. Finally, law enforcement officials are developing newer sense-enhancing (or sense-replacing) technology: handheld gun detectors are able to provide police officers with the shape and location of metal objects concealed on a person, while ion scans can be used on tables or the interior of automobiles to determine whether narcotics or explosives have recently been in contact with the surface.

The proliferation and increased effectiveness of sense-enhancing technologies have given rise to significant legal questions about whether and how to regulate them. As noted above, sense-enhancing technologies come in many different forms and can be used in many different ways, from everyday uses of commonplace items (such as pointing a flashlight down a dark alley) to specialized uses of more sophisticated devices (such as calculating the speed of cars with radar guns) to surveillance that intrudes quite dramatically into an individual’s privacy (such as detecting what a person is carrying under his or her clothes, or monitoring activities might be occurring inside the house). Legal regulation of these devices falls under two categories: first, the restrictions placed on law enforcement officials using these devices to investigate crime; and second, the restrictions placed on citizens using the devices for their own private purposes.

In the context of law enforcement, the primary question is a constitutional one: under what conditions (if any) is a government agent required to procure a **search warrant** before using sense-enhancing technology to conduct surveillance? Under the Fourth Amendment to the Constitution, a law enforcement officer is generally required to obtain a search warrant before conducting an intrusive search; in order to obtain such a warrant, the officer must prove to a magistrate that there is probable cause to believe that a suspect is engaged in illegal activity. If the magistrate agrees and issues the warrant, the officer can search the suspect, or the suspect’s **home**, automobile, or office, in almost any manner the officer wishes.

In the early stages of an investigation, a law enforcement officer might not yet have probable cause and therefore would not be able to obtain a warrant. Thus, many types of surveillance (with or without sense-enhancing technology) must be conducted without warrants, and courts strictly regulate what types of warrantless surveillance are permitted. For example, police officers can stake out a house and observe who enters and leaves, but they cannot enter the house without consent and search for contraband. Emerging technologies create a new spin on the old legal question: is a law enforcement officer allowed to conduct warrantless surveillance using sense-enhancing technology, and if so, what types of technology are permissible?

The Supreme Court addressed this question in the landmark case of *Katz v. United States*, 389 U.S. 347 (1967). In *Katz* law enforcement officers placed an electronic listening device on the outside of a public phone booth and eavesdropped

on the defendant's conversation. The defendant claimed that this surveillance method violated his Fourth Amendment rights, and the Supreme Court agreed. In the words of Justice Harlan, the electronic listening device violated the defendant's "**reasonable expectation of privacy**," and therefore law enforcement officers were not allowed to use such devices unless they first obtained a search warrant from a court.

The reasonable expectation of privacy test became the standard for evaluating the legality of sense-enhancing devices for the next 30 years. In evaluating whether or not a certain new technology violated this standard, courts would consider not only the type of technology at issue, but also the way in which it was used. For example, the Supreme Court held that using a homing device to track the movements of suspected criminals was legal if it merely reported the suspects' travels over public highways, but using the same device to track their movements inside a private home violated the Fourth Amendment. Similarly, using a flashlight to examine a public area, a private open field, or even the interior of a car is permissible because such actions do not violate an individual's reasonable expectation of privacy.

In 2001 the Supreme Court clarified the reasonable expectation of privacy test in the case of *United States v. Kyllo*, 533 U.S. 27 (2001). In *Kyllo*, government agents suspected the defendant was using high-intensity heat lamps to grow marijuana in his home. To confirm their suspicion, they conducted a scan of the house using a thermal imager, a device that detects infrared radiation. The heat patterns detected by the imager provided further evidence that the defendant was using heat lamps, and the agents used that information to acquire a search warrant. As in *Katz*, the Supreme Court held that the warrantless use of this sense-enhancing technology violated the Fourth Amendment, since the suspect had a reasonable expectation of privacy regarding the contents of his home. In so doing, however, the Court defined two different contexts in which the government's use of a sense-enhancing technology would not violate an individual's reasonable expectation of privacy and therefore could be permitted.

First, if the specific use of the technology only detected information that could otherwise have been obtained without physical intrusion into a private area, the surveillance was permissible, regardless of the type of technology used. In other words, if a law enforcement officer used a high-powered parabolic microphone to eavesdrop on a conversation that occurred in a public restaurant, the surveillance would be permissible. The information that the officer received from listening in on the conversation could have been acquired by other means without intruding into a private area (for example, law enforcement officers could place an undercover officer at the table next to the suspects to eavesdrop the old-fashioned way). Likewise, law enforcement officers would be permitted to use extremely high-powered binoculars to observe a suspected drug transaction in a park or on a street corner, since the suspects would be conducting their business in a public place and the activity could have been observed by any individual who was walking nearby. In other words, if the use of the technology merely allows law enforcement officers to more easily or more safely observe or detect things that they could have detected through more conventional means, the surveillance does not violate the Fourth Amendment. To put it another way, if the suspects are in a public place, they do not have a reasonable expectation of privacy regarding anything they say or do, even if law enforcement officers use the newest technology to spy on them.



Even if the surveillance does result in information that could not possibly have been obtained without physical intrusion into a private area, the government agents' actions might still be legal. This is because of the second scenario set out by the Court: if the law enforcement officers are using a technology which is in "general public use," they need not seek a warrant before conducting the surveillance. The term "general public use" was not defined in the opinion, and it will surely be the source of future litigation, but the general outlines were clear enough: devices such as flashlights and binoculars that are routinely used by the general public are in general public use, while newer, rarer technologies (such as gun detectors, which can see through a person's clothing) are not. For example, assume law enforcement officers used a flashlight to look down a private driveway at night and saw two individuals conducting a drug transaction. Without the sense-enhancing technology of the flashlight, the officers could never have perceived the illegal activity unless they had entered the private property. But because flashlights are in general public use, the individuals in the driveway did not have a reasonable expectation of privacy regarding their actions. On the other hand, if the officers used a sophisticated, portable x-ray machine to see through the walls of a house, or a parabolic microphone to eavesdrop on the conversations inside a house, they would be using technology that is not in general public use to detect information that they could not possibly have acquired without a physical intrusion into the private house—and therefore that surveillance would be barred by the Fourth Amendment. This is exactly what happened in the *Kyllo* case itself: the Court decided that the thermal imager was not in general public use, and so it could not be used to gather information about what was going on inside the defendant's private residence. Although some justices pointed out that the thermal imager used in *Kyllo* was widely available on the open market, with over 10,000 units already sold, a majority of the court held that such devices were not in fact in general public use—and probably because they were not yet in such widespread use that their ubiquity would change people's reasonable expectation of privacy. If in the future, if everyone owned a thermal imager and they were routinely used by individuals (as flashlights and binoculars are today), then law enforcement officers could begin to use them with impunity, since in such a world the suspects they would be watching would have no objective reason to believe that the heat emanating from their homes or bodies is private information.

Compared to the well-developed (and well-litigated) standards governing the use of sense-enhancing devices by law enforcement officials, the laws regulating civilian use of those devices are relatively scarce and undefined. Every state has a common law right (that is, a right developed in the courts, not by statute) that protects individuals' privacy, but most of the torts that are connected with that right involve the defendant giving publicity to the private facts in some way. The only applicable restriction in most jurisdictions is the common law tort of intrusion, which generally bars "invasive conduct which is highly offensive to a reasonable person." Thus, a civilian who uses sense-enhancing technology in a way that is invasive and highly offensive would be liable for monetary damages in a civil suit to the person upon whom he or she was spying. At least one state has enacted a statute to deal with the specific problem of sense-enhancing technology: California bars any attempt to observe or detect "personal or familial" activities using a "visual or auditory enhanc-

ing device” (Cal. Civ. Code §1708.8(b) (2001)). As with the common law restriction, violation of this law merely subjects the defendant to civil, not criminal liability. The standard used by the California legislature for civilian misuse of these technologies closely mirrors the standard used by the Supreme Court for law enforcement officials: the use of the technology has to violate a reasonable expectation of privacy, and the information gathered must be of the type that could not otherwise have been gathered without physical intrusion onto private property.

See also: **Constitutional protections; Electronic surveillance**

Suggested Reading: Amsterdam, Anthony G. “Perspectives on the Fourth Amendment,” *Minnesota Law Review* 58 (1974): 349–447; Harris, David A. “Superman’s X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology,” *Temple Law Review* 69 (1996): 29–32; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000; Slobogin, Christopher. “Technology-Assisted Physical Surveillance: The American Bar Association’s Tentative Draft Standards,” *Harvard Journal of Law and Technology* 10 (1997): 390–398; Steinberg, David E. “Making Sense of Sense-Enhanced Searches,” *Minnesota Law Review* 74 (1990): 563–629.

Ric Simmons

Sex offender registries

Sex offender registries (SORs) are databases of information about persons convicted of sex offenses who have completed their sentences or received probations and now reside in the community. SORs are primarily intended to help law enforcement agencies monitor the whereabouts of known sex offenders, thereby preventing crime as well as providing a pool of suspects for police when a sex crime is reported. Depending on the jurisdiction, access to SORs may be restricted to criminal justice officials or made available, via formal community notification systems (CNSs), to community organizations and the general public to assist in the managing of risk to children and other vulnerable persons. SORS and CNSs are predicated on the notion that **sex offenders**, more than other kinds of offenders, have an enduring disposition to offend and should, therefore, have stringent restrictions placed on their rights to privacy and freedom of movement. SORS and CNSs reflect intense public concern about the risk of serious harm posed by sex offenders, particularly to the most vulnerable persons in society, such as women and children. These concerns also create strong pressure on politicians of all stripes to respond accordingly to public demands for action.

In 1990, the state of Washington passed its Community Protection Act in response to strong media and public reaction to a repeat child sex offender’s brutal rape and mutilation of a seven-year-old boy. The SOR component of this legislation requires all convicted sex offenders to register with the police upon release from prison; the CNS component requires dissemination of information about registered sex offenders to community organizations and the general public. Who specifically receives information depends on a three-tier system of assessing the degree of risk (high, moderate, and low) posed by individual offenders.



Other states soon followed Washington's lead. Some states adopted Washington's systems of tiers of risk; other states treated all sex offenders as a single, high-risk class. Of note is that legislation creating SORs and CNSs took on the names of those child victims that advocates used to mobilize public reaction and governmental response. New Jersey's Megan's Law was triggered by the rape and murder of a 7-year-old girl named Megan Kanka. Indiana's Zachary's Law, named after a 10-year-old boy murdered by a child molester, established the first SOR that could be accessed by the public via the **Internet**. Currently over 30 states permit similar online access to SORs.

In 1994, President Bill Clinton sponsored the Jacob Wetterling Act, which required all states to set up SORs or have their criminal justice funding cut by 10 percent. In 1996, this was followed by the federal Megan's Law, which required all states to create CNSs, and the Pam Lychner Act, which created a national SOR, linking state databases to enable tracking of sex offenders across state lines.

Other countries followed the United States' lead in establishing SORs but declined to link them to CNSs. In 1997, the United Kingdom passed a civil statute creating a SOR to help police solve sex crimes. In 2000, the Canadian province of Ontario enacted Christopher's Law. This was followed by federal legislation setting up a national registry (NSOR) in 2004. In Canada's NSOR, strict rules with regard to access and **disclosure** currently require law enforcement personnel to meet the thresholds established under Section 16 of the Sex Offender Information Registration Act in order to access the registry and disclose information in it.

British and Canadian police and politicians resisted community notification legislation, arguing that community notification would impede the usefulness of registration as a law enforcement tool because the loss of liberty and privacy and the stigma resulting from community notification would reduce offender compliance with registration requirements. Indeed, unlike some American states, which have compliance rates of less than 50 percent, compliance with registration requirements has recently been estimated to be over 95 percent in the United Kingdom. Officials representing Ontario's registry and Canada's NSOR, while not providing published evidence, make similar claims.

While the specific characteristics of SORs and CNSs vary by jurisdiction, most share common features. Offenders convicted of identified sexual offenses, once outside of prison, must initially provide and regularly update information about themselves with local police. When formally authorized, this information can legitimately be disseminated to community organizations and the general public. The information provided can include the following: **home** and employment contact information; identifying characteristics such as tattoos and scars; the types of offenses that triggered the need to register; personal information such as age, weight, and place of birth; vehicle make and license number; and recent photographs.

The length of time a released sex offender is required to register varies by jurisdiction, offense type, and offender type. Offenders convicted of multiple counts of child molestation may be required to register for life; those convicted of other offenses, depending on their seriousness, may be required to register for shorter, fixed periods of time. An example of how duration of registration relates to the offense can be found in the Canadian NSOR. It requires offenders to register for 10

years, 20 years, or for life, depending on whether the type of offense the offender was convicted for has been classified as less serious, serious, or very serious.

The decision as to whether a sex offender will be subject to registration also depends on the jurisdiction. In the United States, after receiving written notification, offenders who have completed their sentences or are on parole or probation are required to register with local police. In Canada, the decision is made not at the time of release, but rather by the trial judge immediately after the imposition of sentence. In most circumstances, the prosecutor makes a formal request to the court for inclusion in the sex offender registry, and the trial judge then ultimately determines whether the offender will be subject to the registry and for how long the offender will have to register upon release.

Opponents of SORs and CNSs point to the myriad pragmatic and civil libertarian difficulties they pose. Opponents argue that sex offenders who have paid their debt to society should not have additional measures imposed upon them after sentence completion, should not have to share personal information, and should not be subject to any increased police scrutiny that an otherwise “normal” offender would avoid.

Opponents further argue that, even if one accepts that police should have access to sex offender information, the public should not have such access. When any interested person in a jurisdiction with Internet access to its SOR can access a sex offender’s personal information by home **computer**, constitutionally protected privacy rights have been seriously eroded. A tertiary concern stems from a slippery-slope critique. If society chooses to invade the privacy rights of a particular offender group, what will stop society from invading the privacy of other offender groups? This critique contends that when the rights of one minority group are infringed upon, the rights of all members of society are threatened.

There have been few legal challenges specific to offender privacy and sex offender registries. Most courts have either deferred making a decision in anticipation of future legislation or had their decisions rendered moot by the introduction of newer legislation. The following cases are notable exceptions.

In New Jersey, in *Doe v. Poritz*, despite a strong dissent, the court held that sex offender registry and community notification does not violate offenders’ privacy rights. In *A. v. New Jersey*, the court limited the scope of the *Poritz* decision. It held that complete public access to offender information is unconstitutional, and that the offender’s home address must be removed from the community notification website.

In Ontario, in *R. v. Burke*, the court held that the sex offender registry was a grossly disproportionate violation of privacy for this specific offender. Conversely, in *R. v. Ayoob*, the court did not find that there was a grossly disproportionate violation of that specific offender’s privacy rights. In both cases, the decision ultimately turned on the criminal record of the offender and the seriousness of the sex offense violation. In December 2005, the Ontario Superior Court of Justice ruled that Ontario’s SOR was constitutional.

The balance between individual privacy and public protection is most difficult to achieve in the case of offenders considered to be dangerous and morally unclean. On the one hand, those who support SORs and CNSs argue that knowing one is being watched deters one from re-offending. On the other hand, critics of



SORs and CNSs are concerned that members of a specifically targeted offender group who have served their time are being denied basic privacy rights that other released offenders would have been granted. Such critics ask how a democratic society can maintain its higher moral authority when one segment of the population has its privacy rights violated, and how the invasion of constitutionally protected civil liberties can be justified when evidence to support its deterrent effect is lacking.

See also: **Constitutional protections; Public health and safety**

Suggested Reading: Kabat, Alan. "Scarlet Letter Sex Offender Databases and Community Notification: Sacrificing Personal Privacy for a Symbol's Sake," *American Criminal Law Review* 35 (1998): 333; Petrunik, Michael. "Managing Unacceptable Risk: Sex Offenders, Community Response, and Social Policy in the United States and Canada," *International Journal of Offender Therapy and Comparative Criminology* 46 (2002): 483–511.

Miahel Cole
Michael Petrunik

Sex offenders

How sex offenses are defined has varied over time and across cultures. Even today definitions vary across jurisdictions in the United States. The public response to these offenses and to the people who commit them, however, has been more consistent and driven largely by fear, outrage, and a demand for protection. The contemporary political and legal treatment of sex offenders mirrors public opinion, and the result has been to make sex offenders subject to additional limitations on their privacy even after they have served their sentences. This entry will discuss current developments in the criminal justice system in the treatment of sex offenders that expand control over sex offenders in terms of legal processing, treatment options, and integration back into society.

Some states have passed laws that allow for the civil commitment of sex offenders after they have served their criminal sentences. To some legal scholars, these laws are viewed as a resurrection of the sexually violent predator (SVP) legislation enacted during the mid 1900s. The supporting logic in favor of this trend is that some sex offenders tend to have high recidivism rates and are therefore likely to re-offend. In these cases the statutory standards favor public safety over individual rights. Although the need for continued treatment is ostensibly the goal of this legislation, it tends to emphasize an incapacitative objective over rehabilitation. The result is that many sex offenders may be kept under some form of state control indefinitely for the purpose of preventing crimes they "might" commit.

One treatment option that has been adopted by states for use with sex offenders is chemical castration. This treatment involves injection of a synthetic hormone (Depo-Provera), which lowers the blood serum testosterone levels in males. Taken on a regular basis, this hormone reduces sexual impulses, the frequency of erotic fantasy, erections, and ejaculations. Chemical castration has been in use in the treatment of sex offenders since 1944, but at that time it was administered with the informed consent of the individual. Today, chemical castration statutes are different. In 1997 California became the first state to enact a law mandating chemical

castration for twice-convicted sex offenders whose victims were under the age of 13. Chemical injections begin prior to release on parole and are continued while the offender is under community supervision. If the offender refuses, parole is denied.

Fundamental rights of privacy and procreation are at issue when mandatory Depo-Provera injections are imposed. Privacy concerns arise because the individual's right to control his own person and the right to refuse treatment are compromised. The right to privacy and bodily autonomy also extends to the right of an individual to make procreative decisions. The effects of Depo-Provera that result in a reduction of sperm production are believed to be temporary and reversible when injections stop. The sex offender in temporary treatment of this kind still has the ability to engage in sex and procreate. For sex offenders who are sentenced to lifetime injections, however, the right to procreate may be denied permanently. Bolstering this argument is the lack of understanding about the long-term side effects of Depo-Provera on sexual performance and potency. There are cases in the California court system that oppose the use of mandatory organic treatment for offenders. Groups such as the **American Civil Liberties Union (ACLU)** are challenging chemical castration by comparing it to mandatory **sterilization**, which was declared unconstitutional in *Skinner vs. Oklahoma* (1942).

In 1994 the abduction of an 11-year-old boy in Minnesota prompted Congress to pass a law mandating that all 50 states create **sex offender registries** with local law enforcement agencies so that an offender's current residence can be identified (Jacob Wetterling Crime Against Children and Sexually Violent Offender Registration Act, 1994). After another tragic episode involving the murder of Megan Kanka in New Jersey by a previously convicted child molester, Megan's Law was added to the Wetterling Law in 1996. According to this law, states are mandated to have procedures in place to inform the public about sex offenders who live in their communities. The rationale for community notification is that public safety, especially the protection of children, will be enhanced if the community has knowledge about the presence of convicted sex offenders residing in the neighborhood. Even juvenile sex offenders, whose privacy is usually well guarded by the criminal justice community, can be subject to sex offender registration.

In a review of notification laws in all 50 states, research has found that notification methods commonly include press releases, flyers, door-to-door contact, neighborhood meetings, and the use of **Internet** websites. About half of the states assign offenders to one of three risk levels and notify the public differentially according to the risk an offender poses to the community. Other states employ broad community notification, publicizing the locations of all sex offenders without regard for risk assessment. Legal scholars have argued that using the Internet to provide public notification of sex offenders when a dangerousness hearing has not occurred is a privacy violation, but the courts thus far have largely rejected this claim.

In cases involving sex offenders, much of the current legislation tends to favor the need for public safety over the privacy standard the supports the right to be left alone. Another privacy standard affecting this group involves the right to control information about oneself. The challenge here has focused on the release of information about offenders and how that information might be used.

The type of information collected on sex offenders varies, but at a minimum includes the offender's name, address, and law enforcement identification number. In some states this information can also include a photograph, **fingerprints**, handwriting samples, employment information, residence history, vehicle registration numbers, HIV status, and **DNA** samples. Considering the potential for its misuse, the ease with which some of this personal information can be accessed by the public is a major concern relating to sex offenders' privacy.

Several states' sex offender registries are made available to the public through toll-free and pay phone lines, CD-ROMS, or the Internet so as to meet community notification mandates set forth in Megan's Law, but private citizens who take it upon themselves to notify communities have been known to obtain lists of registered sex offenders and post them on the Internet without the endorsement of law enforcement. Understanding the potential for the misuse of sex offenders' personal information, some states have taken added measures to ensure its proper use. For example, the Sex Offender Registry Board of the Commonwealth of Massachusetts requires users of its Internet registry to acknowledge and accept an agreement regarding the appropriate use of information before accessing details of level 3 (high-risk) sex offenders. Specifically, the registry viewer must agree not to use the information to commit a crime, discriminate against, or harass an offender. The penalty for breaching the agreement involves a fine, incarceration, or a combination of both. Once the registry is accessed, users can obtain a sex offender's full name, age, race, sex, height, weight, hair color, eye color, exact address, the number and types of sex offenses that he or she has been convicted of, the date of conviction(s), a color photograph of the offender, and information pertinent to whether the offender lives or works in the area.

Technology has played a dual role in contemporary issues surrounding sex offending. While the Internet has opened up a whole new hunting ground for sexual predators and created new potential for non-forcible sex offenses against children, it has also played an instrumental role in disseminating offender information to law enforcement agents and communities under the guiding principle of public safety. As of February 2001, 29 states had publicly accessible Internet sites that contained searchable information on individual sex offenders.

In addition to the creation of sex offender registries, federal legislation also permits DNA testing and the collection of samples from sex offenders for identification purposes. The DNA Analysis Backlog Elimination Act of 2000 grants authority to the attorney general to require sex offenders convicted in federal courts to provide DNA samples for inclusion in the **Federal Bureau of Investigation (FBI)**'s Combined DNA Index System (CODIS). Twenty-two states report that they collect and maintain DNA samples as a required part of sex offender registration, while 19 additional states report limited or no collection of DNA samples. This information is often collected along with other identifying information such as fingerprints and handwriting samples, which can then be used either to link a sex offender to future crimes or to crimes that have taken place in the past.

Other laws such as buffer-zone laws restrict where a sex offender can live and are used in some form by as many as 14 states. Most of these laws prohibit sex offenders from living within a specified radius around schools and day-care centers, but some buffer-zone laws are so strict that they also prohibit sex offenders

from taking up residence near parks, playgrounds, trails, swimming pools, libraries, churches, bus stops, and any other place where children usually gather. The radii within which sex offenders are prohibited from living vary but can range anywhere from 1000 to 2500 feet. In some cases this means that entire cities and towns are off limits to sex offenders, and that sex offenders who already live within restricted areas can be evicted and forced out of their **homes**.

The long-term effects of these trends on the treatment of sex offenders and the protection of the public have not yet fully understood, and many issues remain to be examined. The limited research that does exist suggests that some offenders have experienced loss of jobs, homes, property damage, and harassment. One of positive aspects of notification laws according to offenders is an increased commitment to prevent re-offending.

The logistic demands of implementing these laws are also at issue, which should factor into the continued balance between public safety and individual freedom. An overreliance on these laws may not afford the protection hoped for by the public. For example, findings from several studies demonstrate that buffer-zone laws fail to cause reductions in sex offense recidivism. Moreover, the underlying premise for buffer-zone laws appears to be unfounded because sex offenders who live near places where children usually gather, such as schools or parks, are no more likely to re-offend than are sex offenders who do not live near children.

Suggested Reading: Center for Sex Offender Management. *Sex Offender Registration: Policy Overview and Comprehensive Practices*. www.csom.org/pubs/sexreg.html. Online, November 1999; Commonwealth of Massachusetts Sex Offender Registry Board. *Sex Offender Registry Board User Acknowledgement and Acceptance*. ma-sorb.gis.net/intro.htm. Online, November 1999; Farkas, M. A., and A. Stichman. "Sex Offender Laws: Can Treatment, Punishment, Incapacitation, and Public Safety Be Reconciled?" *Criminal Justice Review* 27 (2002): 256–283; Levenson, J. S., and L. P. Cotter. "The Effect of Megan's Law on Sex Offender Reintegration," *Journal of Contemporary Criminal Justice* 21 (2005): 49–66; National Victim Assistance Academy. *Sexual Assault*. www.ojp.usdoj.gov/ovc/assist/nvaa2002/chapter10sup.html. Online, November 1999; Terry, K. J. *Sexual Offenses and Offenders: Theory, Practice and Policy*. Belmont, CA: Thomson/Wadsworth, 2006; U.S. Department of Justice. Bureau of Justice Statistics. *Summary of State Sex Offender Registries, 2001*. (2002). www.ojp.usdoj.gov/bjs/pub/pdf/ssor01.pdf. Online, November, 1999; Wilson, F. T. "Out of Sight, Out of Mind: An Analysis of *Kansas v. Crane* and the Fine Line between Civil and Criminal Sanctions," *Prison Journal* 84 (2005): 379–394.

April Pattavina
Tiana Marie Platz

Sexual harassment

Title VII of the Civil Rights Act of 1964 prohibits discrimination in employment on the basis of sex, as well as on the basis of the other protected grounds of race, religion, and national origin. Although sexual harassment is not expressly prohibited by the statute, the courts, including the United States Supreme Court, have concluded that harassing conduct that is motivated by sex constitutes discrimination with respect to a term or condition of employment. Similarly, harassment on

the basis of race, religion, or national origin may also constitute discrimination in connection with a term or condition of employment.

Traditionally, the courts have recognized two forms of sexual harassment. The first form, generally referred to as “quid pro quo” sexual harassment, involves a situation in which an employment opportunity or an employment detriment is conditioned on an individual’s receptiveness to, toleration of, or rejection of sexual conduct. Under language more recently adopted by the United States Supreme Court, this form of sexual harassment is defined as harassment that results in a “tangible employment action,” such as a hiring, firing, promotion, demotion, or other similar action. The second type of sexual harassment is referred to as “hostile environment” sexual harassment; it involves sexual conduct that does not result in a tangible employment action but that creates an offensive, abusive, or hostile working environment.

Under the rules adopted by the Equal Employment Opportunity Commission, the administrative agency charged with enforcement of Title VII, and applied by the courts, in order for harassment to be actionable, it must meet certain requirements. For both “quid pro quo” and “hostile environment” sexual harassment, the harassing conduct must be unwelcome and must have been undertaken because of or motivated by sex. In addition, in order for “hostile environment” sexual harassment to be actionable, it must be sufficiently severe or pervasive to alter one’s working conditions or create a hostile or abusive working environment.

Employers face potential liability for sexually harassing conduct that occurs among their employees and in the context of the workplace. With respect to harassing conduct engaged in by a supervisory employee toward his or her subordinate employees, employers are automatically liable when that harassing conduct results in a tangible employment action, such as a hiring, firing, demotion, or other similar action. When no such tangible employment action results from the harassing conduct, employers still face liability for the sexually harassing conduct engaged in by supervisors unless the employer can show both that the employer acted reasonably to prevent sexual harassment and to remedy sexually harassing conduct when it occurred, and that the employee who was subject to the sexually harassing conduct did not act reasonably in either reporting the conduct or in otherwise acting to avoid harm caused by that conduct. With respect to sexually harassing conduct that occurs between co-workers or by third parties, the employer can face liability for that conduct if the employer knew or had reason to know of the conduct and did not act to prevent or remedy that conduct. Under Title VII of the Civil Rights Act of 1964, individuals who actually engage in the harassment do not face individual liability, although it is possible that they might face liability for the sexually harassing conduct under state law claims against the individual harassers.

The privacy implications of sexual harassment are extensive, both for the individual accused of harassment and for the target of harassing conduct. Perhaps the element of sexual harassment law that threatens the most extensive potential invasion of privacy for targets of harassment is the requirement that harassment has to be shown to be “unwelcome” in order to be actionable. In order for a target of harassment to demonstrate that the harassment was unwelcome, he or she has to show that the conduct was not invited or otherwise incited, as well as being required to show that the conduct was offensive to him or her. Accordingly, courts

have admitted evidence of past sexual conduct on the part of the target, as well as evidence about the target's dress, speech, or other conduct in the workplace to determine whether the conduct might have been invited or encouraged. Courts have also entertained evidence about whether the target of harassment has had sexual relationships with other individuals in the workplace, presumably on the basis that the existence of such relationships might be relevant to the question of whether sexual conduct by the harasser was welcomed. In some cases, courts have even admitted evidence as to the target's conduct outside of the workplace context to determine whether the conduct in question might have been welcomed or—more extremely—whether the target of harassment was the “type” of person who, because of his or her conduct, could be deemed to have welcomed sexual conduct generally.

There have been efforts to limit the invasion of privacy that can be caused by inquiries into the “welcomeness” of sexually harassing conduct. Formerly, “rape shield” statutes sought to prevent inquiries into the past sexual conduct of rape victims in an effort to show “sexual predisposition.” The Federal Rules of Evidence, in Rule 412, have been amended to also apply with respect to civil actions involving sexual conduct, including actions claiming sexual harassment. That rule seeks to reverse the presumption that evidence of a target's past sexual conduct is admissible in such actions. Instead, the rule is that evidence of the target's past sexual conduct or “sexual predisposition” is inadmissible unless its evidentiary value “substantially outweighs” the danger of harm that that evidence poses to the victim or other parties. Accordingly, under this rule, employers seeking to introduce evidence of an employee's past sexual conduct will have to show not only the relevance of the conduct to the existence of actionable discrimination but also a special need on the part of the employer with respect to that evidence.

Privacy may also be affected by inquiries into the past sexual conduct of individuals accused of harassment. Those inquiries might be made for a number of reasons or purposes. For example, because sexual harassment may be less likely to occur in front of witnesses than other forms of discriminatory conduct, and therefore whether the conduct in fact occurred may be at issue, employees bringing sexual harassment claims may well feel compelled to produce other victims of the individual accused of harassment, thereby arguing for the relevance of certain forms of past sexual conduct by the alleged harasser.

In addition, to the extent that a victim of harassment may be claiming that he or she was disadvantaged because of a failure to engage in sexual conduct with the harasser, while other individuals who were willing to engage in such conduct received employment benefits, it may be necessary to inquire into the voluntariness of those other sexual relationships. In particular, because the law may recognize a cause of action for sexual harassment by individuals disadvantaged by the existence of other coerced sexual relationships in the workplace—because it suggests that the employment opportunity really was conditioned on willingness to submit to unwanted sexual conduct—but does not recognize a cause of action for individuals disadvantaged by the preferential treatment based on existence of other voluntary sexual relationships among their supervisors and co-workers, the voluntariness of sexual relationships to which the employee herself or himself is not a party may become relevant to the validity of the employee's sexual harassment claim. This possibility affects the privacy interests of the alleged harasser and other employees in the workplace.

The requirement that sexually harassing conduct be undertaken “because of sex” also has implications for the privacy interests of both the victims of harassment and the individuals accused of harassment, particularly with respect to sexual harassment that occurs between members of the same sex, but also with respect to instances of opposite-sex harassment. Although the United States Supreme Court has recognized that harassment between members of the same sex can constitute discrimination because of sex in violation of Title VII of the Civil Rights Act of 1964, the Court made clear that such harassment is actionable only if it can be proven to have occurred because of sex; the sexual nature of the conduct has not been considered sufficient to establish the “because of sex” requirement. The Court suggested that one way to create an inference that sexually harassing conduct between members of the same sex is based on sex is to show “credible evidence that the harasser was homosexual.” Accordingly, to the extent that the employee claiming to have been harassed seeks to establish that the same-sex harassment to which he or she was exposed was based on sexual desire and therefore because of sex, the sexual orientation of the alleged harasser may become legally relevant. While it is not entirely clear what might constitute “credible evidence” of sexual orientation, one might imagine that past same-sex sexual conduct on the part of the alleged harasser might be sought to be introduced in order to establish that requirement of actionable sexual harassment.

Information about the sexual orientation of the victim of harassment may also become legally relevant in connection with the need to establish that the sexually harassing conduct has occurred because of sex. While harassment that is deemed to be motivated by sex can be actionable under Title VII, harassment that is based on the victim’s sexual orientation generally is not, because the courts have consistently interpreted Title VII’s protections against sex discrimination not to extend to discrimination based on sexual orientation. Accordingly, if employers or individuals accused of harassment are able to establish that the targets of harassment were selected for harassment because they were gay men or lesbians, not because they were men or women, the harassment of those individuals would not violate the law’s prohibition of sex discrimination, as that law is traditionally interpreted and applied. In this way, the sexual orientation of the victims of harassment—or at least the perceived sexual orientation of those victims—becomes legally relevant to a claim of sexual harassment.

The requirement for actionable “hostile environmental” sexual harassment that the conduct is sufficiently severe or pervasive to create an offensive or abusive working environment can also affect the privacy interests of employees targeted for harassment. The courts have made clear that there is both a subjective and an objective component of this requirement. That is, not only must the employee show that he or she subjectively perceived the environment to be abusive, but the employee must also show that the challenged conduct caused the environment to be objectively hostile or abusive. This requirement raises the possibility that the employer, defending against a hostile environment claim, will attempt to show that the individual targeted for harassment was not actually offended by the conduct. This showing would likely take the form of attempting to demonstrate other behavior on the part of the victim of harassment that would show a lack of offense or toleration of sexually offensive conduct, such as evi-

dence suggesting that the employee herself or himself engaged in sexually offensive conduct or otherwise was the “type of person” who would not be offended by sexual conduct in the workplace. Even the requirement that the harassing conduct be objectively offensive poses privacy implications, in that an employer may well attempt to show that, even though the employee was subjectively offended by the conduct, his or her reaction was not reasonable; for example, perhaps because some experience in his or her past—childhood or adult **sexual violence**, assault, or some mental condition—caused the victim to be unusually and atypically sensitive to sexual conduct in the workplace.

Even the standards applied by the courts for imposing liability on employers for the sexually harassing conduct of supervisory and nonsupervisory employees may have implications for the privacy interests of individuals accused of harassment and the individuals targeted for harassment. Although employers face automatic liability for sexual harassment engaged in by supervisory employees when that conduct results in a tangible employment action, employers do have the opportunity to avoid liability for supervisory sexual harassment when no such tangible employment action occurred. Accordingly, employers seeking to avoid liability on the grounds that the target of harassment unreasonably failed to report the conduct or otherwise unreasonably failed to avoid harm caused by the conduct may well be tempted to seek to explore aspects of the employee’s past conduct or past experiences with the harasser in order to establish the unreasonableness of the target’s response to that conduct. For example, while the relative youth or sexual inexperience of a victim of harassment might be viewed as justification for a delay in reporting harassing conduct, the employer might well attempt to prove the opposite in order to argue that such an employee targeted by sexual harassment should have immediately recognized the nature and gravity of the harassing conduct and therefore reported the conduct without delay.

Of course, even the requirement that individuals who have been sexually harassed report the sexual conduct to which they have been subjected to the appropriate authorities affects the privacy interests of the individuals victimized by sexual harassment. The sexually harassing conduct that forms the basis of complaints of sexual harassment is likely to consist of sexual advances and demands for sexual conduct, sexual touching, sexually degrading comments and inquiries into the person’s sexual practices, and even sexual assaults and rape. Even individuals who have resisted such conduct or who have been subjected to forcible sexual conduct are likely to be embarrassed about the fact that the conduct has occurred and may think—perhaps with some justification—that they will not be believed or will be blamed for the conduct. Individuals who have felt compelled to submit or to tolerate sexually harassing conduct may well believe they bear some responsibility for the conduct to which they have been subjected, or at least may believe that others will think that they are at fault in some way. Accordingly, many victims of sexual harassment may well be reluctant to disclose the conduct to which they have been subjected, even to persons close to them, such as **family** members and close friends. Requiring that they report such conduct to the proper authorities, such as supervisors and human resource personnel, can be particularly difficult to do and intrusive of privacy interests, particularly if the employer has not set up a mechanism by which those reports can be made in a secure and safe manner.



Some tension between the laws covering sexual harassment and the privacy interests of employees is inevitable. An exclusive focus on the need to prevent sexually harassing conduct may give too little weight to the privacy interests of employees, while too much focus on privacy may prove insufficient to protect the victims of sexual harassment for the damaging aspects of that activity.

See also: **Gender; Privacy, definition of; Privacy and inequality; Women and privacy**

Suggested Reading: Hébert, L. Camille. "The Disparate Impact of Sexual Harassment: Does Motive Matter?" *University of Kansas Law Review* 53 (2005): 341–395; Hébert, L. Camille. "Sexual Harassment and Discrimination 'Because of . . . Sex': Have We Come Full Circle?" *Ohio Northern University Law Review (symposium issue)* 27 (2001): 439–484; Lindeman, Barbara, and David D. Kadue. *Sexual Harassment in Employment Law*. Washington, DC: Bureau of National Affairs, 1992 and 1999 cumulative supplement; MacKinnon, Catherine A. *Sexual Harassment of Working Women*. New Haven, CT: Yale University Press, 1979; Mink, Gwendolyn. *Hostile Environment: The Political Betrayal of Sexually Harassed Women*. Ithaca, NY: Cornell University Press, 2000.

L. Camille Hébert

Sexual violence

Sexual violence describes a variety of nonconsensual, offensive conduct involving the use of genitals or other **private parts** such as breasts and buttocks. Rape is a form of sexual violence and is generally defined as the nonconsensual sexual penetration by force or threat of force. Penetration includes vaginal, oral, and anal, and does not require proof of full intrusion into the body. For example, mere contact with the labia is sufficient in most states to prove vaginal penetration. Penetration can involve the perpetrator as the one receiving or causing the penetration. In some states, the element of force has been eliminated, and rape can be proved simply by establishing penetration and the absence of consent.

Laws against sexual violence typically provide for the harshest sanctions when the conduct involves penetration into or by the victim's body. Early laws against sexual violence evolved from the common law idea that a sexual offense was a crime against a man's property. This is because women and children were defined in law as men's property rather than as individuals with their own rights. As women gained political status, the law evolved to recognize sexual violence as a crime against the autonomous self and bodily integrity of the victim. Despite these gains and although in theory sexual violence law is designed to promote personal autonomy, virtually every state defines rape as the forcible sexual penetration of another without consent. Critics argue that by requiring proof of force in addition to nonconsensual actions, autonomy is not adequately preserved, and that if the goal is to protect the integrity of free will, sexual harm without consent, irrespective of force, should define the crime.

Although sexual violence is a crime even when it occurs between spouses, until the 1990s, at least some states had a so-called marital exception, such that sexual violence perpetrated by a man against his wife could not be prosecuted. No state retains an explicit marital rape exception today. However, in some states, rape of a wife by her husband is harder to prove and/or carries less punishment than if the

same crime happened to a stranger. Proof of nonconsent is required in all states in order for a healthy adult victim to establish that an unlawful act occurred, but consent is irrelevant for certain victims, such as those under a certain age. In most states, a child cannot lawfully consent to sexual penetration until age 16, although they may lawfully consent to nonpenetrating sexual contact at a slightly younger age. In some states, the age of consent changes based on the age of the person with whom the minor has sexual contact. For example, a 15-year-old may be prohibited from consenting to sexual contact with an adult, but may lawfully consent to the same sexual contact with another 15-year-old individual.

In many states, irrespective of age, victims cannot lawfully consent if they are disabled, heavily intoxicated, or otherwise incapable of making a knowing, intelligent, and voluntary decision about sexual conduct. Likewise, in many states, people cannot lawfully consent to sexual contact in certain trust relationships, such as teacher/student and doctor/patient. Most sexual violence occurs in private, and the majority of such violence occurs between people known to each other. Thus, privacy theory and privacy laws often inhibit the ability of law enforcement and other public officials to monitor, intervene, and redress sexual violence.

Sexual violence can be redressed under civil or criminal law. If it involves an individual in a vulnerable class, it might be redressed by a state agency, such as a department of mental health. When a child is victimized, social service agencies might become involved and could remove the child from a home, either temporarily or permanently, irrespective of whether a criminal prosecution ensues. Certain persons with reasonable cause to believe a child has been or is being sexually abused are obligated to report abuse to government officials responsible for providing protective services to children. Failure to report is a crime in most states when the person with such knowledge is in a “caretaking” position, such as that of a teacher, day-care provider, or doctor.

When a civil claim is filed to redress sexual violence, the remedy for the victim is the recovery of money damages. Sexual violence may also fall under the definition of **sexual harassment** and/or civil rights laws. Title VII and Title IX are the popular titles of federal laws that prohibit sex discrimination, including sexual harassment and sexual assault, in the workplace and in school respectively. Legal actions filed under Title IX and Title VII allow for equitable remedies in addition to money damages, such as court orders requiring a school to change its policies and procedures. When sexual violence is redressed in civil law, the victim is a formal party to the case and is represented by his or her own personal attorney. The victim can choose whether to file or withdraw a civil claim, and the actions of the victim may bear on liability during a determination of fault. For example, a victim might be found 20 percent responsible for an assault if she sues her landlord for negligently allowing a rapist to break in and assault her, and the evidence also shows that the victim, by her own negligence, contributed to her own risk of harm.

When sexual violence is redressed through criminal law, the victim is not a formal party to the case, and the prosecution does not represent the victim. The victim is a witness for the government, and there is no assessment of comparative fault between the victim and the accused. Criminal law theory is only concerned with holding the offender accountable. When a crime of sexual violence is



prosecuted in criminal court, the state and/or defense may issue subpoenas to compel the testimony of the victim and/or to compel the production of materials and things related to the crime. Likewise, a judge may issue a court order for the same purposes.

Although a subpoena in a civil case can seek broad discovery of “relevant evidence” and information that “may lead to the discovery of relevant evidence,” in a criminal case, subpoena power is strictly limited. The prosecution has authority to send subpoenas to private persons for trial, for grand jury investigations to uncover relevant evidence, and for other legitimate needs during evidentiary hearings. The accused has constitutional authority to send subpoenas to private persons only for specifically identified evidence needed for use in the trial. The accused in a criminal case has no constitutional authority to send subpoenas to the victim or to any private person for the purpose of conducting “discovery.” The accused has “discovery rights” only against the opponent, which is the state.

In civil and criminal cases, if a procedurally invalid subpoena is issued, such as when a defense attorney sends a subpoena seeking “discovery” during the pretrial period, the recipient is authorized, if not obligated, to refuse to comply. It may even be appropriate to seek sanctions against the attorney who sent the unlawful subpoena. If a procedurally valid subpoena is issued and asks for privileged, confidential, or private information, the recipient is authorized and usually legally obligated to refuse to comply and to notify the sender and the court of the nature of his or her objection. Most sensitive material, such as a victim’s therapeutic counseling records or records of conversations between a victim and her private attorney, is protected by statute, common law, and a constitutional right of privacy. All these bases of legal protection should be asserted by the holder of the information. Except in extremely rare circumstances, a judge will summarily deny a defense request for sensitive material.

In the very unusual case where further inquiry is essential, a judge may conduct a hearing to balance the competing interests and thereafter order **disclosure** of certain information that, on balance, must be disclosed in response to a compelling and legitimate litigation need. In most cases, a judge will conduct an “in camera” review to determine whether information believed to be in a protected file in fact exists. An in camera review involves the judge, alone, reading the file to determine whether any portion of the contents must be disclosed to help clarify an issue legitimately in dispute in a particular litigation.

During a criminal trial, and in some states even during a civil trial, the accused often tries to uncover information pertaining to the victim’s past sexual conduct and use that evidence in the trial. This type of evidence is protected from disclosure in every state under rape-shield laws. One or more exceptions in the law may apply so that absolute protection against disclosure is not guaranteed; however, the victim can also rely on the Supreme Court decision of *Lawrence v. Texas*, 539 U.S. 558 (2003), to insist on protection against disclosure of past sexual conduct, because the Court held in *Lawrence* that lawful sexual activity between adults is protected by a fundamental constitutional right of privacy. With the *Lawrence* decision, victims have a stronger argument that their sexual privacy is shielded not only by a statute but by the Constitution.

Victims in sexual violence trials are often concerned about being identified in the media, and while most states have laws that prohibit public disclosure of a victim's identity, the Supreme Court has held that an absolute bar on disclosure is probably unconstitutional. Nevertheless, most media exercise voluntary restraint and opt not to identify a victim without the victim's permission.

See also: **Constitutional protections; Privacy, definition of; Privacy and inequality; Sexual harassment; Women and privacy**

Suggested Reading: Mackinnon, Catherine. *Sex Equality*. New York: Foundation Press, 2002; Murphy, Wendy. "Minimizing the Likelihood of Discovery of Victims' Counseling Records and Other Personal Information in Criminal Cases: Massachusetts Gives a Nod to a Constitutional Right to Confidentiality," *New England Law Review* 32 (1998). <http://www.nesl.edu/lawrev/vol32/4/MURPHY.HTM>. Online, April 2006; Murphy, Wendy. "The Victim Advocacy and Research Group: Serving a Growing Need to Provide Rape Victims with Personal Legal Representation to Protect Privacy Rights and Fight Gender Bias in the Criminal Justice System," *Journal of Social Distress and the Homeless* 11 (2001): 123; Smith, Steven. "Constitutional Privacy in Psychotherapy," *George Washington Law Review* 49 (1980): 22; Taslitz, Andrew E. *Rape and the Culture of the Courtroom*. New York: New York University Press, 1999.

Wendy J. Murphy

Silver platter doctrine

One of the most important constitutional safeguards of privacy is the Fourth Amendment's guarantee against unreasonable searches and seizures. A key to enforcing this provision is the exclusionary rule, which restricts the use of evidence seized in an illegal search. For many years the silver platter doctrine served as a loophole to the exclusionary rule, allowing evidence obtained in an unconstitutional search by state or local law enforcement officials to be used in a federal prosecution. This loophole was closed in 1960 and the doctrine is now generally held to be unconstitutional.

The silver platter doctrine developed along with the exclusionary rule, which was established in *Weeks v. United States*, 232 U.S. 383 (1914). The rule originally applied only to federal criminal prosecutions. Evidence uncovered by state or local law enforcement officers in what would have been an illegal search if performed by federal personnel was held to be admissible as long as federal officials did not participate in the search or connive at it. In the words of Supreme Court Justice Felix Frankfurter (in *Lustig v. United States*, 1949), if such evidence was handed to federal agents "on a silver platter," it was admissible in a federal court. This created a sense of apparent inconsistency, especially after the Supreme Court held that the "core" of the Fourth Amendment should apply to the states. In 1960 the Supreme Court ruled in *Elkins v. United States* that such evidence was inadmissible. The following year, the Court applied the exclusionary rule to the states.

Recognition of the doctrine also raised the question of whether it applied in reverse, that is, whether evidence illegally seized by federal agents could be used in a state prosecution. In 1956 the Court ruled that it could, as long as it had not been specifically suppressed in federal court proceedings. The application of the exclusionary rule to the states in 1961, however, made the point largely irrelevant.



The unconstitutionality of the silver platter doctrine applies only in criminal prosecutions. In 1976 the Supreme Court ruled in *Janis v. United States* that evidence seized illegally by one level of government could be used by the other as evidence in civil cases, a provision mostly relevant in tax cases.

A related question has been whether evidence uncovered by a private citizen in what would have been an illegal search if conducted by an agent of law enforcement could still be used. This circumstance, outside the scope of the key silver platter decisions, has been addressed largely at the state level. In an influential decision in 1976, the California Supreme Court held in *People v. Mackinnon* that police could not “stand idly by” and allow a search that would be illegal if they undertook it themselves. However, in order for this restraint to apply, the police must have both the knowledge of the illegal search and the means to prevent it.

See also: **Search warrant**

Suggested Reading: Barton, Robert R. *Texas Search and Seizure*. Huntingdon, NY: Juris, 2002; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul: West, 1999; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul: West, 1996; Leonard W. Levy, Kenneth L. Karst, and Dennis J. Mahoney (eds.). *Encyclopedia of the American Constitution*, 4 vols. New York: Macmillan, 1986; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow Publishers, 2000.

William C. Lowe

***Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 109 S.Ct. 1402 (1989)**

In 1987 the Federal Railroad Administration (FRA) passed the Federal Railroad Safety Act in an attempt to address the issue of employees who were intoxicated from alcohol and drugs while operating locomotives within the United States. The act cited a study conducted in 1979 illustrating the extent and seriousness of the problem. In consideration of the potential destruction and financial loss resulting from the actions of intoxicated railroad employees, the Supreme Court decided that the act justified potentially intrusive methods of reducing the employees' use of drugs or alcohol while on the job.

Subpart C of the act required immediate and mandatory **blood testing** and **urine analysis** from any employee involved in a major train accident. It defined a major train accident as an incident where death occurs, where a hazardous spill resulting in evacuation or injury occurs, or where damage caused to railroad property totals \$500,000 or more. The act also gave railroads the discretionary power, under subpart D, to demand breathalyzer or urine tests from employees suspected of being intoxicated. The Railway Labor Executives' Association filed suit, attempting to prohibit the new regulations. The association argued that a violation of the Fourth Amendment could occur if an employee was required to submit to any form of testing without probable cause. By requiring an employee to submit to **drug testing** based simply on the random discretion of the FRA, such a search would lack the certainty requirement consistent with probable cause; thus, the search would be violation of the Fourth Amendment. After the federal district court had heard the association's argument, it held that, although the Fourth Amendment does protect

an individual's right to the integrity of his or her own body, the need of society to remedy the serious problem of intoxication, which may cause damage to life and property, is more important than the traditional requirement of probable cause to make a search constitutional under the Fourth Amendment.

When the case reached the Ninth Circuit Court of Appeals, this court reversed the district court's decision. The court of appeals agreed with the district court that the rules stipulated in subpart D could violate the employees' right to privacy under the Fourth Amendment. The court of appeals also affirmed that, because of the significant safety concern for the public, the traditional requirement of probable cause was not realistic in requiring blood, urine, or breath tests. However, the court of appeals reversed the district court's decision on the grounds that such blanket authority to require testing was too sacrificial of constitutional protections. The court of appeals decided that, at a minimum, there should be a prerequisite of reasonable suspicion of intoxication before the FRA could require an employee to submit to testing. The court held that, because the FRA regulations did not require that the suspicion be related to an individual, the suspicion could not be reasonable. Based on this reasoning, the court of appeals reversed the decision of the district court and concluded that the FRA should find specific reasonable suspicion of intoxication before it could order an employee to submit to a drug test.

The Supreme Court decided to hear the case under a writ of certiorari and reversed the decision of the court of appeals to invalidate the regulations stipulated in the act. The Court, however, recognized the long history of precedence that protected individuals from a compelled intrusion into their privacy. Even though the collection and analysis of biological samples by government agencies are searches subject to constitutional discretion, not every search could be considered unlawful or in violation of the Constitution. The Court then attempted to weigh the balance between the individual's rights to a **reasonable expectation of privacy** against the needs of society for safe railroading practices. Consequently, it recognized that, under certain circumstances similar to the operations of prisons, schools, and governmental offices, there are exceptions to the normal requirements that government officials conduct searches within the scope of the Fourth Amendment. Along those same lines, the Court deemed the tasks of railroad officials as safety sensitive and as beyond the normal Fourth Amendment requirement of probable cause.

The Court addressed the concern of the court of appeals using the same line of protective reasoning it had provided to justify the surrendering of the traditional requirement of probable cause. It held that the blanket authority given in the Federal Railroad Safety Act, for the purposes of random testing without reasonable suspicion or probable cause, was required to ensure the results the act had been created to achieve. The FRA had provided the records of years of investigative study that demonstrated there was no way to perfectly and accurately determine the intoxication of specific employees while they were working on safety-sensitive tasks. Instead, the FRA claimed blanket testing to be the most effective way to deter employees from using drugs or alcohol while working. In other words, the possible discovery of intoxication and threat of dismissal was the most effective way to keep employees from using drugs and alcohol while on the job. If employees could not predict when a test would occur, then the effect of deterrence would be greatly increased. The Court agreed that the benefit to society through deterring



employees from using drugs and alcohol while working was important enough to sacrifice the traditional rules required for a Fourth Amendment search.

See also: United States. v. Scheffer, 523 U.S. 303 (1998); Vernonia School District v. Wayne Acton, 515 U.S. 646 (1995); Workplace privacy

Suggested Reading: Amsterdam, Anthony G. "Perspectives on the Fourth Amendment," *Minnesota Law Review* 58, no. 3 (1974): 349–447; Barte, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul: West, 1999; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

Sean M. Peek

Smart cards

A smart card is a plastic card, typically the size of a standard **credit card**, which is embedded with a micromodule containing a single silicon integrated circuit chip with a memory and microprocessor. A familiar example is a magnetic strip card. Other examples include optical cards, memory cards, and microprocessor cards. Memory and microprocessor cards are truly smart cards in that they each contain an integrated circuit chip that can store information, perform local processing, and complete complex calculations. These integrated circuit cards use radio frequency chips to operate, whereas an optical card requires a laser to read the card. The benefits of smart cards are their size, their cost, and their protection against fraud. The concerns are that smart cards enable intrusive profiling of individuals by integrating different databases and **biometric identifiers** within the card.

See also: Automatic Teller Machine (ATM); National identity cards; Radio Frequency Identification (RFID)

Suggested Reading: eGov Strategies. <http://www.egovstrategies.com>. Online, April 2006; Hwang, Min-Shiang, and Li-Hua Li. "A New Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics* 46 (2000): 28–30.

Jill Joline Myers

Sobriety checkpoint

A sobriety checkpoint is a police roadblock set up ostensibly to screen motorists to determine if they have been operating **automobiles** under the influence of alcohol. Sobriety checkpoints have become part of the well-publicized efforts to stop drunk driving on American highways. Powerful citizen advocacy groups such as Mothers Against Drunk Driving (MADD) have influenced politicians and government officials to take steps such as lowering the blood alcohol threshold to determine legal intoxication and to support tactics such as sobriety checkpoints to stop

drunk drivers. Yet, because of the potentially invasive nature of the sobriety checkpoint, the practice appears to threaten **constitutional protections** and challenge assumptions on the limitations of governmental powers.

The sobriety checkpoint is usually a short interruption of a driver's journey that allows police to assess whether the driver is intoxicated. The delay is less invasive than an **automobile search**, where police officers physically examine the automobile, sometimes without a **search warrant**, when there is probable cause. Because police at a checkpoint stop all drivers, one has to assess whether the loss of some rights for a greater society good, such as removing drunk drivers from the roadways, is sufficient ground to allow government intrusion on all individual drivers. An expectation of privacy and having the right to travel without arbitrary actions by the government are reasonable and well within the context of constitutional protections provided for by Article IV of the Constitution as well as by the Fourth Amendment.

Two cases, *Michigan Department of State Police v. Sitz* (1990) and *Illinois v. Lidster* (2004), provide legal standing for sobriety checkpoints. In *Illinois v. Lidster*, the Supreme Court determined that such checkpoints do not violate one's Fourth Amendment rights. The Court further determined in the same case that the lacking of any individualized suspicion by the police cannot by itself determine the outcome of a case because, in the opinion of the Court, one's car may not be treated as one's home (see *New York v. Class*, 475 U.S. 106). Also, in *Michigan Department of State Police v. Sitz*, the Supreme Court ruled that special law enforcement concerns can justify checkpoint stops even if there is no individualized suspicion. In short, the police can arrest a driver for drunk driving without knowing anything about that driver's drinking until intoxication is discovered at the checkpoint.

What about individuals who neither drink nor wish to be subjected to sobriety checkpoints? The Court's concern for overall societal benefits may outweigh individual interest. Again, the *Michigan State Police* case is especially significant because of the rather extensive rationale for sobriety checkpoints in the majority opinion by the late Chief Justice William Rehnquist. The following statements are part of that opinion: "No one can seriously dispute the magnitude of the drunken driving problem or the State's interest in eradicating it. . . . In sum, the balance of the State's interest in preventing drunken driving, the extent to which this system can reasonably be said to advance that interest, and the degree of intrusion upon individual motorists who are briefly stopped, weighs in favor of the state program" (496 U.S. 444).

The chief justice's words make clear that the Court was weighing the merits of the rights of the individual against the interest of government. The majority opinion by Rehnquist remains the official position of the Court on sobriety checkpoints. However, Justice John Paul Stevens declared in his dissenting opinion, "Unfortunately the Court is transfixed by the wrong symbol, the illusory prospect of punishing countless intoxicated motorists, when it should keep its eyes on the road plainly marked by the Constitution." So while the Supreme Court has upheld the constitutionality of sobriety checkpoints, it also established specific guidelines for their use. Police are required to give notification of a checkpoint, and they cannot detain motorists for an unreasonable amount of time. The Court has also indicated that an



arrest rate of less than 5 percent would raise questions of whether there is a legitimate government interest in the activity.

Subsequently, the decision has had an impact on sobriety checkpoints in other states. The United States Congress also conducted public hearings on drunk driving and its adverse impact. A federal statute was passed that allowed the secretary of transportation to withhold part of a state's federal highway funds if the state did not pass laws requiring the drinking age to be at least twenty-one. The federal action was supported in the 1987 case of *South Dakota v. Dole*, 483 U.S. 203. Citizens have also been part of the widespread efforts that have resulted in public policies and judicial decisions that allow law enforcement officials to carry out sobriety checkpoints. As previously noted, MADD has been the catalyst for numerous public hearings on drunk driving and its impact at both the local and national levels. Public awareness programs and advertisements on the number of automobile accidents and deaths attributed to drunk driving have helped bring the issue to the public's mind and to the attention of politicians. Other citizen groups, businesses, entertainment organizations, and government agencies have become advocates against drunk driving through supporting numerous public service announcements and advertisements. Thanks to modern technology, a causal surfing of the web resulted in this writer identifying more than 30 advocacy and community groups involved in this issue. Besides MADD, the array of advocacy groups against drugs and alcohol include Citizens Against Drug Impaired Drivers and Citizens for Reliable and Safe Highways. Business groups such as the National Association of Convenience Stores and entertainment organizations represented by the Entertainment Council, Inc., are listed as advocates against drunk driving. Professional groups such as the National Association of Broadcasters and government agencies such as the National Safety Transportation Board, United States Department of Transportation, Centers for Disease Control and Prevention, the United States Department of Justice, and the United States Department of Education are also numbered as advocates against drunk driving. The support of government agencies is significant because their advocacy is often followed by official policies on a particular subject. This is especially true of the Department of Transportation division of National Highway Traffic Safety Administration, which has issued guidelines for carrying out sobriety checkpoints. The Department of Transportation, under former secretary Elizabeth Dole, successfully defended the national government's power to withhold a state's federal highway funds when the state did not comply with a federal mandate to stop underage drinking.

The sobriety checkpoint is a policy that illustrates judicial balancing of individual privacy rights against the interests of the whole of society, and citizen influence. Because the court has provided legitimacy and rationale for stopping motorists to determine if they are intoxicated, the sobriety checkpoint has become a fixture for all who drive on American highways. The activities of powerful advocacy groups, particularly Mothers Against Drunk Driving, represent how citizens can impact decisionmakers. Such citizen influence guarantees that those inclined to drink and drive will likely face less than sympathetic law enforcement officials and judges. Motorists who are law abiding as well as nondrinkers will continue to experience the invasiveness of the sobriety checkpoint given the widespread public sup-

port to stop drunken driving and the belief that sobriety checkpoints will both deter and catch drunk drivers.

See also: Constitutional protections; Terry v. Ohio, 392 U.S. 1(1968)

Suggested Reading: Barton, Robert R. *Texas Search and Seizure*. Huntingdon, NY: Juris, 2002; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul: West, 1999; Glick, Henry R. "Court Politics and the Judicial Process." In Virginia Gray and Russell L. Hanson (eds.), *Politics in the American States: A Comparative Analysis*, 8th ed. Washington, DC: Congressional Quarterly Press, 2004; Hubbart, Philip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; National Highway Traffic Safety Administration. *Saturation Patrols and Sobriety Checkpoints: A How-to Guide for Planning and Publicizing Impaired Driving Enforcement Efforts*. Washington, DC: National Highway Traffic Safety Administration, 2000; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000; Taylor, Lawrence. *Drunk Driving Sobriety Checkpoints*. Drunk Driving Law Center, www.duicenter.com/checkpoints. Online, December 2005.

D'Linell Finley

Social Security number

The Social Security Act of 1935 established Social Security numbers (SSNs) for the sole use of the Social Security program. Less than a decade later, President Franklin D. Roosevelt signed Executive Order 9397, permitting federal agencies to use the identifying numbers as part of a new record-keeping system. SSNs became taxpayer identification codes in 1961 when the **Internal Revenue Service (IRS)** starting using them. The Tax Reform Act of 1976 enabled driver's license and motor vehicle registration entities, welfare agencies, and state and local tax organizations to use SSNs.

A SSN is a unique nine-digit numerical sequence issued to every U.S. citizen by the Social Security Agency (SSA). The first three numbers identify the person's residence as provided on the application form. The SSA discloses the numbers being used in each area on a routine basis. While it is widely rumored that the middle two digits represent a person's ethnicity, there is no evidence to substantiate this claim.

An individual's Social Security number is **confidential** information; it should never be offered on a routine basis. One's Social Security card, containing the number, should be safeguarded. It should never be carried with the individual unless there is a unique circumstance requiring the card. When people give out their SSNs, they are allowing others to gain access to their **personally identifiable information**. An average person cannot correct these important data if an error is discovered. Nor does the person have the legal right to correct any errors.

An individual needs to maintain vigilance in order to protect and prevent abuse of the Social Security number. Even if someone directly inquires about an individual's number, offering that number is not mandatory. There are several important questions to ask regarding why the number is needed, how it will be used, and what the consequences are for noncompliance. Once this information



is known, the person's choice to provide the Social Security number is an informed-albeit voluntary-decision.

There is significant legal constraint concerning government personnel asking for a person's Social Security number. However, there is no legal governance over private companies regarding their policies on acquiring, maintaining, or disclosing this private information. If a government agency employee asks for an individual's Social Security number, the government worker is required to supply information on a Privacy Act **disclosure** notice as outlined in the **Privacy Act of 1974**, which addresses all three important questions mentioned earlier. Nongovernmental firms are not required to comply with this legal condition. If a private company's policies on private information are improper, a customer's only alternative is to locate a different company with which to do business.

The concerns with SSN security are twofold. SSNs are used to link together data about a person using a variety of sources. The person's SSN is the identifying common denominator. Secondly, many individuals regard presentation of one's SSN as representation and authorization of the individual's identity. Medical records as well as brokerage files treat a person's SSN as the true indicator of the client's identity. Banks treat the client's SSN as a secret passcode known only to the account owner; in reality, one only needs to present the account holder's name, along with his or her SSN, and state that the account number has been forgotten. Usually the bank will permit a transaction such as the transfer or withdrawal of funds. These two concerns stand in direct conflict with each other. Commonly used on drivers' licenses, mailing labels, and grade transcripts from colleges, these readily available codes—depicting people's identities—should never be used for identity **authentication** purposes.

The Privacy Act of 1974 is the main law that addresses the use of SSNs. It mandates that a federal agency, when asking for a person's SSN, must inform the person of four things: the statute or order permitting the solicitation, the voluntary or mandatory nature of compliance with the request, the intended purpose and how the information (if disclosed) will be used, and any consequences for noncompliance. The act establishes that it is illegal to repudiate a person's rights because of refusal to provide his or her SSN. One exception to this is if federal law necessitates SSN disclosure. A second exception is the disclosure to a government agency whose record-keeping system predates 1975.

At their inception, and for several decades past that point, it was clearly noted on the card itself that SSNs were not to be used for identification purposes. However, no law was passed to confirm this guiding principle. Many private citizens are enraged by the U.S. government's violation of this founding SSN precept. The IRS states that any U.S. citizen earning income is required to have a Social Security number. The IRS also requires employers to report income earned by an employee by the employee's SSN. Some legal scholars consider the legal foundation on which the IRS bases its authority to be very shaky. However, it is important to realize that the IRS incarcerates violators of their policies. Given this, the majority of citizens and employers comply with the IRS.

The Social Security Agency (SSA) rarely issues a new SSN to a person experiencing extreme duress from a stalker or as a result of identity theft. This task requires, however, convincing all parties involved that all other possible options

have been explored and used. The SSA does not promise to issue a new number and leaves the decision of how to proceed to the judgment of the local office. While there are companies willing to provide an individual with a new SSN, the only legal route to obtaining a new SSN is through the Social Security Agency. Any company claiming to provide this service is fraudulent.

See also: **Identity fraud**

Suggested Reading: O'Reilly, James. *Federal Information Disclosure*, 3rd ed. St. Paul: West, 2000; Privacy Rights Clearinghouse. www.privacyrights.org. Online, December 2005; Social Security Agency. www.ssa.gov. Online, December 2005.

Christine Berry Lloyd

Sodomy

In the early twentieth century, the Ariston Turkish and Russian Baths were among the places in New York City where men met for anonymous sexual encounters. In 1903, working with a local anti-vice organization, police placed the bathhouse under **surveillance** and arrested 16 men on sodomy charges in a late-night sting operation. One man was eventually sentenced to 20 years in prison. The Ariston raid was the first of many raids on gay bathhouses in major urban centers. A century later, the U.S. Supreme Court declared sodomy laws unconstitutional, noting in its majority decision that the meanings of both sodomy and sexuality have changed greatly over time. Understanding the history of sodomy and sodomy laws is important for a broad understanding of sexual privacy for at least two reasons. At the most obvious level, the policing of sodomy has entailed serious encroachments on sexual privacy, uniquely affecting gays and lesbians. Also, the term “sodomy” acts simultaneously as a stigma-drenched criminal category and as a criterion and cultural shorthand for what it means to be gay or lesbian.

In modern usage, sodomy refers to nonprocreative sexual practices, typically oral or anal sex. From the colonial period through most of the nineteenth century, however, sodomy laws criminalized a wide range of sexual conduct that often fell under proscriptions against “crimes against nature” or against “unspeakable acts”: bestiality, public masturbation, and pedophilia. A wealth of historical evidence suggests that sodomy laws did not target sexual intimacy among same-sex couples in particular. Colonial authorities considered sodomy a capital offense, but they did not view sodomy as linked to an offender’s sexual orientation. A concern with non-reproductive sexual acts and sex between parties of vastly different social statuses (adult/child or master/servant) characterized the law’s statutory scope and enforcement. In general, police and prosecutors pursued sodomy charges in instances where men sexually preyed upon children. In New York City, for example, almost all sodomy prosecutions involved men accused of harming children under the age of 18.

The dominant understandings of sexuality and same-sex desire changed radically in the late nineteenth and early twentieth centuries, and the policing and surveillance of sodomy changed in response. During these years of sexual upheaval—revealed in the growth of scientific understandings of human sexuality, a selective erosion of Victorian sexual mores, and shifting norms of courtship—prosecutors made more frequent use of sodomy laws, and they used them to target gay men. In the early

twentieth century, sodomy prosecutions soared in cities like Boston, Philadelphia, St. Louis, and Los Angeles. Whereas the older use of the sodomy law primarily addressed men's coercive sex with weaker or nonconsenting parties, the twentieth-century use of the law increasingly tied nonnormative sex with a homosexual status group.

With a new understanding of sodomy and homosexual identity in place, police and courts mounted a large intervention into the private lives of gays and lesbians. The net of sexual surveillance expanded during the first half of the twentieth century, as some anti-vice and anti-crime organizations were given quasi-police powers to investigate and secure evidence of sexual immorality. Following the repeal of Prohibition, vibrant urban gay subcultures were effectively crushed by the state liquor authority and other state agencies that made saloon licensing contingent on the owners' cooperation in excluding supposed sexual degenerates. During the Cold War, the state surveillance of gays and lesbians intensified, and the U.S. government launched an extensive attack on suspected gays and lesbians in the civil service. Moreover, sodomy laws disproportionately affected the less fortunate. The greatest number of sodomy arrests occurred in impoverished sections of U.S. cities. Historian George Chauncey notes that the primary targets of sodomy arrests in New York City during the 1940s and 1950s were Puerto Rican and African American.

In the words of legal scholar William Eskridge, "The modern regulatory state cut its teeth on gay people." These efforts were buoyed by the modern conflation of gay identity and sodomy. The seemingly inseparable link between sodomy and same-sex desire broadly affected sexual privacy by cementing a connection between deviant sexual practices and gays and lesbians. Writing about the creation of modern sexuality in the late nineteenth century, social theorist Michel Foucault argued that "homosexuality appeared as one of the forms of sexuality when it was transposed from the practice of sodomy onto a kind of interior androgyny, a hermaphroditism of the soul." In other words, the modern act of sodomy was seen not just as a sexual act like other sexual acts, but it functioned as a proxy for something deeper in the individual. Earlier medical, legal, and cultural understandings of sodomy variously positioned it as a vice, addiction, or human failing. Likewise, men in the nineteenth century could have sex with other men without impugning their masculinity or respectable status. In the modern age, however, sodomy came to be viewed as an index of a particular sexual self. Not captured in sodomy arrest records or rates of prosecution, this effect of the understanding of sodomy is more subtle, although no less consequential, in eroding sexual privacy. The practice of sodomy marks individuals as deviant or criminal, while gays and lesbians are simultaneously marked as deviant for presumably engaging in the practice of sodomy.

In their ruling in *Bowers v. Hardwick*, 478 U.S. 186 (1986), the U.S. Supreme Court gave hard legal backing to the taken-for-granted link between sexual deviance and gays and lesbians. In the majority ruling, Justice White claimed that proscriptions on "homosexual conduct" had "ancient roots." In a concurring opinion, Justice Burger referenced Judeo-Christian ethics and Western civilization to condemn "homosexual sodomy." Leading up to the *Lawrence v. Texas*, 539 U.S. 558 (2003), decision, a group of historians filed an amicus brief with the Court in which they explained that the phrase "homosexual sodomy" would have been "literally incomprehensible to the Framers of the Constitution" because sodomy was viewed

as a discreet act and not as an indication of a person's sexual orientation. Nonetheless, the link between sodomy and sexual identity has been generally accepted as a taken-for-granted fact in legal and popular culture, and was succinctly voiced in 1993 when former senator Strom Thurmond shouted on the Senate floor during a debate about gays in the military that "heterosexuals do not practice sodomy!"

In the years leading up to the Court's 2003 disposal of Bowers in *Lawrence v. Texas*, legal scholarship has brought to light evidence that sodomy laws bestowed legal legitimacy on gross intrusions in the private **family** lives of gays and lesbians, and they allowed employers and state officials to commit egregious forms of discrimination. For instance, in *Bottoms v. Bottoms*, Pamela Bottoms successfully fought for custody of her three-year-old grandson upon learning that her daughter, Sharon Bottoms, was a lesbian living with another woman. The trial judge invoked Virginia's sodomy law to invalidate the mother's custody rights, reasoning that the mother routinely engaged in illegal acts and was therefore an unfit parent. When the case reached the Virginia Supreme Court in 1993, the Court upheld the original ruling and noted that "conduct inherent in lesbianism" is punishable as a felony in Virginia and "that conduct is another important consideration in determining custody." In another case, Robin Shahar's offer of employment at the Georgia attorney general's office was rescinded when her employer, Michael Bowers, learned of her upcoming commitment ceremony to another woman. When Shahar sued, Bowers cited Georgia's sodomy law as a defense, arguing that employing a lesbian is akin to employing someone committing ongoing criminal behavior. The Eleventh Circuit sided with Bowers and denied the basis for Shahar's anti-discrimination suit.

Bottoms v. Bottoms, *Shahar v. Bowers*, and the history of sexual regulation show how sodomy laws not only governed private sexual conduct, but also shaped the categories in which people were placed and the enduring associations attached to those categories. Sodomy laws effectively created a criminal class, giving legal justification to intrusions into the private lives of gays and lesbians. Over the course of the twentieth century, sodomy statutes defined homosexuals as a class on the margins of the law and gave legal ammunition to the opponents of sexual liberty.

Suggested Reading: Berland, Renée. "Looking Back: Scholarship in Early American Sex," *American Literary History* 17 (2005): 148–159; Brief of Professors of History George Chauncey, Nancy F. Cott, John D'Emilio, Estelle Freedman, Thomas C. Holt, John Howard, Lynn Hunt, Mark D. Jordan, Elizabeth Lapovsky Kennedy, and Linda P. Kerber as Amici Curiae in Support of Petitioners, *Lawrence v. Texas*, 539 U.S. 558 (2003) (No. 02-102); Chauncey, George. *Gay New York: Gender, Urban Culture, and the Making of the Gay Male World, 1890–1940*. New York: Basic Books, 1994; D'Emilio, John, and Estelle Freedman. *Intimate Matters: A History of Sexuality in America*. New York: Harper and Row, 1988; Eskridge, William N. *Gaylaw: Challenging the Apartheid of the Closet*. Cambridge, MA: Harvard University Press, 1999; Foucault, Michel. *History of Sexuality: An Introduction*. New York: Vintage, 1984; Johnson, David K. *The Lavender Scare: The Cold War Persecution of Gays and Lesbians in the Federal Government*. Chicago: University of Chicago Press, 2004; Robertson, Stephen. *Crimes against Children: Sexual Violence and Legal Culture in New York City, 1880–1960*. Chapel Hill: University of North Carolina Press, 2005.

Brian L. Donovan

***South Dakota v. Opperman*, 428 U.S. 364 (1976)**

In this case, Mr. Opperman's **automobile** had been impounded by police for being illegally parked. While in possession of the vehicle, officers conducted a routine search and inventory of all the items found inside. The search included the main section of the car as well as the glove compartment. While logging the items within the glove compartment, the officers found a small amount of marijuana. When Opperman arrived at the station to retrieve his property and to reclaim his vehicle, he was arrested and charged with possession of marijuana.

At the trial, a police officer testified that the purpose of the search was to protect the valuable items that were seen in the vehicle. He stated that the impound lot was not well protected, and since cars had been broken into, the department thought it prudent to search and inventory all the items inside the vehicles within their custody. Opperman's motion to suppress the discovery of the marijuana was denied by the trial court, and he was convicted and sentenced to a \$100 fine and 14 days in county jail.

On appeal, the Supreme Court of South Dakota reversed the conviction on the grounds that the search made by the officers had not been reasonable, and that it had been a violation of Opperman's Fourth Amendment rights of privacy. After granting a writ of certiorari, the Supreme Court of the United States reversed the state court. The Court reasoned that the nature of an automobile is not the same as the nature of a **home**. As such, the **reasonable expectation of privacy** in an automobile is less than the expectation of privacy in a home. In other words, the restrictions that bind law enforcement will be less strict when conducting searches of automobiles than when conducting searches within homes. In this case, Opperman's automobile had been subject to a legal seizure because the vehicle had been parked in a no-parking zone for an extended period of time. The Court justified the local police department's standard search and inventory practices based on three reasons. First, the court recognized a legitimate need to protect the items found inside an impounded vehicle from unexpected loss or theft. Second, there was a legitimate need to protect police from claims of lost or stolen items while vehicles were legally within their custody. Finally, the Court found the department's practices reasonable because of the need to protect the officers and department from potentially dangerous items inside impounded vehicles.

Furthermore, the Court looked to the Fourth Amendment standard for reasonableness to determine the scope of constitutionally protected inventory searches. It concluded that inventory searches conducted under the circumstances in this case were not the same as searches that required probable cause in order to be reasonable. The probable cause standard for a reasonable search was not applicable to this case. Since a search requiring probable cause typically occurred in criminal investigations, it was not necessary for searches conducted under routine inventory circumstances, where there was no reasonable belief of criminal activity, to meet the same probable cause standard. The Court held that the Fourth Amendment does not require that every search be conducted only after probable cause has been established. Rather, it held that every search be conducted within the realm of reasonableness, a concept established through the totality of circumstances surrounding the specific situation.

The Court ultimately ruled that Opperman was not entitled to an order to suppress the evidence because the search had been conducted within the realm of reasonableness. The decision was supported by Justices Burger, Blackmun, Powell, Rehnquist, and Stevens. Their opinion asserted that the fact that the search was conducted in an automobile gave the police department more leeway under the protections of the Fourth Amendment. The Court held that since the automobile had been legally impounded and the search had been done as a routine safety precaution, it was reasonable for the officers to conduct the search. Moreover, the type of search conducted had not been related to a criminal investigation and therefore was not required to meet the probable cause standard typically required for most searches to be legitimate under the Fourth Amendment.

The dissenting argument in this case was that case law was clear as to under what circumstances the right to privacy in an automobile was just as merited as the right in a home. The dissenting judges—White, Marshall, Brennan, and Stewart—rationalized that people were likely to store their papers and effects in their automobiles from time to time and were entitled to the same expectation of privacy that they would have in their homes.

Further, the dissent disagreed with the opinion that the routine search into an automobile for the protection of valuable items should be without the same constitutional requirements as other searches. The testimony in the case stated that the search had been conducted as a standard procedure and not because there was anything valuable in **plain view**. There was no reason to believe that anything valuable existed inside the vehicle. To enter into the vehicle for no reason was absolutely a violation of an individual's right to privacy under the Fourth Amendment. Furthermore, if an item of some value could be seen in plain view, the entry into a locked vehicle to obtain that item for the protection of the owner does not permit the continued search into the enclosed glove compartment. The right to search the vehicle for items surpassed the point of reasonableness once the search was extended to areas that were not in plain view, such as a suitcase, a bag, or a glove compartment.

The dissent argued that the majority opinion incorrectly drew a distinction between the right to be secure in a home and the right to be secure in an automobile. The dissent argued there was no difference, and that the right was equal in both circumstances. Also, the dissent disagreed with the belief that there was not a need for the same constitutional requirements that all other searches must have. The reasonableness and extent of this search needed to be based on the same standards that apply to other intrusions. The fact that this search had been undertaken without criminal suspicion did not excuse it from the same limitations specified within the Constitution.

See also: Automobile search; Cady v. Dombrowski, 413 U.S. 433 (1973); *Carroll v. United States*, 267 U.S. 132 (1925); **Constitutional protections**; *Schmerber v. California*, 384 U.S. 757 (1966); *Terry v. Ohio*, 392 U.S. 1 (1968)

Suggested Reading: Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul: West, 1999; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham,

NC: Carolina Academic Press, 2005; Pettifor, Bonnie, and Charles E. Petit. Weeks v. United States: *Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

Sean M. Peek

Spam

Spam refers to unsolicited or unwanted **electronic mail**, usually sent in large quantities and consisting of commercial advertisements. Spam has been described as “the scourge of the Information Age.” The vast majority of e-mail sent today is spam, although much of it is diverted before delivery. Spam is generally viewed as objectionable because of its often offensive content, the resources it consumes, its effects on **computer** and network security, and the secondary effects of responses to spam. A variety of technological and legal mechanisms have been deployed against spam, although it has proven to be an extremely persistent problem.

Most efforts to define spam limit it to unsolicited messages—those sent to recipients who have no relationship to the sender, and who have not consented to receive the messages. Because some unsolicited messages are unobjectionable, however, the definition of spam is usually further limited to include only commercial messages or those sent to a large number of recipients within a short period of time. Spam therefore is commonly described as unsolicited commercial e-mail (UCE) or unsolicited bulk email (UBE).

There are many other definitions of spam. In some e-mail systems, for example, spam-filtering criteria are determined based upon the messages that individual users choose to identify as spam, rather than by application of objective criteria. Spam may also be defined based upon the sender’s failure to comply with various rules, such as **disclosure** requirements or processes for collecting or removing addresses from a mailing list.

The most common technological response to spam is the deployment of automated techniques that attempt to identify which incoming messages are spam, then block or divert those messages while permitting legitimate messages to pass through. Filtering and blocking can be performed by end users or by service providers who receive e-mail on the end users’ behalf. All filtering technologies carry a risk of false positives, false negatives, or both. Because the danger that legitimate communications will be lost if the rate of false positives is too high, users tend to prefer more conservative filters, despite the fact that they permit more spam to pass through undetected. A mechanism that merely flags or temporarily diverts putative spam rather than blocking it completely is another viable option.

Filtering technologies often employ whitelists and blacklists—lists of addresses from which a particular recipient does or does not wish to receive e-mail messages, regardless of other message characteristics. A related approach, a challenge-and-response system, requires unrecognized senders to respond to an automated challenge message before their e-mail will be delivered to the recipient. Challenge-and-response systems have been widely criticized for the overhead they impose, especially on senders, and many legitimate senders routinely ignore challenges, so such systems tend to produce a high false positive rate in practice.

Many end users attempt to control circulation of their e-mail addresses in order to limit the amount of spam they receive. For some this is a fairly effective method, although it is impractical for those who want to publicize their addresses for legiti-

mate purposes, and it is common for senders of spam to gain unauthorized access to lists of e-mail addresses by a variety of means.

Other technical responses to spam include limits on third-party relaying of e-mail, limits imposed by service providers on their own users' outbound e-mail, and various methods of sender **authentication**. These approaches to date have had only a limited impact on the volume of spam, but they may well fare better in the future.

Since the mid-1990s, spam has been the focus of hundreds or thousands of court cases. Perhaps the two most important of these are *CompuServe Inc. v. Cyber Promotions, Inc.*, (1997) and *Intel v. Hamidi*. In *CompuServe Inc. v. Cyber Promotions, Inc.*, an e-mail marketing firm had unrelentingly sent unsolicited e-mail advertisements to hundreds of thousands of CompuServe subscribers, ignoring CompuServe's objections and circumventing its efforts to block the messages. CompuServe sued, alleging that the messages amounted to a "**trespass to chattels**" a somewhat obscure legal theory based upon unauthorized interference with personal property. The court recognized the claim and enjoined the marketing firm from sending unsolicited advertisements to CompuServe's subscribers.

The same theory was used in many other spam-related cases following *CompuServe Inc. v. Cyber Promotions, Inc.*, but it was dealt a blow by the California Supreme Court in the case of *Intel Corp. v. Hamidi* (2003). In this case, a disgruntled former employee of Intel Corporation had waged a campaign against the company and its practices, and as part of that campaign, the employee had sent mass e-mail messages to thousands of Intel employees using their Intel e-mail addresses. Intel demanded that he stop sending e-mail into its system and attempted to block the messages on its own; the company then resorted to litigation after these efforts were unsuccessful. The court rejected Intel's trespass to chattels claim on the ground that Intel could not demonstrate any direct injury to its e-mail system from the messages; its objection was to the content and indirect effects of the messages, which was deemed beyond the scope of the trespass tort.

Legislatures have also attempted to control spam, arguably with even less success than the courts. More than half of the states in the United States enacted anti-spam legislation between 1997 and 2003, although only two of these laws (in California and Delaware) contained broad prohibitions on spam, neither of which was ever enforced. In late 2003 the federal CAN-SPAM Act was enacted. CAN-SPAM primarily targets fraudulent activities in commercial e-mail rather than the sending of spam itself. The law did authorize the Federal Trade Commission (FTC) to establish a registry of addresses to which spam could not be sent; although the FTC elected not to implement this provision of the law, in part because of concerns that the **confidentiality** of addresses in the registry could not be assured. Some jurisdictions outside the United States have enacted much stronger restrictions on spam, although to date the impact of such laws on international spam, at least, seems to be fairly minimal.

See also: **Internet**

Suggested Reading: Burns, Conrad. Opening Statement of Subcommittee Chairman Conrad Burns. In *Spamming: Hearing Before the Subcommittee on Communications of the Senate Committee on Commerce, Science and Transportation*. U.S. Senate Hearing 105-1028, June 17, 1998. commerce.senate.gov/hearings/hearin98.htm. Online, November 2005; Coalition Against Unsolicited Commercial Email. www.cauce.org/. Online, November 2005; *Controlling the Assault of Non-Solicited*

Pornography and Marketing (CAN-SPAM) Act of 2003. Public Law 108-187, 15 U.S.C. §§7701-7713. www.spamlaws.com/federal/can-spam.shtml. Online, November 2005; Cranor, Lorrie Faith, and Brian A. LaMacchia. "Spam!" *Communications of the ACM* 41, no. 8 (Aug. 1998): 74-83. lorrie.cranor.org/pubs/spam/. Online, November 2005; Postel, Jon. *On the Junk Mail Problem*. Network Working Group RFC 706 (November 1975). www.ietf.org/rfc/rfc0706.txt. Online, November 2005; Sorkin, David E. "Technical and Legal Approaches to Unsolicited Electronic Mail," *University of San Francisco Law Review* 35 (2001): 325-384. www.sorkin.org/articles/usf/. Online, November 2005.

David E. Sorkin

Spyware. See Internet

***Stanley v. Georgia*, 394 U.S. 557 (1969)**

In *Stanley v. Georgia*, the United States Supreme Court ruled that the First and Fourteenth Amendments of the United States Constitution prohibit the government from criminalizing the mere possession of obscene material if the material is held privately. The Supreme Court drew a clear distinction between this case and its previous line taken in earlier cases that allowed states to criminalize pornography that was either sold or distributed to the public. In this case, the Supreme Court focused on the much more limited reach of the obscene material, in that it was merely possessed in the privacy of the defendant's **home**. The sanctity of privacy in one's own home convinced the court to declare unconstitutional the Georgia criminal statute against obscenity at issue in the case.

The defendant in the case, Mr. Stanley, faced an investigation for alleged involvement in illegal bookmaking (betting) activities. A judge had issued a **search warrant**, and federal and state agents searched Mr. Stanley's home. Although they found virtually no evidence of bookmaking, in the process of the search they looked through a desk drawer in an upstairs bedroom. In this drawer they found three reels of eight-millimeter film. The agents also discovered a projector and a screen in an upstairs living room. Using these, they watched the films and seized them after concluding that the films were obscene.

The defendant was arrested and charged with knowing possession of obscene material under Georgia law. The Georgia statute at issue criminalized the knowing possession of obscene material, and under the statute, "a matter is obscene if, considered as a whole, applying contemporary community standards, its predominant appeal is to prurient interest, i.e., a shameful or morbid interest in nudity, sex or excretion." After a jury trial, he was convicted. The State Supreme Court of Georgia affirmed his conviction, and he appealed to the U.S. Supreme Court.

Importantly, Mr. Stanley did not deny that the films were obscene; rather, he focused his argument elsewhere. Although he raised numerous challenges in his appeal to the U.S. Supreme Court, the Court needed to focus on only one to overturn his conviction. The Court accepted his contention that by criminalizing the mere private possession, the Georgia obscenity statute violated the First Amendment, which applies with equal force to the states by virtue of its incorporation under the Fourteenth Amendment.

The Court began by analyzing the Georgia Supreme Court's earlier decision in upholding the conviction against Mr. Stanley. That court had found the Georgia statute constitutional because of earlier cases from the U.S. Supreme Court that allowed the states to criminalize obscene material that was distributed or sold. It found no meaningful distinction between the mere possession and the commercial sale of obscene material.

Nevertheless, both Mr. Stanley and the state of Georgia agreed that this case presented a case of first impression, in that no other case had presented the exact issue under the facts of this case: "whether a statute imposing criminal sanctions upon the mere knowing possession of obscene matter is constitutional."

The state of Georgia argued that the decision in *Roth v. United States*, 354 U.S. 476 (1957), made the case against Mr. Stanley an easy one. It pointed out that in *Roth*, the U.S. Supreme Court had declared that "obscurity is not within the area of constitutionally protected speech or press." Thus, because the Supreme Court had declared that obscenity is not speech protected by the First Amendment, Georgia contended that the states may regulate obscene material without virtually any limits.

Despite the earlier line of cases such as *Roth*, however, the Supreme Court found an enormous distinction based on the facts of Mr. Stanley's case. In rejecting Georgia's argument, the Court noted that "neither *Roth* nor any subsequent decisions of this Court dealt with the precise problem involved in the present case." Those earlier cases dealt with mailing and advertising obscene material, which involved public distribution in some manner. Therefore, none of the earlier statements by the Court "were made in the context of a statute punishing mere private possession of obscene material."

The Court then reemphasized that this case was different from all the rest before it. And, although those earlier cases might have deemed obscene speech to be not fully protected by the First Amendment, the Court refused to find obscene speech to be completely outside the scope of the First Amendment. The Court insisted that the earlier precedent merely established that the government has an "important interest in the regulation of commercial distribution of obscene material. That holding cannot foreclose an examination of the constitutional implications of a statute forbidding mere private possession of such material."

With this backdrop, the Court formulated its general defense for the First Amendment right of the freedom to receive information and ideas. The Court concluded, "This right to receive information and ideas, regardless of their social worth is fundamental to our free society. Moreover, in the context of this case—a prosecution for mere possession of printed or filmed matter in the privacy of a person's own home—that right takes on an added dimension. For also fundamental is the right to be free, except in very limited circumstances, from unwanted governmental intrusions into one's privacy." This dual privacy concern gave the Court enormous pause in upholding a statute that criminalized the mere possession of pornography in one's own home. The Court concluded, "If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds." While recognizing the remaining right of states to regulate



obscene material in the public realm, the Court refused to extend that power to control against an individual's mere private possession.

See also: Constitutional protections; Osborne v. Ohio, 495 U.S. 103 (1990); Paris Adult Theatre I v. Slaton, 413 U.S. 48 (1973); Privacy, definition of

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul: West, 1999; Bodenhamer, David J. and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Hall, Kermit L. *Conscience, Expression and Privacy: The Supreme Court in American Society*. New York: Garland Publishers, 2000; Smith, Robert Ellis. *Compilation of State and Federal Privacy Laws*. Providence, RI: Privacy Journal, 1992; Turkington, Richard C., and Anita L. Allen. *Privacy Law: Cases and Materials*. St. Paul, MN: West, 2002.

Ryan C. Hudson

Stephanie's law

Stephanie's law was signed into law by New York Governor George E. Pataki on June 23, 2003, and has been in effect since August 4, 2003. This New York law joined several other states' laws that criminally prohibit the secret surveillance of individuals in their homes, private residences, and other places that individuals would expect privacy. Named after Long Island resident Stephanie Fuller, whose landlord, William Shultz, had secretly videotaped her bedroom in her rented apartment, Stephanie's law updated state and local "Peeping Tom" and privacy statutes in New York. Stephanie's law provided stricter punishment for video voyeurism or any form of secret surveillance; however, the law also set limited boundaries on where and when individuals' rights to privacy will be protected. Thus, while individuals' right to privacy is protected from secret surveillance in their private homes and in some public settings, Stephanie's law does not protect violations of privacy in public space.

In response to many national incidents of video voyeurism, New York enacted Stephanie's law in order to expand protections of privacy to include incidents where voyeurs used new types of technology. Fuller discovered she was being secretly videotaped by landlord Schultz when her boyfriend noticed strange wires coming out of the smoke alarm in her bedroom. Police later found videotapes in Schultz's apartment, and Fuller was worried that he was selling on the **Internet**. Because Schultz used a video camera that was not filming Fuller through a window, he could not be charged with as violating New York's "Peeping Tom" laws. Instead, Mr. Schultz was charged with **trespassing**; he thus received a fine of \$1500 and was sentenced to three years probation and 280 hours of community service. A previous anti-voyeuristic statute in New York, Article 26 of the General Business law, included a \$300 fine and 15 days of imprisonment for video voyeurism. However it could not be used to prosecute Schultz as the law did not prohibit secret surveillance in private residences. Fuller also discovered similar cases where perpetrators faced other charges for video voyeurism. Other landlords had been found taping their residents, and a kindergarten teacher was charged with endangerment of a minor after filming five girls putting on their swimsuits. Arguing that

these crimes were similar to sexual assault, Fuller began a state-wide campaign. Fuller, joined by other previous victims, lobbied the state legislature for two years to redefine the laws to take into account new types of surveillance technology and classify these types of privacy invasions as sexual assaults.

Stephanie's law amends New York penal code to redefine unlawful surveillance as a Class E felony, punishable by up to four years imprisonment for first offenders, and up to seven years for repeat offences (§70.00[2][e] New York Penal Code, §250.5 New York Penal Code). Under the law, a video voyeur can face two separate charges of criminal unlawful surveillance and dissemination of an unlawful surveillance image regardless of the type of camera or device used in the crime. The law defines unlawful surveillance as the use or instillation of a recording or imaging device to view, broadcast, or record a person dressing and undressing, or his or her sexual or **private parts** for the purpose of entertainment of profit without the individual's permission and where the person has a **reasonable expectation of privacy** (§250 New York Penal Law). Thus, under this new law, Shultz could have been prosecuted for installing the video camera in Fuller's bedroom as well as for selling any of his tapes over the Internet. In addition, the law requires offenders to register with the state **sex offender registry**. Therefore under Stephanie's law, offenders who violate victims' privacy in turn lose their right to privacy.

Stephanie's law joins several other state laws that restrict video voyeurism including laws in the state of Washington, Tennessee, Wisconsin, Virginia, California, and Illinois. Like these states' anti-voyeurism laws, Stephanie's law focuses its protection of privacy on the physical location where the incident occurred rather than on the individual privacy invasion committed. Although Stephanie's law provides tougher sentences on voyeurism than past state laws, many legal critics argue that the law will do little to protect individuals in public spaces. The law prevents individuals from using electronic devices under an individual's clothing, known as "upskirting"; however, the law only prohibits such acts in places where an individual has a reasonable expectation of privacy. Thus under Stephanie's law, individual privacy is protected in a private place such as a "bedroom, changing room, fitting room, restroom, toilets, bathroom, washroom, shower, and any room assigned to guests or patrons in a motel, hotel, or inn" (§250.50 New York Penal Code). The law, however, does not protect individual privacy in public spaces such as malls, restaurants, bus stops, or other crowded areas where upskirting is likely to take place. For example, in the state of Washington, with a similar anti-voyeurism law, two men, Mr. Glas and Mr. Wells, who were convicted of videotaping and upskirting women in a local mall, were later acquitted by the state court because "public places could not logically constitute locations where a person could reasonably expect to be safe from casual or hostile intrusion of surveillance" (*State vs. Glas*, Wash. 2d 410, 2002).

California approved additional amendments when previous anti-voyeurism laws did not protect individuals from several incidents of video voyeurism, including upskirtings in public stores and malls. Following an incident where a man used a gym bag to upskirt several dozen women in crowded stores, the California legislature amended existing laws to focus on the individual violation acts rather than the location. Thus under §647[k][1] of California Penal Code, it is illegal to use hidden cameras to photograph or record another identifiable person under or through that person's clothing for sexual gratification without consent or knowledge of the person.



Although the California code also stipulates that the act should occur under circumstances where the person has a reasonable expectation of privacy, the California law also protects people in public spaces because it includes acts that invade under and through clothing. The expectation is that people are using clothing to protect their privacy, and that using cameras over or through the clothing is in itself an invasion regardless of whether it occurs in public or private spaces.

Unfortunately, video voyeurs have a loophole within the California law as well. In order to be found guilty, the state must prove that the video voyeur took the images for sexual gratification or arousal, and the victim must be identifiable. These two loopholes are problematic as they exclude a majority of invasion of privacy acts. Since most upskirting does not include the victim's face, California law exempts most types of these invasions. In addition, including a sexual gratification clause excludes secret taping used for entertainment or commercial website use. Thus, Stephanie's law provides more protection than its Californian counterpart since the New York law does not require the victim to be identifiable and recognizes that video voyeurism may be for profit.

Victims of upskirting and secret surveillance find the most protection in Illinois. The Illinois anti-voyeurism law prohibits using concealed video and photographic equipment through or under the clothes worn by another person for the purpose of viewing the body or undergarments without the person's consent (section 5/26-4 Illinois Criminal Code).

Although limited, Stephanie's law provides stricter protections against invasions of privacy with video cameras and other recording devices. Supporters of Stephanie's law, including Fuller herself, argue that the law updates the protection of privacy to include new types of surveillance and treats offenders appropriately. Moreover, Stephanie's law expands privacy protection into areas where privacy was always assumed to be protected, including private residences and changing rooms. Several state legislators who supported the law argued that it not only updated laws that had provided loopholes to high-tech video voyeurs but also provided a necessary deterrent through the implementation of prison time. Critics of the statute, however, claimed that the law is too strict on offenders rather than too lax in its definitions of privacy. If convicted under Stephanie's law, individuals may face between two to seven years imprisonment and must register with the state's sex offender registry when released. Some argue that this punishment is too severe for a nonphysical assault, especially when victims cannot be identified as in many incidents of upskirting. Instead, critics argue that stricter trespassing laws and or counseling is a more appropriate way of dealing with video voyeurs than prison time.

See also: **Landlord and tenant**

Suggested Reading: Fahy, Jill. "Victim Changes the System," *Daily Star*, <http://www.thedailystar.com/news/stories/2003/09/19/stepha.html>. Online, September 2003; Gormley, Michael. "Pataki, Legislature to Make Video Voyeurism a Crime," *Associated Press* (June 11, 2003); Martinez, Jose. "N.Y. Makes Video Peeping a Felony," *Daily News* (June 24, 2003): 23; Valetk, Harry A. "Keeping Tom from Peeping: New Law Will Not Protect All Victims of High-Tech Voyeurs," *New York Law Journal* (August 5, 2003): 5.

Evelyn A. Clark

Sterilization

Sterilization is a surgical procedure designed to prevent reproduction. Legally and politically in the United States, sterilization is couched in terms of the right of the state to control humans through health and safety regulations versus the individual's right to control her or his own body. Socially, however, sterilization practices resonate with social control measures disproportionately targeted at certain minority groups.

The right to control one's body is not explicitly a **constitutional protection**; rather, it is an assumption grounded in private property rights. Historically children, slaves, servants, and women were denied bodily autonomy. For example, slaves were owned by masters, and wives were subject to the whims of their husbands. While the issue has been modified for other adults, many feminist scholars continue to argue that bodily autonomy of women is not equal to that of men. During the twentieth century, the U.S. Supreme Court emphasized bodily privacy rights in contrast to private property considerations. *Griswold v. Connecticut*, 381 U.S. 479 (1965) established that individuals have some guarantees of bodily privacy based on interpretations of the First, Fourth, and Fourteenth Amendments. But this has limitations as well. For example, the Court has appeared to use private property definitions at times and privacy issues at other times. The *Skinner v. Oklahoma* (1942) case establishing that reproduction is a right also determined that the state has a right to prevent procreation for those on public assistance. The boundaries between public and private control of the human body are not fixed, and judgments continue to be less systematically applied, particularly when minority groups (women, people of color, gays, lesbians, and transsexuals) are concerned.

Coerced or compulsory sterilization is a **birth control** practice most frequently associated with the eugenics movement, a social and medical movement designed to improve the quality of the overall population through reproductive controls. The movement's early twentieth-century objective was to eliminate social and biological problems such as poverty and birth defects through both positive and negative eugenic measures. Positive strategies included character and behavior training programs designed for Anglo Saxons (population augmentation). Negative strategies involved sterilization and immigration restrictions (population control). The movement occurred during a time of rapid industrialization, urbanization, and immigration, all of which contributed to the idea that the lower classes of society would outnumber the upper strata, presumably causing genetic deterioration.

Courts devised compulsory sterilization primarily for developmentally disabled persons but also targeted homosexual, indigent, deaf, blind, epileptic, criminal, and physically deformed populations. In addition, many leaders of the eugenics movement attempted to enlist government approval for sterilization on a much broader scale. By 1920, 10 states had legislated authority to sterilize certain individuals convicted of criminal offenses as well as those confined to asylums for the insane. In contrast to the larger scientific community, courts generally supported eugenics laws to protect **public health and safety**. Judicial advocates argued that genetic deterioration was an impending risk that warranted violation of civil liberties.

The U.S. Supreme Court decision *Buck v. Bell* (1927) was one of the most sweeping compulsory sterilization cases. Carrie Buck, a 17-year-old developmentally disabled girl, had been involuntarily committed to the Virginia Colony for the

Epileptic and Feeble-Minded. Judges permitted Ms. Buck's sterilization (without consent) by means of salpingectomy (tubal ligation). The logic behind the decision rested on the notion that she would endanger the general population by procreating if she was released. Attorneys for the state argued that her **family** presented a genetic predisposition for mental incapacitation, and sterilization was a reliable method of preventing further reproduction of the feeble-minded. The strong support for sterilization given by Supreme Court Justice Oliver Wendell Holmes, Jr., provided the justification for continued practices. As a result of this ruling, many states engaged in widespread compulsory sterilization practices, terminating these only when legislative incentives prohibited the practice. The original case, however, has never been reversed. The *Buck* case occurred in a cultural context of fear and intimidation of various minority groups as well as the expansion of state authority over private matters. More importantly, the case illustrates the tensions between the goal of individual bodily liberty and the state's right to impose restrictions through public health, social reform, or other political measures.

Although the eugenics movement was struck a serious blow when prominent Nazi officials revealed that their genocide policies were based on the logic and practice of sterilization techniques used in the United States, coercive sterilization was still performed in the United States until the 1970s, just in more subtle forms. For example, as part of their ongoing medical training, surgical residents performed tubal ligations on Hispanic women and radical hysterectomies on Native American women. Members of these groups were not informed about the nature of the procedures. In other situations, medical authorities denied African American welfare recipients obstetric care until they agreed to undergo sterilization procedures. Once the media exposed these practices, sterilization measures largely ended, and governors of the states involved issued public apologies.

Sterilization measures did not end completely, however; they were simply transformed into more surreptitiously manipulative techniques. Such was the case with the use and abuse of Norplant, the contemporary link to the eugenics movement. Introduced in 1991, Norplant is a progesterone-based contraceptive including six small cylindrical one-inch tubes that are implanted in a woman's upper arm by a medical practitioner. Each tube releases a dose of progesterone for five years. Boasting a 99 percent effectiveness rate, some policymakers refer to Norplant as a form of temporary sterilization since it can be reversed. Only traditional forms of sterilization are more effective. Since use of Norplant requires virtually nothing from the recipient as compared to other contraceptive measures, it appeared to be a liberating form of birth control. But within a year of its introduction, use of Norplant became the means by which the state attempted to reduce the reproductive choice of certain groups of women. Historically, sterilization rates have been consistently highest with African American, Native American, Puerto Rican, and poor women. It is these very populations that have been the primary targets for Norplant.

Once Norplant was introduced to the general population, various constituencies attempted to issue directives for its use. While studies revealed that medical professionals gave erroneous information to African American, Native American, Puerto Rican, and poor female clients, judicial advocates instituted more sweeping measures. Judges offered women convicted of child or drug abuse the choice of extended jail time or reduced jail time accompanied with the use of

Norplant. Policymakers in 13 states created bills designed to coerce women to use Norplant. Some bills provided that upon the birth of a child to a welfare recipient, the state would pose the choice of Norplant to prevent any further pregnancies or threaten loss of benefits. Others offered money, food, and clothing in return for using Norplant. Although none of the bills introduced was officially passed, that the measures were considered precariously links the contemporary political and social climate and practices to the larger historic arena of the eugenics movement.

The logic of the proposed legislation was genuinely flawed, since blatant stereotypes regarding welfare abuse-women on public assistance have more children, for example-were used as causes of societal problems. Further, mandating Norplant would not have been a solution to the problems of drug or child abuse. The link to sexism is striking since no such measures have ever been proposed for men convicted of drug abuse. The assumption that women were still the group solely responsible for birth control clearly bolstered the initiatives. Further, the high rates of sterilization of women of color, coupled with insufficient health care for that group, suggested not only population control, but institutional racism and sexism.

Most importantly however, sterilization use and abuse should not be limited to an analysis of civil liberties exclusively. The state defines the issue as an issue of rights: the right of the individual's personal liberty versus the right of the state to protect the larger well-being of society through health and safety regulations. However, this presents a significant contradiction. States also have attempted to prosecute individual women on the basis of fetal rights. A fetal right is a right for an unborn being whose existence is legally disputed. Yet if the state coerces administration of Norplant, then the fetus, the being whose existence is in legal limbo, will be prevented from coming into existence. So by preventing the existence of the unborn fetus, its nonexistence is ensured. Such practices underscore the fact that individual rights are not the primary concern; rather, social control issues are most relevant. As privacy interests are structured through race, class, **gender**, and sexuality, a policy designed exclusively around issues of privacy will most likely fail to address the full extent of coerced sterilization and other reproductive abuses against minority groups.

See also: **Privacy and inequality; Reproductive rights; Sex offenders; Women and privacy**

Suggested Reading: Curry, Lynne. *The Human Body on Trial: A Handbook with Cases, Laws and Documents*. Santa Barbara, CA: ABC-CLIO, 2002; Roberts, Dorothy. *Killing the Black Body: Race, Reproduction and the Meaning of Liberty*. New York: Vintage Books, 1997; Young, Margot E. "Reproductive Technologies and the Law: Norplant and the Bad Mother," *Families and Law* 21, no. 3-4 (1995): 259-281.

Sue E. Spivey

Stop and frisk

Despite Fourth Amendment protections against unreasonable searches and seizures, police officers may stop pedestrians and subject them to a "pat-down search" without a **search warrant** under certain circumstances. The process has come to be called a "stop and frisk."



The landmark case approving a stop and frisk search was *Terry v. Ohio*, 392 U.S. 1 (1968). In that case, the Court acknowledged that “we deal here with an entire rubric of police conduct—necessarily swift action predicated upon the on-the-spot observations of the officer on the beat—which historically has not been, and as a practical matter could not be, subjected to the warrant procedure. Instead, the conduct involved in this case must be tested by the Fourth Amendment’s general proscription against unreasonable searches and seizures.”

The Court went on to rule that for a warrantless stop to be constitutionally acceptable, “the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion.” The Court went on to suggest an objective test for review of an officer’s actions: “would the facts available to the officer at the moment of the seizure or the search ‘warrant a man of reasonable caution in the belief’ that the action taken was appropriate?”

Notice, there is nothing in the Court’s instructions about protecting a pedestrian’s expectations of privacy. Instead, the Court said there must be a balancing between “the need to search [or seize] against the invasion which the search [or seizure] entails.” The Court specifically held that “inarticulate hunches,” or good faith alone, would not be sufficient to justify a stop or a search. “If subjective good faith alone were the test, the protections of the Fourth Amendment would evaporate, and the people would be ‘secure in their persons, houses, papers, and effects,’ only in the discretion of the police.”

There are two elements to a stop and frisk: the stop and the search. Initially, the courts were quite strict in limiting the justifications for stopping citizens. Slowly, the courts adopted a more liberal “reasonable suspicion of criminal activity” test to justify the stops. Law enforcement agencies instructed police that justifiable reasons for a *Terry* stop included but were not limited to: (1) a person does not seem to fit in the neighborhood; (2) a person matches a description of a person known to be sought by law enforcement agencies; (3) a person is loitering, hanging around a set location with no clear purpose, or is acting strangely; and, (4) a person is running away from or is present in a crime-scene area.

There were still problems for police officers because many of the actions they believed were suspicious were activities engaged in by law-abiding citizens. Since Fourth Amendment rights apply only when there has been a seizure of a person, the courts began to focus on when a “seizure” had occurred in an effort to reduce the difficulties in analyzing the justification for a stop in the first place. The result was that the test became not why did the officer stop someone for questioning, but rather did the person who was stopped believe that leaving was possible.

The Court addressed the freedom to leave issue in *United States v. Mendenhall*, 446 U.S. 544 (1980). In that case, Sylvia Mendenhall was going from one plane to another in a Detroit airport when she was observed by Drug Enforcement Administration (DEA) agents, who believed she was acting suspiciously. The agents stopped her to request identification. When she produced a driver’s license in one name and an airplane ticket in another name, the officers asked her to accompany them to an office on another floor in the airport. She agreed. Once in the office, Mendenhall was asked if she would consent to a strip search. Again, she agreed. A female officer escorted Mendenhall to a restroom and conducted the search. Heroin

was found. Mendenhall later argued her stop in the airport and the later search violated her Fourth Amendment rights.

The Supreme Court found the stop did not amount to a “seizure” and stated,

We adhere to the view that a person is “seized” only when, by means of physical force or a show of authority, his freedom of movement is restrained. Only when such restraint is imposed is there any foundation whatever for invoking constitutional safeguards. The purpose of the Fourth Amendment is not to eliminate all contact between the police and the citizenry, but “to prevent arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals” (*United States v. Martinez-Fuerte*, 428 U.S. 543 (1976)). As long as the person to whom questions are put remains free to disregard the questions and walk away, there has been no intrusion upon that person's liberty or privacy as would under the Constitution require some particularized and objective justification.

When the initial contact between police and suspect is not on a street but in a bus or on a train, the freedom to leave question makes less sense. Thus, in *Florida v. Bostick*, 501 U.S. 429 (1991), the Supreme Court defined the appropriate question as “whether a reasonable person would feel free to decline the officers’ requests or otherwise terminate the encounter.”

Once a suspect has been stopped, there is no automatic right to frisk. Officers must have an articulable reason to justify the invasion of a person’s privacy. Concern about an officer’s safety or the safety of others must be established, but it is fairly easy for officers to legitimately make that claim. For example, when persons refuse to answer questions or attempt to leave and avoid the officer, those acts in themselves can justify a *Terry* search.

The *Terry* decision was limited to a search for weapons with the intent of protecting the safety of investigating officers. In 1993, however, the Supreme Court expanded the permissible scope of an officer’s seizure “if in the course of a weapons frisk, ‘plain touch’ reveals presence of an object that the officer has probable cause to believe is contraband, the officer may seize that object” *Minnesota v. Dickerson*, 508 U.S. 366 (1993). Ironically, in *Dickerson*, the Court rejected an officer’s seizure of a small plastic container, ruling the officer should not have continued his search by manipulating the container with his fingers while it was still in the defendant’s pocket since the officer had determined the suspect did not have a weapon.

The concept of a *Terry* search has also been extended by the courts to include items a person may be carrying if there is a “reasonable, articulable suspicion, premised on objective facts” that the items being carried contain contraband or evidence of a crime.

See also: **Automobile; Automobile search; Reasonable expectation of privacy; Strip search**

Suggested Reading: Amsterdam, Anthony G. “Perspectives on the Fourth Amendment,” *Minnesota Law Review* 58, no. 3 (1974): 349–447; Barteo, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black’s Law Dictionary*, 7th ed. St. Paul: West, 1999; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press,



2000; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

David J. Brown

Strip search

A strip search is a search of an individual by a law enforcement officer or other agent of government that requires the rearrangement or—more commonly—removal of some or all of the person’s clothing to permit the visual inspection of the body, especially the private parts—the genitals, anus, and breasts—for weapons, illegal goods (contraband), or evidence of a crime. A body cavity search, a variant of the strip search, involves the internal physical examination of body cavities, including (in unusual circumstances) internal organs. Strip searches constitute the most intrusive and dehumanizing type of search, and thus are among the most serious encroachments on personal privacy. Since most strip searches are conducted on people in police custody, it is in such situations that the practice most often comes into conflict with privacy rights.

Although strip searches of arrested individuals have a long history in Anglo-American law and were well established in the American colonies before their independence, the topic gained visibility and widespread public awareness only in the second half of the twentieth century. A number of reasons account for this. One was the enhanced consciousness of privacy rights in an era that first saw the Supreme Court recognize, in *Griswold v. Connecticut*, 381 U.S. 479 (1965), a constitutional right to privacy. Another was the greater importance given rights of those accused or convicted of crimes as part of the “due process revolution” of the 1960s. This was partly fueled by accusations that strip searches were often used to harass, intimidate, and humiliate **prisoners**. Also a factor was the greater prominence of the War on Drugs and the awareness that dealers and users could find ingenious ways of secreting controlled substances, money, or weapons within their bodies. A final factor was the sensationalistic media attention given to anything related to nudity.

Constitutional protections and regulation of strip searches are grounded in the Fourth Amendment’s prohibition against unreasonable searches. While much of Fourth Amendment jurisprudence has focused on questions surrounding the searching of areas such as **homes** and residences, offices, and **automobiles**, relatively less attention has been given to searches of the body, and many questions await full definition. Generally, the courts have upheld strip searches as searches “incident to arrest,” a major category of exceptions to the requirement of a **search warrant**.

The key Supreme Court decision involving strip searches was *Bell v. Wolfish* (1979). This case arose out of the overcrowded conditions and administrative practices, including strip searches, in New York City’s Metropolitan Correctional Center (MCC), particularly those practices affecting pretrial detainees. While

acknowledging the offensive character of strip searches, the Court also noted that those in custody, even if not convicted of a crime, have a “diminished” rather than **reasonable expectation of privacy**. In overturning a lower court decision that found the detainees’ rights had been violated, the Court refrained from laying down detailed rules for prison management and instead stated that a wide-ranging deference should be accorded to the judgment of correctional officials. Ultimately, it put forth a balancing test that pitted the individual prisoner’s reduced privacy interest against the state’s security interest in maintaining order and safety in the facility. In this context, it found the MCC’s use of strip searches was not unreasonable.

After *Bell*, the Supreme Court offered little guidance as to what might characterize an unreasonable strip search, although the Court left open the possibility that such a circumstance might exist. It fell to the state and lower federal courts to wrestle with the issue. Although not always consistent, a pattern did emerge. While continuing *Bell*’s deference toward penal authorities and upholding, for example, random strip searches of prison inmates, the courts have generally held that there must be some basis for strip searches of pretrial detainees, and that blanket provisions that all persons detained by police be strip searched regardless of the alleged offense or circumstance of arrest go too far. While some judges have argued in favor of a standard of probable cause that a strip search will uncover contraband or weapons, the most widely accepted standard is that of “reasonable suspicion”: an officer’s ability to articulate grounds for suspecting that a person might be secreting such material would be sufficient to justify a strip search. General circumstances in which strip searches might be justified include the following: when the person has been arrested for a crime that involves weapons, violence, force, or contraband; when the person has a record of a past arrest—even for a minor offense; when the person would be likely to remain in custody for some time; when the person would be likely to mingle freely with other prisoners; or, when the person has been deemed to be a danger to himself or others. A search warrant, of course, can also justify a strip search.

The courts also made it clear that otherwise constitutional searches could be conducted in a manner that would make them illegal. For example, the Chicago Police Department’s practice of strip searching all female suspects taken into custody while only frisking males was ruled unconstitutional in 1983. In other cases, persons arrested for minor offenses and lacking past arrest records of the sort that would arouse reasonable suspicion have been held to have been strip searched illegally.

The courts have established a variety of general rules that should apply to the manner of strip searches. Such searches should be done by officers of the same sex as the person being searched, officers of the opposite sex should not be present in the same space, and the space should itself offer protection from outside observation. Strip searches may be done in the field only in emergency circumstances. Moreover, records of strip searches should be kept, including the reasons for the search.

While the courts have labeled manual body cavity searches to be the most intrusive and invasive type of search, they have not consistently set a higher standard for them than the reasonable suspicion that would allow visual strip searches. However, they are more likely to require a search warrant, and most jurisdictions require that they be done by medical professionals.

As in other searches, one of the major sanctions against the abuse of strip searches is the exclusionary rule barring from court any evidence gained in an illegal search. Another recourse that has become increasingly common in challenging strip searches is to bring suit, sometimes as a class action. A number of well-publicized decisions have found in favor of those who had been subjected to strip searches. In 2004, for example, Sacramento County, California, agreed to pay \$15 million to some 16,000 people who had been illegally strip searched by the county sheriff's department from 2000 through 2003. Such suits have been especially common in challenging blanket strip search policies, and their success has had a significant impact in prompting law enforcement agencies to change their policies in the direction of more individualized criteria based on reasonable suspicion. The courts have generally been less likely, however, to find police or corrections personnel personally liable for illegal strip searches.

Law enforcement personnel continue to make widespread use of strip searches, adjusting their policies and practices to judicial interpretation. In addition to stressing that such searches are necessary to gathering evidence and keeping contraband and weapons out of jails and prisons, law enforcement personnel also hold that strip searches have a deterrent effect.

Although most strip searches and controversies involving them have originated in the criminal justice system, they sometimes occur in other spheres as well. One of these is in schools. School officials generally enjoy greater latitude in conducting searches than do police, and strip searches have sometimes been resorted to, especially in efforts to locate drugs or stolen property. Here, too, the increasing number of lawsuits has had a curbing effect. Some states, such as Iowa, have banned school strip searches entirely. Many districts have either banned them or greatly tightened the circumstances in which they can occur.

Some have predicted that new developments in imaging technology will make strip searches obsolete in the twenty-first century. While less intrusive **x-ray devices** may reduce the indignity and humiliation inherent in the process, it will not necessarily mean an increase in privacy.

Suggested Reading: Christianson, Scott. *With Liberty for Some: 500 Years of Imprisonment in America*. Boston: Northeastern University Press, 1998; Helmer, Gabriel M. "Strip Search and the Felony Detainee: A Case for Reasonable Suspicion," *Boston University Law Review* 81 (2001): 339–388; Plitt, Emory A., Jr. *Searches of Arrested Persons*. Americans for Effective Law Enforcement, www.aele.org. Online, December 2005; Schwartz, Barry. "Deprivation of Privacy as a 'Functional Prerequisite': The Case of Prison," *Journal of Criminal Law and Police Science* 63 (1972): 229–239; Shuldiner, Paul R. "Visual Rape: A Look at the Dubious Legality of Strip Searches," *John Marshall Law Review* 13 (1979): 273–303.

William C. Lowe

Surveillance

Perhaps it is fitting that the topic of surveillance, so shrouded in intrigue, is often ambiguous and misunderstood. One error involves the common tendency to see surveillance as the opposite of privacy. Another is to associate it only with government and with law and order activities in particular. Privacy and surveillance can be interwoven. Viewed in social process terms, they are different sides of the same

coin. Surveillance may be the means of crossing borders that protect privacy. This is illustrated by strong public concern with the nefarious and multifarious electronic, chemical, and database means of collecting **personally identifiable information** without the individual's knowledge and consent. Yet surveillance can also be the means of protecting privacy. Consider the passwords and audit trails required to use some databases, or the various defensive measures such as a perimeter video camera used to protect the **home**. Whether surveillance or privacy invasion is seen depends partly on the point of view taken.

When this duality is considered in the abstract, it is difficult to reach broad conclusions about the appropriateness of either surveillance or privacy. They can be socially desirable, as well as destructive. Surveillance can serve goals of protection, administration, rule compliance, documentation, and strategy, as well as goals involving inappropriate manipulation, restricted life opportunities, social control, and spying. Privacy can be central to an individual's dignity and liberty as well as to intimacy, honest communication, group borders, and democracy, but it can also hide socially destructive behaviors such as abuse within families and white collar crime.

With the development of new communication and **computer** technologies and new ways of living that increasingly rely on non-face-to-face forms of interaction, questions of personal information have taken on new social significance. The microchip and computer are central to surveillance developments and, in turn, reflect broader social forces set in motion with industrialization that involve empirical documentation, rationality, bureaucracy, and capitalism. The increased availability of personal information is one strand in the constant expansion of knowledge witnessed in recent centuries, and of the centrality of information to the workings of contemporary society.

The dictionary defines surveillance as "close observation, especially of a suspected person" or persons. Examples include an individual suspected of bank robbery who is discretely followed by police and is apprehended after robbing another bank, or the discovery that a leader of an anti-globalization protest movement is a police informer.

The above examples are instances of "traditional surveillance," and the dictionary definition fits. Yet it is too narrow. The focus of surveillance goes beyond suspects, crime, and national security. To varying degrees, surveillance is a property of any social system—from two friends to a workplace to a government. Examples of this understanding of surveillance include a supervisor monitoring an employee's productivity, a doctor assessing the health of a patient, a parent observing a child at play in the park, the driver of a speeding car asked to show a driver's license, or a voyeur. Each of these also involves surveillance.

Information boundaries and contests are found in all societies and in all living systems. Humans are curious and yet also seek to protect their informational borders, even as they must also reveal their information. To survive, individuals and groups engage in, and guard against, surveillance. Seeking information about others, whether within or beyond one's group, is characteristic of all societies, as are efforts to protect information. However, the form, content, and rules about information vary considerably. In the case of surveillance, for example, there are variations between relying on informers, intercepting smoke signals, taking satellite

photographs, gathering information from “cookies” placed on the computers of **Internet** users, or mapping the spread of a contagious disease. With respect to communicating information, there are differences between the expectation that close friends will share secrets, the varied **disclosure** notice and **Freedom of Information Act** requirements, and the expectations surrounding the **confidentiality** of sealed or classified records.

The traditional forms of surveillance contrast in important ways with what can be called the “new surveillance,” a form that became increasingly prominent toward the end of the twentieth century. The new social surveillance can be defined as “scrutiny through the use of technical means to extract or create personal or group data, whether from individuals or contexts.” Examples include the use of video cameras; computer matching, profiling and **data mining**; work, computer, and electronic location monitoring; **DNA** analysis; **drug testing**; brain scans for lie detection; various self-administered tests; and thermal and other forms of imaging to reveal what is behind walls and enclosures. The use of “technical means” to extract and create the information implies the ability to go beyond what is offered to the unaided senses or voluntarily reported. Much new surveillance involves an automated process that extends the senses and cognitive abilities through using material artifacts or software.

Using the broader verb “scrutinize” rather than “observe” in the definition calls attention to the fact that contemporary forms of surveillance often go beyond the visual image to involve sound, smell, motion, numbers, and words. The eyes do contain the vast majority of the body’s sense receptors, and the visual is a master metaphor for the other senses (e.g., saying “I see” for “I understand”). Yet the eye as the major means of direct surveillance is increasingly joined or replaced by other means. The use of multiple senses and sources of data is an important characteristic of much of the new surveillance.

Traditionally, surveillance involved close observation by a person, not a machine. But with contemporary practices, surveillance may be carried out from afar, as with satellite imaging or the remote monitoring of communications and work. Nor need it be done through close, detailed monitoring—much initial surveillance involves superficial scans looking for patterns of interest to be pursued later in greater detail. Surveillance has become both farther away and closer than previously. It occurs with sponge-like absorbency and laser-like specificity.

In a striking innovation, surveillance has also been applied to contexts (geographical places and spaces, particular time periods, networks, systems, and categories of person), not just to a particular person whose identity is known beforehand. Moreover, the new surveillance technologies are often applied categorically (e.g., all employees are drug tested or all travelers are searched, rather than those whom there is some reason to suspect).

Traditional surveillance often implied a noncooperative relationship and a clear distinction between the object of surveillance and the person carrying it out. In an age of servants listening behind closed doors, binoculars, and telegraph interceptions that separation made sense. It was easy to distinguish the watcher from the person being watched. In the new surveillance, with its expanded forms of self-surveillance and cooperative surveillance, the easy distinction between the agent and the subject of surveillance can be blurred.

In related forms, subjects may willingly cooperate by submitting to personal surveillance in order to have consumer benefits (e.g., frequent flyer and shopper discounts) or for convenience (e.g., access to fast-track lanes on toll roads for which fees are paid in advance). Implanted chips transmitting identity and location that were initially offered for pets are now available for their owners (and others) as well. In some work settings, smart badges worn by individuals do the same thing, although not with the same degree of voluntarism.

Beyond the individual forms, surveillance at an aggregate level is central to social management. The careful tracking of behavior through computer records (referred to by Roger Clarke as “dataveillance”) is believed to offer a more rational and efficient approach to social organization and control. The new surveillance relative to traditional surveillance has low visibility, or is often invisible. Manipulation as against direct coercion has become more prominent. Monitoring may be purposefully disguised as with a video camera hidden in a teddy bear or a clock. Or it may simply come to be routinized and taken for granted as data collection is integrated into everyday activities. For example, use of a credit card for purchases automatically conveys information about consumption, time, and location of the purchase.

With the trend toward ubiquitous computing, surveillance and sensors in one sense disappear into ordinary activities and objects, **automobiles**, **cellular telephones**, toilets, buildings, clothes, and even bodies. The relatively labor-intensive bar code on consumer goods that requires manual scanning may soon be replaced with inexpensive embedded **radio frequency identification (RFID)** computer chips that can be read automatically from short distances. The remote sensing of preferences and behavior offers many advantages, such as controlling temperature and lighting in a room or reducing shipping and merchandising costs, while also generating records that can be used for surveillance.

There may be only a short interval between the discovery of the information and the automatic taking of action. The individual as a subject of data collection and analysis may also become almost simultaneously the object of an intervention, whether this involves the triggering of an alarm or the granting (or denial) of some form of access, for example, the ability to enter through a locked door, use a computer, or make a purchase.

The new forms are relatively inexpensive per unit of data collected. Relative to traditional forms, it is easy to combine visual, auditory, text, and numerical data. It is relatively easier to organize, store, retrieve, analyze, send, and receive data. Data are available in real time, and data collection can be continuous and offer information on the past, present, and future, as through statistical predictions. Simulated models of behavior can then be created. The new surveillance is more comprehensive, intensive, and extensive. The ratio of what the individual knows about himself or herself relative to what the surveilling organization knows is changing dramatically.

I. Surveillance Structures and Processes

Surveillance can be analyzed by breaking it into components. These indicate where to look and what to measure. This can help in identifying the variation that is central to explanation, understanding, and evaluation. Structures that are fixed at one point in time (like a photograph) can be differentiated from processes that

involve interaction and developments over time (like a video). The next section considers some surveillance structures.

Organizational surveillance is distinct from the *non-organizational surveillance* carried on by individuals. As James Rules has noted, modern organizations are the driving forces in the instrumental collection of personal data. As organizations increasingly use personal data for what David Lyon calls social sorting, the implications for many aspects of life are profound, whether they involve work, consumption, health, travel, or liberty. At the organizational level, formal surveillance involves a *constituency*. This term is used broadly to refer to those with some rule-defined relationship or potential connection to the organization. This may involve formal membership or merely contact with the organization, as through renting a video or showing a passport at a border.

Organizations have varying degrees of internal and external surveillance. Erving Goffman has identified many kinds of employee or inmate monitoring, such as within “total institutions.” These offer examples of the *internal constituency surveillance* found in organizations. Here individuals “belong” to the organization in a double sense. First they belong as members. But they also in a sense are “belongings” of the organization. They are directly subject to its control in ways that non-members are not. Thus, there is a loose analogy to the ownership of property.

External constituency surveillance is present when those who are watched have some patterned contact with the organization, for example, as customers, patients, malefactors, or citizens subject to the laws of the state. Those observed do not “belong” to the organization the way that an employee or inmate does. Credit card companies and banks, for example, monitor client transactions and also seek potential clients by mining and combining databases. The control activities of a government agency charged with enforcing health and safety regulations is another example. In this case, the organization is responsible for seeing that categories of person subject to its rules are in compliance, even though they are not members of the organization. The same compliance function can be seen with nongovernmental organizations that audit or grant ratings, licenses, and certifications.

In the case of external *non-constituency surveillance*, organizations monitor their broader environment in watching other organizations and social trends. The rapidly growing field of business intelligence seeks information about competitors, social conditions, and trends that may affect an organization. One variant of this is **industrial espionage**. Organizational planning (whether by government or the private sector) also requires such external data, although this is usually treated in the aggregate instead of in personally identifiable form.

Personal surveillance, in which an individual watches another individual (whether for protection, strategic, or prurient reasons) apart from an organizational role, is another major form. It may involve *role relationship surveillance* as with **family** members (parents and children, a suspicious spouse) or friends looking out for and looking at each other (e.g., monitoring locations through use of a cell phone). Or it can involve *non-role relationship surveillance* such as in the free-floating activities of the voyeur whose watching is unconnected to a legitimate role.

With respect to the roles that are played, the *surveillance agent* (watcher/observer/seeker) can be identified. The person about whom information is sought is a *surveillance subject*. All persons can play both roles, although hardly in the same

form or degree. These roles may change depending on the context and over a person's life cycle; the roles are also sometimes blurred and may overlap.

Within the surveillance agent category, the surveillance function may be *central* to the role, as with police, **private investigators**, spies, work supervisors, and investigative reporters. Or it may simply be a *peripheral* part of a broader role whose main goals are elsewhere. Illustrative of this are check-out clerks who are trained to look for shoplifters, or dentists who are encouraged or required to report suspected child abuse when seeing bruises on a child's face.

A distinction rich with empirical and ethical implications is whether a situation involves those who are a party to the generation and collection of data (*direct participants*) or instead involves *third parties*. Third parties may legitimately obtain personal information through contracting with the surveillance agent (e.g., to carry out drug tests or to purchase consumer preference lists). Or information may be obtained because confidentiality has been violated by the agent, or because an outsider has obtained it illegitimately (e.g., **wiretapping**, hacking, corrupting those with the information).

The presence of third parties raises an important secondary-use issue: can data collected for one purpose be used without an individual's permission for unrelated purposes? In Europe the answer generally is no. In the United States, where a much freer market in personal information exists, there are fewer restrictions. Large organizations warehouse and sell vast amounts of very personal information, without the consent and with no direct benefit to the subject.

Surveillance can also be analyzed with respect to whether it is *nonreciprocal* or *reciprocal*. Surveillance that is reciprocal may be *asymmetrical* or *symmetrical* with respect to means and goals. In a democratic society, citizens and government engage in reciprocal, but distinct forms of mutual surveillance. Citizens can watch government through Freedom of Information Act requests, open hearings and meetings, and conflict of interest and other disclosures required as a condition for running for office. However, citizens can not legally wiretap, carry out Fourth Amendment searches, or see others' tax returns. In bounded settings such as a protest demonstration, there may be greater equivalence with respect to particular means; for example, police and demonstrators may videotape each other.

Agent-initiated surveillance, which is particularly characteristic of compliance checks such as an inspection of a truck or a boat, can be differentiated from *subject-initiated surveillance* such as submitting one's transcript, undergoing osteoporosis screening, or applying for a job requiring an extensive background investigation. In these cases, the individual makes a claim or seeks help and essentially invites, or at least agrees to, scrutiny.

With agent-initiated surveillance, the goals of the organization are always intended to be served. Yet this need not necessarily conflict with the interests of the subject—the protection offered by school crossing guards and the efficient library service that depends on good circulation records benefit the organization and the subject. Public health and medical surveillance have multiple goals, protecting the community as well as the individual. Efficiently run companies provide jobs and services. Providing a limited amount of personal information on a warranty form and having a chip record usage of an appliance, such as a lawn mower or a car, may

serve the interest of both consumers and businesses (e.g., being notified if the manufacturer finds a problem or offering proof of correct usage if the device fails).

Subject-initiated surveillance may reflect goals that serve the interests of the initiator, but they often overlap the goals of the surveilling organization. Examples include some protection services that have the capability to remotely monitor home and business interiors (video, audio, heat, gas, motion detection) or health systems for the protection of the elderly and ill (e.g., an alarm is sent if the refrigerator of a person living alone is not opened after 24 hours). Since these are forms of surveillance more likely to involve informed consent, these are less controversial than secretly generated agent surveillance. What is good for the organization may also be good for the individual, although that is not always the case and depends on the context.

II. Surveillance Processes

Rather than being static and fixed at one point in time, surveillance can be viewed as a fluid, ongoing process that involves interaction and strategic calculations over time. Part of the fascination with the study of surveillance lies in its dynamic nature, as groups in conflict relationships reciprocally and continuously adjust their tactics to each other. Here the moral ambivalence that infuses the topic as a result of conflicting values and social interests can also be seen.

The *myth of surveillance* involves creating and sustaining the belief through the mass media that a technique is omnipresent and omnipotent. When such literal watching (whether real or metaphorical) is not possible, there is an effort to create uncertainty about whether or not surveillance is present. This is presumed to be a deterrent. However, in a complex world of conflicting interests, unexpected developments, and technology that breaks, perfect knowledge and control are rarely possible. New conditions may appear and efforts to resist surveillance are common.

A number of *behavioral techniques of neutralization*—strategic moves by which subjects of surveillance seek to subvert the collection of personal information. Among these are direct refusal, discovery, avoidance, switching, distorting, countersurveillance, cooperation, blocking and masking. Responses to drug testing illustrate most of these.

One type of response is *refusal*—just saying no or feigning an inability to offer the sample in spite of trying. Social systems often leak, and the date of a supposed random or surprise test or search can sometimes be inferred involving a *discovery* move. Employees may receive notice of a test. Such foreknowledge permits *avoidance* moves involving abstinence, the hiding or destroying of incriminating material, not going to work on that day, or leaving early because of illness. With *switching*, drug-free urine (whether purchased commercially in liquid or powdered form, or obtained from a friend) replaces the person's own urine. *Distorting responses* (e.g., diuretics and commercially available detox products) manipulate the surveillance-collection process such that while offering technically valid results, invalid inferences are drawn. Given empathy and the multiplicity of actors and interests in complex organizations, various *cooperative* moves in which controllers aid those purportedly controlled may also be seen.

Countersurveillance involves an ironic turning of the tables in which the very technologies used to control others come to be used to advance the interests of those controlled. Thus, when facing a urine drug test, employees can first experi-

ment at home, testing themselves with a variety of readily available products like those used in the official test. The wide availability of new tools such as covert audio and video recording offers the surveilled the chance to turn the usual stratification tables. The resulting data can be used defensively or to coerce those in positions of authority since there is the potential, for example, for the documentation of unwanted sexual advances and police abuse.

Another set of processes involves decisions about whether or not to surveil, and if so which technique to use, how to apply it, and to whom (e.g., to everyone, randomly, or selectively based on criteria). In addition, decisions need to be made about: whether or not the surveilled are to be informed of and have any say in the process or in how the data are used; who will have access to the data; what the degree of security will be; and, how long the data will be kept. The social scientist seeks to identify and explain these patterns and their prior correlates.

Such decisions have consequences. Subsequent developments can be contingent on the choices made. For example, some techniques that can be narrowly applied, such as the use of DNA for identification purposes, will require the creation of large databases against which a sample can be compared. A decision to watch everyone (categorical suspicion) avoids claims of discrimination in targeting, but it is more expensive and can lead to widespread feelings of privacy invasion.

Another aspect of process involves the path or “career” of surveillance events. In many, perhaps a majority, of cases, no action follows from surveillance because nothing of interest is discovered. The surveillance is intended to serve a scarecrow function or simply to generate a documentary record. Information may be saved until it is needed or a critical amount has been obtained. Or occasionally, too much is discovered to act on, or the surveilled can exert counterpressure to prevent action from being taken.

Yet techniques, too, have careers. The surveillance appetite can be insatiable and often shows a tendency to expand to include new goals, agents, subjects, and forms. Awareness of this requires asking of any new tactic, regardless of how benignly its means and ends are presented, where might it lead? The expansion of a technology introduced in a limited fashion can often be seen. Extensions beyond the initial use, whether reflecting *surveillance creep* or, in many cases, *surveillance gallop*, are common. There may be new uses for the data. For example, the **Social Security number** that Congress intended only to be used for tax purposes has become a de facto national ID number, and video cameras once restricted to prisons and high-security areas, are now found in offices, shopping malls, and homes.

New surveillance agents and subjects may appear. A common process is a progression from use on animals to prisoners, criminal suspects, noncitizens, the ill, children, and then throughout the society. Tactics developed by government for defense and law enforcement often spread to manufacturing and commercial uses, and then to uses in interpersonal relations by friends, family, and others. One example of this trend is the expansion of drug testing from the military to sensitive categories such as transportation workers to the workforce at large, and then even to parents who test their children. The patterning of the use of global positioning satellite data is equivalent. Yet expansion is only one path. A technique may be developed but not widely used; for example, this has been the case with handwriting analysis (graphology) in the United States, although not in France. Or if adopted, a

tactic may diffuse slowly rather than rapidly throughout the social order. Television, for example, had been available since the late 1920s, decades before it came into widespread use.

Sometimes a rarely studied phenomenon of *surveillance contraction* occurs. Widely used tactics may come to be less used as a result of political controversy, the development of regulations, and unintended consequences, or as a result of the development of better tactics. For example, congressional legislation in 1988 severely restricted the use of the polygraph for employment purposes.

III. What Is to Be Done?

Social understanding and moral evaluation require attending to the varied contexts and goals of surveillance. The many settings, forms, and processes of surveillance preclude any easy explanations or conclusions. Two broad, contrasting views of the new surveillance can be identified. A pessimistic Frankensteinian/Luddite view holds that surveillance technology is inhuman, destructive of liberty, and untrustworthy. In addition, since surveillance technology develops out of an inequitable social context, it is seen as likely to reinforce the status quo.

A more optimistic view places great faith in the power of technology, which is seen to be neutral. More powerful surveillance tools are seen as necessary in today's world, where efficiency is so valued and where there is a multiplicity of dangers and risks. Surveillance is a sword with multiple edges. The area is fascinating precisely because there are no easy scientific or moral answers.

There are value conflicts and ironically conflicting needs and consequences, all of which make it difficult to take a broad and consistent position in favor of, or against, expanding or restricting surveillance. For example, society values both the individual and the community. Members of society want both liberty and order. Individuals seek privacy and often **anonymity** but also know that **secrecy** can hide dastardly deeds, and visibility can bring accountability. Although individuals value freedom of expression, too much visibility may inhibit experimentation, creativity, and risk taking.

As with any value-conflicted and varied-consequence behavior, particularly those behaviors that involve conflicting rights and needs, it is essential to keep the tensions ever in mind and to avoid complacency. Occasionally, when wending through competing values, the absolutist, no compromise, don't cross this personal line or always cross it standard is appropriate. But more often compromise—if rarely a simplistic perfect balance—is required. When privacy and civil liberties are negatively affected, it is vital to acknowledge, rather than to deny this impact, as is so often the case. Such honesty can make for more informed decisions and also serve an educational function.

Surveillance practices are shaped by **manners**, organizational policies, laws, and by available technologies and countertechnologies. These draw on a number of background value principles and tacit assumptions about the empirical world that need to be analyzed. Whatever action is taken, there are likely costs, gains, and trade-offs. At best we can hope to find a compass rather than a map, and a moving equilibrium rather than a fixed point for decisionmaking. The following questions (Marx, 2005) can help.

Questions for Judgment and Policy Regarding Surveillance

1. *Goals*: Have the goals been clearly stated, justified, and prioritized?
2. *Accountable, public, and participatory policy development*: Has the decision to apply the surveillance technique been developed through an open process and, if appropriate, with the participation of those to be surveilled? This involves a transparency principle.
3. *Law and ethics*: Are the means and ends not only legal but also ethical?
4. *Opening doors*: Has adequate thought been given to precedent creation and long-term consequences?
5. *Golden rule*: Would the watcher be comfortable with being the subject rather than the agent of surveillance if the situation were reversed?
6. *Informed consent*: Are participants fully apprised of the system's presence and the conditions under which it operates? Is consent genuine—beyond deception or unreasonable seduction—and can participation be refused without dire consequences for the person?
7. *Truth in use*: Where personal and private information are involved, does a principle of unitary usage apply, in which information collected for one purpose is not used for another? Are the announced goals the real goals?
8. *Means-ends relationships*: Are the means clearly related to the end sought and proportional in costs and benefits to the goals?
9. *Can science succeed?* Can a strong empirical and logical case be made that a means will in fact have the broad positive consequences its advocates claim? Does the system or technique really work?
10. *Competent application*: Even if it works in theory, does the system (or operative) using it apply it as intended?
11. *Human review*: Are automated results with significant implications for life chances subject to human review before action is taken?
12. *Minimization*: If risks and harm are associated with the tactic, is the tactic applied to minimize these, displaying only the degree of intrusiveness and invasiveness that is absolutely necessary?
13. *Alternatives*: Using a variety of measures, not just financial ones, are alternative solutions available that would meet the same ends with lesser costs and greater benefits?
14. *Inaction as action*: Has consideration been given to the “sometimes it is better to do nothing” principle?
15. *Periodic review*: Are regular efforts made to test the system's vulnerability, effectiveness, and fairness and to review policies?
16. *Discovery and rectification of mistakes, errors, and abuses*: Are there clear means for identifying and fixing these and, in the case of abuse, applying sanctions?
17. *Right of inspection*: Can individuals access and challenge their own records?
18. *Reversibility*: If evidence suggests that the costs outweigh the benefits, how easily can the surveillance be stopped? What is the extent of capital expenditures and available alternatives?
19. *Unintended consequences*: Has adequate consideration been given to undesirable consequences, including possible harm to watchers, the watched, and third parties? Can harm be easily discovered and compensated for?
20. *Data protection and security*: Can surveillants protect the information they collect? Do they follow standard data protection and information rights as expressed in the Code of Fair Information Protection Practices and the expanded **European Data Protection Directive**?



A central point of much social and legal analysis is to call attention to the contextual nature of behavior. Certainly these questions and the principles implied in them are not of equal weight, and their applicability will vary across time periods, depending on need and perceptions of crisis, across contexts (e.g., public order, health and welfare, criminal and national security, commercial, private individuals, families, and the defenseless and dependent), and particular situations within these. Yet common sense and common decency argue for considering them.

Suggested Reading: Allen, Anita. *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability*. Lanham, MD: Rowman and Littlefield, 2003; Bennett, Colin, and R. Grant (eds.). *Visions of Privacy*. Toronto: University of Toronto Press, 1999; Brinn, David. *The Transparent Society*. New York: Perseus, 1999; Clarke, Roger. "Information Technology and Dataveillance," *Communications of the ACM* 31 (1988): 498–512; Ericson, Richard, and Kevin Haggerty. *Policing the Risk Society*. Toronto: University of Toronto Press, 1997; Foucault, Michael. *Discipline and Punish: The Birth of the Prison*. New York: Pantheon, 1977; Gandy, Oscar. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press, 1993; Gilliom, John. *Overseers of the Poor*. Chicago: University of Chicago Press, 2001; Goffman, Erving. *Asylums: Essays in the Social Situation of Mental Patients and Other Inmates*. Garden City, NY: Anchor Books, 1961; Lyon, David. *The Electronic Eye: The Rise of Surveillance Society*. Polity, 2001; Lyon, David (ed.). *Surveillance as Social Sorting*. London: Routledge, 2003; Marguilis, Steven T. (ed.). "Contemporary Perspectives on Privacy: Social, Psychological, Political," *Journal of Social Issues* 59 (2003): 243–261; Marx, Gary. "Seeing Hazily (but not Darkly) through the Lens: Some Recent Empirical Studies of Surveillance Technologies," *Law and Social Inquiry* 30 (2005): 339–399; Marx, Gary. *Windows into the Soul: Surveillance and Society in an Age of High Technology*. Chicago: University of Chicago Press, forthcoming; Rule, James. *Private Lives and Public Surveillance: Social Control in the Computer Age*. New York: Schocken Books, 1974; Solove, Daniel. *The Digital Person*. New York: New York University Press, 2004; Staples, W. *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. Lanham, MD: Rowan and Littlefield, 2000; Tunnell, Kenneth. *Pissing on Demand*. New York: New York University Press, 2004; Zureik, Elia, and M. Salter. *Global Surveillance and Policing*. Devon, UK: Wilan, 2005.

Gary T. Marx

Surveillance cameras

Surveillance cameras are ubiquitous. The use of closed-circuit television (CCTV) to monitor locations around the world has exploded during the last decade. The United Kingdom (UK) leads the world in the deployment of CCTV technology in public spaces. According to researchers, the number of surveillance cameras in private premises in London alone is estimated to be around 500,000. This tally brings the total number of private and public cameras in the UK to approximately 4,285,000. The network of cameras is so dense—1 camera for every 14 people—that in many urban areas people may be monitored and filmed as often as 300 times per day.

Although the use of CCTV technology in the United States is less prevalent than in the United Kingdom, it is steadily increasing. For example, in 2002 the U.S. National Park Service installed surveillance cameras around national monuments in Washington, D.C. Other cities including Baltimore, Chicago, and New Orleans have installed camera surveillance networks with financing from the federal government, including from the Department of Homeland Security (DHS). Chicago added 2,250 cameras to its Homeland Security Grid financed by a \$5.1 million grant from DHS. These cameras are linked to a \$43 million operations center constantly monitored by police officers. Baltimore used federal grants to finance camera purchases and its \$1.3 million Watch Center. A 1,000-camera surveillance system is expected to be fully deployed by the end of the year as a result of federal dollars being spent in New Orleans.

As of October 1999, there were an estimated one million video cameras in operation in the United States for the purpose of promoting public safety and security. In 1998, New York Civil Liberties Union volunteers conducted a project to produce a comprehensive map of public and private surveillance cameras in Manhattan. The group reported 2,397 CCTVs with only 55 cameras in use by the Department of Transportation as part of their vehicular traffic control system. Minneapolis and Washington, D.C., have conducted similar projects. Although no one tracks actual numbers of surveillance cameras in the United States, the Carnegie Mellon Data Privacy Lab estimates there are 10,000 publicly available online webcams displaying public places in the United States.

Silent videotape **surveillance** is largely ungoverned by statute. Courts have held that silent video surveillance even without the knowledge of those videotaped is not covered under the **Electronic Communication Privacy Act of 1986** (ECPA). Silent video surveillance is not an aural transfer because it does not involve a human voice and therefore is not regulated under the legislation. There are almost no federal regulations, state statutes, or express statutory provisions regarding the interception of nonverbal video surveillance.

In addition to the federal government, some states such as Missouri and Washington provide a limited restraint to video surveillance. Specifically, they have adopted statutes prohibiting the use of video surveillance for the purposes of peeping or **voyeurism**. The federal Video Voyeurism Prevention Act of 2003 makes it a crime to capture an improper image of an individual if the perpetrator knowingly does so under circumstances violating the privacy of that individual. Currently under consideration is legislation attempting to include mobile **cellular telephone** camera videos within the federal bill because of the enormous growth in the mobile personal communication industry. Cell phones with camera capabilities soared in popularity from under 9 million shipped to the United States during 2003, to 27 million in 2004. The number is expected to reach 100 million in 2008 (*PC World*, 2004).

Cameras are used routinely in public places to deter shoplifting, to prevent crime and terrorism, and to record illegal acts. Persons in public venues are not the only objects for the camera. Items, activities, and events are all subject to the scrutinizing eye of video surveillance, no matter how seemingly remote the public location appears. In *California v. Ciraolo*, 476 U.S. 207 (1986), the Supreme Court held that a police aerial observation made from an altitude of 1000 feet of a **home**

where marijuana cultivation was suspected did not violate the Fourth Amendment because private and commercial flights in the public airways are routine; therefore, it was unreasonable to expect constitutional protection. In domestic settings, CCTV use is usually legally acceptable; courts have found no invasion of privacy by cameras in most areas of a home. For instance, in *State v. Diaz* (1998), the use of so-called nanny cameras was found not to violate privacy rights. However, in cases such as *Miller v. Brooks* (1996), the use of cameras in places where a person has a **reasonable expectation of privacy**, such as a **restroom** or bedroom, were found to violate privacy statutes or to be a tortious invasion of privacy.

In *United States v. Knotts*, the Supreme Court found no expectation of privacy when the government attached a radio-tracking device to a canister of chemicals subsequently traced to the defendant's house. Specifically, the Court held that a person traveling in an **automobile** on public thoroughfares has no reasonable expectation of privacy in his or her movements from one place to another. Surveillance is acceptable in virtually all places where a potential for visual observation exists.

With video recording by the government virtually unregulated, except under basic Fourth Amendment protocol, people are concerned that privacy outside the home is becoming extinct. To that end, the federal government, through the National Institute of Justice (NIJ), has funded research into the use of CCTV cameras to monitor public spaces. Furthermore, the trade organization for security professionals, ASIS International, commissioned the Carnegie Mellon Data Privacy Lab to assess the number and nature of webcams that observe people in public spaces. Ultimately, the goal is to analyze and propose related policies and best practices for the security industry that measure the relationship between technology and privacy.

The bounds of CCTV are constantly being widened to include additional purposes. Originally installed to deter theft and monitor traffic (for example as **red-light and speeding cameras**), their use has expanded to include detecting undesirable behavior such as public order transgressions to deter violence and vandalism in public parks. CCTV is becoming an integral part of a government's crime-control policy and social-control theory. It is promoted as a primary solution for urban dysfunction. The technology has had a dramatic impact on the evolution of law enforcement policy. In Britain, for example, CCTV is the single most heavily funded crime prevention measure, accounting for three-fourths of the total spending on crime prevention by the Home Office.

Despite the explosive growth in video surveillance, concerns exist within the public arena regarding the implications of CCTV use on privacy rights as well as on civil rights. It is also a matter of debate whether CCTV use reduces or deters crime. Some governmental uses of the technology spark little controversy, such as CCTV use in correctional facilities. Other uses, however, raise serious constitutional privacy concerns. Even though the effectiveness of these cameras in identifying crime and terrorist activities and their efficiency as a deterrent and deployment tool are still debatable, CCTV proponents seem to be gaining support. The displacement of crime to a different location is one factor that clouds the findings of the study. The Electronic Privacy Information Center (EPIC), a watch group for privacy concerns, reports that although millions are spent on CCTV systems, studies show that they have little effect on criminal activity.

EPIC also reports that studies show that there is a serious risk of racial profiling and discrimination with the use of camera surveillance networks. EPIC members are concerned that the homeland security camera systems will be misused or abused. Numerous examples of abuse are already on record, such as the situation of the manager of a Florida newspaper, who extended a legitimate system to include a hidden video camera in the employee bathroom. A second example of abuse occurred when employees of Dunkin' Donuts used the company's video and audio surveillance technology to listen in on customers. In addition, a JC Penney employee discovered that a guard was showing a videotape in which he had zoomed in on her breasts using the store's ceiling cameras. In England, B-grade filmmakers raided footage from public video cameras to make risqué movies featuring unsuspecting persons. With the increase in CCTV use, coupled with new technology making these cameras active as opposed to passive viewing vessels, instances of abuse could grow exponentially.

The technological changes related to CCTVs in the first five years of this century are remarkable. Remote-controlled CCTV cameras can be made to pan, tilt, and zoom in on specific activities or items. Newer cameras also have night-vision capabilities and wireless technologies. A full range of viewing, recording, and storage connections can be integrated with the cameras. Digital video recorders developed for use with CCTV surveillance systems have hard drive capacities to store up to 10 weeks of recording with retrieval and video content analysis.

Other technological developments include the conversion from analog to digital and the development of smart cameras with event detection and notification for networked video systems. Object tracking, another new innovation, enables a viewer to follow a subject from camera to camera in order to monitor the target of interest even when the target moves through the field of view. There are also advances in imaging with reduction of field pattern noises, remote streaming video recording, and viewing capability from handheld devices. Cyber Bug, a three-pound, pilotless aircraft drone designed for **airborne surveillance and intelligence** and operated by remote control, sends streaming video to military officers on the ground. The Coast Guard is developing similar drones that can be launched vertically and that will provide 16 continuous hours of surveillance. Other improvements include wireless connectivity and access through the **Internet**, cost reductions, outdoor automatic day/night adjusting cameras, and tapeless systems that allow storage capacities in excess of one million gigabytes.

The change from analog to digital devices and the ease of video enhancement for clarification purposes create a new set of issues relating to abuse and privacy implications. Historically, when a convenience store surveillance camera caught a crime on video, the analog tape was seized as evidence, and the item was admitted if properly authenticated. Now, the first question raised is what must be seized as evidence: the digital recording produced off the hard drive of a **computer** or the hard drive itself. Each time a digital image is created in a new format, it has the potential to be altered. Thus, a new field of science known as forensic video analysis has emerged. Forensic video analysis is the scientific examination, comparison, and evaluation of video in legal matters. A lack of legal precedent and scientific authority exists within this novel field, so the extent to which a recognized expert

can clarify, enhance, reproduce, and accurately retrieve information is all relatively new and uncharted territory.

Although forensic video comparison evidence analysis is a relatively new field, the use of comparison evidence in many other scientific disciplines is widely accepted. Comparison evidence has been used in the area of **fingerprint** analysis, **DNA** examination, footwear and hand print comparison, facial mapping, and ear prints. Comparison evidence is also used in tool-mark identification, firearm and bullet matching, paint chemistry matching, duct tape matching, and drug sampling. It is also used in questioned document, fiber, and hair examinations. The technical basis for all comparison evidence requires the identification and analysis of (1) a class characteristic (an identifiable feature that assists in narrowing down the statistical probability that a person or object belongs to the same group as a known person or object that shares the same features) and (2) a unique characteristic (identifiable features found on a specific person or object that are found on no other person or object of a similar class). For example, a forensic video analysis of car headlight spread can be performed since all cars display unique headlight patterns. Questions as to potential tampering, best evidence (hard drive versus a digital reproduction), and the use of comparison analysis by a reverse projection image method are current concerns. Furthermore, questions related to time-lapse photography, compression and scan conversion processes, aspect ratio to calibration, and issues concerning retrieval of digital information in remote storage (particularly storage outside of the United States) highlight additional evolving issues.

The government does not provide the only threat to privacy in this regard. Private citizens and business are using CCTV technology to protect themselves, to monitor specific activities, or to send images via their mobile camera phones. Concerns regarding the enactment and application of new regulations merit serious attention in the future. In addition, the government's acquisition of privately recorded CCTV data for law enforcement purposes needs further scrutiny.

Suggested Reading: Carnegie Mellon Data Privacy Lab. *Surveillance of Surveillances*. privacy.cs.cmu.edu/dataprivacy/projects/. Online, November 2005; Electronic Privacy Information Center (EPIC). *Observing Surveillance Project*. www.observingsurveillance.org. Online, November 2005; EPIC. *A Review of Current Research into the Effectiveness of CCTV Systems in Reducing Crime*. <http://www.epic.org/privacy/surveillance/spotlight/0505/nacro02.pdf>. Online, November 2005; EPIC. *Spotlight on Surveillance: Facial Recognition Systems Have an Ugly Effect on Personal Privacy*. www.epic.org/privacy/surveillance/spotlight/1105/. Online, November 2005; McCahill, Michael, and Clive Norris. *CCTV in London: On the Threshold to Urban Panopticon? Analyzing the Employment of CCTV in European Cities and Assessing Its Social and Political Impacts*. www.urban-eye.net/results/ue_wp6.pdf. Online, November 2005; Minneapolis Surveillance Camera Project. www.mpls-watched.org. Online, November 2005; NYCLU Surveillance Camera Project. www.mediaeater.com/cameras/overview.html. Online, November 2005; Pompano, Angelo J. *Privacy in the Age of Video Surveillance: This Is Not Your Father's Candid Camera*. Yale-New Haven Teachers Institute, yale.edu/ynhti/curriculum/units/2000/3/00.03.05.x.html#f. Online, November 2005; U.S. Department of Justice. *CCTV: Constant Cameras Track Violators*, 2002. www.ncjrs.org/pdffiles1/jr000249d.pdf. Online, November 2005; U.S. Gen-

eral Accounting Office. *Video Surveillance Information on Law Enforcement's Use of Closed Circuit Television to Monitor Selected Federal Property in Washington D.C.* Report to the Chairman, Committee on Government Reform, House of Representatives, www.gao.gov/atext/d03748.txt. Online, November 2005.; Welsh, Brandon C., and David P. Farrington. *Crime Prevention Effects of Closed Circuit Television: A Systematic Review*. Home Office Research Study 252. (2002). www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf. Online, November 2005.

Jill Joline Myers

T



Telecommunication Act of 1996

The U.S. Congress passed the Telecommunication Act of 1996 on February 1, 1996. The act rewrote the Communications Act of 1934 and aimed to foster fair competition by deregulating the telecommunication industry. Section 222 of the act, entitled “Privacy of Customer Information,” states that telephone carriers have an obligation to protect the **confidentiality** of information relating to their customers and requires carriers to obtain customer consent for the use, **disclosure**, and access to Customer Proprietary Network Information (CPNI).

CPNI is data on individual calling behaviors, such as frequency, location, duration of calls, and types of services subscribed to by the individual customer. Telephone companies collect this information to establish customer profiles for billing and marketing purposes. CPNI is potentially detrimental to privacy because it infringes on one’s right not to be monitored and on one’s control of personal information. Since CPNI is a powerful source for the telecommunication industry for identifying potential customers and designing marketing strategies, it may also violate the individual rights of solitude and **anonymity**.

Section 222 lists three tiers of customer information and corresponding protections. Customer approval is not required for customer list information (name, address, and telephone number) used to publish directories. Carriers can also disclose anything that does not constitute **personally identifiable information** without consent so long as the disclosure is made on reasonable and nondiscriminatory terms. Nevertheless, any access or disclosure of individual CPNI requires prior approval from the identified individual. Congress was vague in stipulating how companies should obtain such approval.

On February 19, 1998, the Federal Communications Commission issued an order requiring carriers to notify their customers about their right to control the use of their CPNI and to obtain their **opt-in** consent before accessing customer information outside the range allowed under Section 222. The FCC’s interpretation of Section 222 is to protect consumer privacy and to engineer a regulatory framework that promotes competition by limiting the ability of large carriers to monopolize the use of CPNI. The incumbent carrier, therefore, could not market products for different services to which a customer did not apply, but could market its products



within existing service relations. The telecommunication industry soon contested that the order was impermissible regulation of commercial speech and in violation of the First Amendment.

In August 1999, the U.S. Court of Appeals for the Tenth Circuit ruled in *U.S. West v. FCC* that the FCC's interpretation of Section 222 was in violation of the First Amendment. Circuit Judge Tacha stated that the First Amendment protects the right both to disseminate and to receive information, and a ban on either component of communication is a restriction on free speech. The court further used the precedent of the 1979 Supreme Court case of *Smith v. Maryland* to reason that CPNI privacy rights are not self-evident, recognized rights under the protection of the Fourth Amendment. The FCC, therefore, could not favor individual privacy over protected commercial speech.

The FCC responded in 2002 by stating that either "opt-in" or "opt-out" customer consent could be used for the collection of CPNI. The Cellular Telecommunications and Internet Associations issued a "consumer code" in September 2003 for self-regulatory measures to protect consumer privacy.

See also: Cable Communications Policy Act of 1984

Suggested Reading: Cate, Fred H., Robert E. Litan, Peter J. Wallison, and Michael Staten. *Financial Privacy, Consumer Prosperity, and the Public Good*. Washington, DC: Brookings Institute, 2003; Gandy, Oscar. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press, 1993; Smith, Jeff H. *Managing Privacy: Information Technology and Corporate America*. Chapel Hill: University of North Carolina Press, 1994; Sparks, Shaun. "Opting In Is Out: Balancing Telecommunications Carrier Commercial Speech Rights with Consumer Data Protection," *International Journal of Communications Law and Policy* 5 (Summer 2000); U.S. Congress, *Joint Explanatory Statement of the Committee of Conference on the Telecommunication Act of 1996*, 104th Cong., 2d sess., 1996, S. Doc. 652.

Kuoray Mao

Telemarketing

Although telemarketing is often narrowly defined as marketing by telephone, it is used here in a broader context to include any form of unsolicited selling message targeted at individual consumers from a distance. Telemarketing includes direct mail, telephone marketing, commercial **electronic mail** (i.e., "**spam**"), and messages sent to **cellular telephones**, facsimile machines, and **computer** screens. It does not include mass media advertising or passive marketing messages, such as billboards and **Internet** sites, nor does it include personal selling.

Telemarketing raises two major privacy concerns. The first involves the collection and sale of **personally identifiable information** to make targeting individual consumers possible. The second concerns the intrusive nature of telemarketing. Unlike passive marketing messages, which are relatively easy for consumers to ignore, telemarketing requires consumers to deal, in some manner, with each message. Telephone marketing causes the telephone to ring, and today often requires that the consumer delete any message from voicemail or an answering machine. Unwanted e-mail and messages to cell phones must be deleted, and direct mail and

fax messages must be thrown away. Thus, telemarketing imposes higher costs in terms of consumer time and, sometimes, financial disposal costs than passive marketing. Only personal selling, with the salesperson's proverbial foot in the door, is more intrusive for consumers. However, some consumers find telemarketing to be a convenient form of purchasing, and marketers use it because they hope it is more engaging than passive marketing.

Telemarketing began with direct-mail advertising in the nineteenth century. At first, the mailed circulars were of poor print quality, but improved printing technology made catalogs and other more attractive solicitations possible. Consumers also complained of receiving duplicate mailings. This led to the refinement of mailing lists of potential consumers. By 1900, mailing lists were being compiled from directories, newspaper clipping services, and other public sources and sold by categories, such as address or occupation. "Addressing companies" were available to perform direct-mail campaigns, including printing and addressing the advertising material. The **U.S. Postal Service** encouraged the growth of direct mail by offering lower postal rates. Even the mandate to use ZIP codes in 1967, initially opposed by marketers, proved to be an important market segmentation tool. Today about 40 percent of all mail is direct-mail advertising. It is estimated that half of direct mail is never even opened by recipients.

There is virtually no regulation of direct mail in the United States despite the cost of disposal and the fact that consumers spend about eight months of their lifetimes disposing of direct mail. Customers may refuse delivery of materials they declare to be obscene and require such mailers to stop mailing such materials to them (39 U.S.C. §3008-12). It also is illegal to send unsolicited merchandise through the mail and then request payment (39 U.S.C. §3009). Consumers may treat such merchandise as a gift. Consumers do not have to pay to return the item but may bear the costs of disposing of it.

Direct mail is relatively easy to ignore, but for many consumers a ringing telephone is not. In 1991, when enacting the federal Telephone Consumer Protection Act (TCPA), Congress heard evidence that more than 300,000 telephone solicitors contacted more than 18 million Americans every day. In 1998, the Direct Marketing Association estimated that U.S. marketers spent \$62 billion in telephone marketing. Others estimate that telephone marketers must make 50 or more calls to make a sale, but sales from such calls amount to roughly 30 percent of all telephone purchases, or about \$100 billion in 2002. A 2004 survey by the Ponemon Institute found that 60 percent of consumers find telemarketing annoying.

Under federal law, telephone solicitations may occur only between the hours of 8:00 a.m. and 9:00 p.m. for the recipient of the call. Telephone marketers may not harass consumers by repeatedly calling or using obscene or intimidating language. They also must identify themselves as sellers and explain that they are making a sales call before beginning their sales pitch (16 C.F.R. §310). This rule was amended in 2003 to establish the federal **Do-Not-Call Registry**. By March 2005, some 84 million phone numbers had been registered to prevent unsolicited calls from for-profit marketers, including those that solicit charitable contributions. While this list does not preempt the do-not-call lists that 27 states had previously established, several states are consolidating their lists with the federal registry. New amendments also require the transmission of caller identification by the telemarketer



and regulate call abandonment, which occurs when a consumer answers the telephone but there is no marketer on the line.

Because consumers pay for fax paper and often pay for incoming cell phone calls, the TCPA also prohibits solicitations to telephone fax machines without prior consent of the receiver and solicitations made to cell phones by automatic dialing devices without prior consent (47 C.F.R. 64). The Junk Fax Prevention Act of 2005 (47 U.S.C. §227) requires commercial faxes to properly identify the sending company and its phone number as well as provide a notice on how to **opt-out** of future faxes from that firm. It does allow companies to fax customers with whom they have an existing business relationship.

The latest effort to impose marketing costs on consumers without procuring their consent is through e-mail and the Internet. The federal Can Spam Act of 2003 (15 U.S.C. §7701) explicitly preempted tougher state laws to authorize the sending of commercial e-mail as long as the header and subject lines are not misleading and the message discloses the identity of the seller and the fact that it is an advertisement and gives recipients a method of opting out of receiving future e-mails from that marketer. A list of one million e-mail addresses costs as little as \$7, making this a very low-cost marketing medium. Studies show that roughly half of all e-mail traffic is spam, and it costs U.S. business about \$10 billion each year to deal with spam. The Federal Trade Commission has opposed establishing a Do-Not-Spam registry because it believes it would be ineffective, but case law does allow Internet Service Providers to offer spam filters.

As noted previously, marketing calls to cell phones made by an automatic dialing device are illegal without prior permission of the recipient. The question arises whether this also includes text messages, which also cause cell phones to ring. In September 2005, the Arizona Court of Appeals held that computer programs that send text messages by generating a list of text addresses are automatic dialing devices under the TCPA, making the practice illegal. The court further noted that the Can Spam Act prohibits unsolicited commercial messages to mobile service devices.

Finally, Internet users can receive targeted pop-up advertising messages when “surfing” the web. This usually occurs when the consumer’s computer contains “adware” that may simply send advertisements periodically. Some “adware,” however, follows the consumer’s search patterns and attempts to send advertising of interest to the consumer. Furthermore, some search engines sell search terms to advertisers and then display the advertisers’ ads either as a pop-up ad during the search or as a “sponsored result.” The legality of these practices is being considered on two fronts. First, the FTC has pursued firms that do not clearly disclose they are loading “adware” onto consumers’ computers or mislead consumers about the characteristics of the software they are receiving. Second, trademark owners are suing firms that offer their trademarks for sale to other advertisers. Only a few conflicting judicial decisions have been issued thus far on these practices.

Marketers typically have challenged these regulations as violating their free speech rights under the First Amendment. However, courts have found consumer intrusion to be a significant regulatory interest and held that the regulations enacted to date are constitutional. The courts typically examine whether the regulations are narrowly tailored to achieve the regulatory interest and whether alternative channels for the speech are still available.

The first privacy concern listed previously, the collection of personal information in order to target messages, has received relatively little legal attention in the United States. Specific federal laws have been enacted to regulate privacy for websites that seek personal information from children and to protect financial and health care personal information. In addition, the FTC and other agencies pursue cases where firms release or sell personal data in violation of their stated privacy policy. However, no overall privacy protection for personal information exists at the federal level. The U.S. approach is in contrast with that of the European Union. The **European Data Protection Directive** on the Legal Protection of Databases (96/9/EC), adopted in 1996, instructed member states to enact legislation requiring that consumers be informed and consent before companies may collect personal information about them for a database. They must be informed of the database, have the right to correct or delete inaccurate data, and have the right to object to its use for marketing purposes. Europe also has rejected the U.S. piecemeal approach to dealing with intrusion. The 2005 Directive Concerning Unfair Business-to-Consumer Commercial Practices (2005/29/EC) requires member states to enact laws by early 2008 that will prohibit persistent and unwanted solicitations by any remote media without prior consent or the ability to object easily and without cost to stop future solicitations.

Suggested Reading: Ayers, Ian, and Matthew Funk. “Marketing Privacy,” *Yale Journal on Regulation* 20 (2003): 77–137; Cain, Rita Marie. “Federal Do-Not-Call Registry Is Here to Stay: What’s Next for Direct Marketing Regulation?” *Journal of Interactive Marketing* 19 (2005): 54–62; Federal Trade Commission. www.ftc.gov/privacy. Online, February 2006; Petty, Ross D. “Marketing without Consent: Consumer Choice and Costs, Privacy, and Public Policy,” *Journal of Public Policy & Marketing* 19 (2000): 42–53.

Ross D. Petty

Telephone. See *Bartnicki v. Vopper*, 532 U.S. 514 (2001); *Brandeis, Louis D. (1856–1941)*; *Olmstead v. United States*, 277 U.S. 438 (1928); *Wiretapping*

***Terry v. Ohio*, 392 U.S. 1 (1968)**

Terry v. Ohio was a landmark Supreme Court case in which the Court ruled there was no violation of Fourth Amendment privacy rights in allowing police officers to stop and “pat down” persons on the street when the officers have reason to believe they may be dealing with “armed and dangerous” persons. The officer “need not be absolutely certain that the individual is armed; the issue is whether a reasonably prudent man in the circumstances would be warranted in the belief that his safety or that of others was in danger. And in determining whether the officer acted reasonably in such circumstances, due weight must be given not to his inchoate and unparticularized suspicion or ‘hunch,’ but to the specific reasonable inferences which he is entitled to draw from the facts in light of his experience.”

John Terry and Richard Chilton were standing on a street corner in Cleveland, Ohio, in October 1963, when an off-duty police detective observed them. Although he could not say precisely why, he thought the two men looked suspicious. Therefore, he hid by a store some 300 to 400 feet away and watched them. Terry and Chilton appeared

agitated. Terry walked down the street, looked in a store window, and then returned to where Chilton was standing. Then Chilton went to look in the same window and returned to where Terry was standing. This routine was repeated multiple times. At one point they were met by a third man, who spoke with them for a while and left. The separate trips to the store window resumed.

Eventually, Terry and Chilton left their position on the street corner and walked in the same direction the third man had gone. The detective followed. The officer testified later that he believed the men had been “casing a job, a stickup” and thought they might have guns. Terry and Chilton eventually met the third man again, and the detective decided to confront the three men.

The detective approached the men, identified himself as an officer, and asked their names. The three men mumbled a response. When he failed to get a clear response, the detective grabbed Terry and turned him around so he was facing his friends and was between his friends and the detective. At that point, the officer patted down Terry and felt a handgun, but could not get the gun free.

The detective then ordered the three men to enter the store they were in front of and to face the wall with their hands in the air. He removed Terry’s coat, took out the handgun, and then patted down the men, searching for weapons. Chilton had a revolver in his pocket. The third man had no weapons. The officer never put his hands inside the men’s pockets or coats except to remove the handguns. Terry and Chilton were arrested and charged with carrying concealed weapons.

Terry and Chilton asked the trial court to suppress the evidence (the weapons) seized during the police search. The motion was denied, and they were convicted. The Ohio appellate courts confirmed the convictions and the trial court’s refusal to suppress the evidence. The case was argued in the Supreme Court on December 12, 1967.

In an 8-to-1 decision, Justice Douglas dissenting, the Court addressed several pivotal legal issues that have led to a substantial body of law allowing stops and searches in a variety of contexts. Ironically, the Court affirmed the stop and search of Terry and Chilton after reaffirming that they both could rely on the protections of the Fourth Amendment as they “walked down the street in Cleveland.” The men had a **“reasonable expectation of privacy”** since the amendment protects people and not places. The question for the Court became whether the stop and search of the two men was reasonable under the circumstances because “what the Constitution forbids is not all searches and seizures, but unreasonable searches and seizures.”

To reach its decision, the Court had to determine whether the brief stop of the two men constituted a “seizure” that would call for Fourth Amendment protections. The answer was easy. The Court noted, “It must be recognized that whenever a police officer accosts an individual and restrains his freedom to walk away, he has ‘seized’ that person.”

The next question was whether the “pat down” was a search. The Court was nearly contemptuous of the state of Ohio’s argument that the search was a mere “petty indignity” that citizens should be required to endure: “[I]t is nothing less than sheer torture of the English language to suggest that a careful exploration of the outer surfaces of a person’s clothing all over his or her body in an attempt to find weapons is not a ‘search.’ Moreover, it is simply fantastic to urge that such a procedure performed in public by a policeman while the citizen stands helpless, perhaps facing a wall with his hands raised, is a ‘petty indignity.’ It is a serious

intrusion upon the sanctity of the person, which may inflict great indignity and arouse strong resentment, and it is not to be undertaken lightly.”

The next question became the reasonableness of the officer’s actions under the circumstances. The Court adamantly restated its holdings that, whenever possible, officers must obtain warrants before conducting searches. In those instances, the requirement for probable cause set forth in the Fourth Amendment must be met. However, the Court found this situation was different: “We deal here with an entire rubric of police conduct—necessarily swift action predicated upon the on-the-spot observations of the officer on the beat—which historically has not been, and as a practical matter could not be, subjected to the warrant procedure.” Thus, the Court held, the actions did not require “probable cause”; rather, they must be considered in light of what is reasonable and what is not.

The Court required a balancing test to be applied. The officer’s “need to search” had to be balanced “against the invasion which the search (or seizure) entails.” Thus, to justify an officer’s search or seizure, the Court ruled the officer “must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion.” More simply, the Court suggested one test for reasonableness would be whether “the facts available to the officer at the moment of the seizure or the search ‘warrant a man of reasonable caution in the belief’ that the action taken was appropriate.” In establishing this threshold, the Court rejected the notion that an officer’s own subjective justification for a search or seizure should be sufficient: “Good faith on the part of the arresting officer is not enough. If subjective good faith alone were the test, the protections of the Fourth Amendment would evaporate, and the people would be ‘secure in their persons, houses, papers, and effects,’ only in the discretion of the police.”

For Terry and Chilton, the Court found the government has a legitimate interest in preventing, detecting, and investigating crime and in “the appropriate circumstances and the appropriate manner” in which an investigating officer may stop a pedestrian for questioning, even when there is no probable cause for an arrest. The men’s actions were sufficiently suspicious to warrant the detective’s stop.

The question then became whether there was any justification for the search. At that point, the governmental interest was in protecting the officer’s safety. The Court noted the history of violence against police officers and stated:

In view of these facts, we cannot blind ourselves to the need for law enforcement officers to protect themselves and other prospective victims of violence in situations where they may lack probable cause for an arrest. When an officer is justified in believing that the individual whose suspicious behavior he is investigating at close range is armed and presently dangerous to the officer or to others, it would appear to be clearly unreasonable to deny the officer the power to take necessary measures to determine whether the person is in fact carrying a weapon to neutralize the threat of physical harm.

After setting out these parameters, the Court ruled there needed to be a “narrowly drawn authority” for an officer to search for weapons in order to protect that officer’s safety, or other officers’ safety, when the officer believes the suspect may be armed. “The officer need not be absolutely certain the individual is armed; the issue is whether a reasonably prudent man in the circumstances would be warranted in the belief that his safety or that of others was in danger.”

The Court then determined the detective's suspicions were reasonable. The scope of the search was appropriate. Thus, the weapons seized could be admitted as evidence against the men without violating their Fourth Amendment protections.

Subsequent cases focused on what could be seized during the *Terry* **stop-and-frisk** situation. Early on, the Court developed rules to allow the removal of any item of the size and shape of a weapon, but not allow the seizure of items, such as plastic bags containing pills, that clearly were not weapons. The courts then expanded rulings to allow admission of items officers had probable cause to believe were contraband.

Also at issue after *Terry* was the question of when a person had been "seized" as a result of an officer's conduct. This was a critical point, because the protections of the Fourth Amendment do not come into play until there is a "seizure." The standard has evolved to the point where the courts now ask if "in view of all the circumstances surrounding the incident, a reasonable person would have believed that he was not free to leave." The "free to leave" standard was then subsequently reduced further to "free not to answer questions" when the Court allowed officers to stop a bus and question all the passengers on the bus without a warrant.

In the term following *Terry*, the Supreme Court decided *Chimel v. California*, **395 U.S. 752 (1969)**, and ruled that when an arrest is made, it is reasonable for the arresting officer to search "the arrestee's person and the area 'within his immediate control'—construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence." The Court reasoned, "A gun on a table or in a drawer in front of one who is arrested can be as dangerous to the arresting officer as one concealed in the clothing of the person arrested."

In *New York v. Belton*, 453 U.S. 454 (1981), the *Terry* concept was extended again. The Court explained that the concept of "within a person's immediate control" had not been successfully defined. Thus, to provide a "workable rule," it held that "articles inside the relatively narrow compass of the passenger compartment of an **automobile** are in fact generally, even if not inevitably, within 'the area into which an arrestee might reach in order to grab a weapon.'" Applying the rules governing search incident to arrest, the Court also ruled that police could examine the contents of any open or closed container found within the passenger compartment, "for if the passenger compartment is within the reach of the arrestee, so will containers in it be within his reach."

The concept of a *Terry* protective search was extended in 1983 from on-the-street confrontations between police and suspects, or searches of occupied automobiles, to searches of unoccupied stopped cars. In *Michigan v. Long*, 463 U.S. 1032 (1983), the Supreme Court ruled that a warrantless protective search of a car's unoccupied interior was acceptable. In that case, although the driver was outside the car, an officer had searched the interior of the car after seeing a hunting knife on the floor. During the search, marijuana was found, and the driver was charged with possession. The Court ruled:

Our past cases indicate then that protection of police and others can justify protective searches when police have a reasonable belief that the suspect poses a danger, that roadside encounters between police and suspects are especially hazardous, and that danger may arise from the possible presence of weapons in the area surrounding a suspect. These principles compel our conclusion that the search of the passenger

compartment of an automobile, limited to those areas in which a weapon may be placed or hidden, is permissible if the police officer possesses a reasonable belief based on “specific and articulable facts which, taken together with the rational inferences from those facts, reasonably warrant” the officer in believing that the suspect is dangerous and the suspect may gain immediate control of weapons.

The concept was further extended to the **home** in *Maryland v. Buie*, 494 U.S. 325 (1990). There, the Court approved a police “protective sweep” of a residence and held,

We conclude that the Fourth Amendment would permit the protective sweep undertaken here if the searching officer “possesse[d] a reasonable belief based on ‘specific and articulable facts which, taken together with the rational inferences from those facts, reasonably warrant[ed]’ the officer in believing,” *Michigan v. Long* (1983) (quoting *Terry v. Ohio*, 392 U.S. 1, 21 (1968)), that the area swept harbored an individual posing a danger to the officer or others.

Today the courts seem reluctant to limit the warrantless search of persons or places provided police have articulable reasons to suspect that they, or others, might be in danger if the search does not occur. There have been limitations, however. A police search of a suspect’s backpack was ruled improper because police had seized the backpack and the suspect could not gain access to it. The courts also have ruled that finding facts sufficient to justify a stop *after* making the stop is not sufficient to justify making the stop in the first place. An anonymous tip based on a suspicion that a person possibly possesses drugs is insufficient basis for a reasonable suspicion on the part of a police officer. Also, signs of nervousness beyond the norm cannot be the foundation for an officer’s reasonable suspicion. Finally, prior criminal history alone is not a sufficient justification for a warrantless stop.

See also: Automobile search; Cady v. Dombrowski, 413 U.S. 433 (1973); *Carroll v. United States*, 267 U.S. 132 (1925); **Constitutional protections; Search warrant; Schmerber v. California, 384 U.S. 757 (1966); *South Dakota v. Opperman*, 428 U.S. 364 (1976)**

Suggested Reading: Black, Henry C. *Black’s Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Connor, Gregory J., and Douglas R. Mitchell. *Terry Stops: Legal Perspectives/Tactical Procedures*. Champaign, IL: Stipes, 2000; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

David J. Brown

Thermal sensors

A thermal-imaging device, often called a FLIR (forward-looking infrared radar), is used to detect activity and movement via heat patterns on the surface of a selected target by identifying temperature differentials. The device provides a visual image of objects that are warmer or cooler than the baseline. A thermal imager is capable of locating a human in the dark from a distance in excess of



seven kilometers. Although thermal-imaging devices are incapable of seeing through an object, activity or hot spots may be detected if heat from the activity passes through an intermediate object, such as a window or a porous wall.

Thermal imagers are prized commodities that have been applied in a variety of circumstances. The U.S. Border Patrol uses the device for military **surveillance** and detection of illegal immigrants. FLIRs have been used to save persons trapped in smoke-ridden buildings as well as many other search-and-rescue operations. The imager has assisted in locating countless individuals, including missing children, lost Alzheimer's patients, fleeing suspects, and escaped convicts. The devices are often used in drug cases to locate hydroponic laboratories. As a result of the refined sensibility of the equipment, the devices have been used recently to detect and identify emissions and air pollutants that are harmful to the environment.

The usefulness of the technology cannot be denied. These devices allow law enforcement to collect otherwise unavailable information passively without a physical intrusion. Thus, for the most part, the suspect has no knowledge that the equipment has been used. Because thermal imagers operate by observing and recording waste heat radiated through the surface of a structure, concerns were raised that Fourth Amendment privacy protection would be analogized to a **garbage** search inquiry approved by the Supreme Court in 1988 in *California v. Greenwood*. The concern centered on the collection of private information without notice, as well as the acquisition of confidential data in areas where privacy is highly protected like within a residence. Although the FLIR technology supposedly cannot penetrate walls, it actually does to a certain extent. Without adequate control, this infrared technology could allow the government to search and survey, violating the right to privacy.

The issue is temporarily resolved by the 2001 Supreme Court decision in *United States v. Kyllo*. In *Kyllo*, the litigants debated whether the information retrieved by a thermal imager scan was collected through the wall of a home or abandoned property or from heat emanating from the exterior of the home's walls. The Court, however, sidestepped that debate and focused its decision instead on how the thermal imager was used under the *Katz v. United States* two-pronged test. First, did the person have an actual subjective **reasonable expectation of privacy**? Second, was that expectation one that society was prepared to recognize as reasonable? The Court concluded that Kyllo did have a subjective expectation of privacy in the heat emissions within his home since the technology had the potential of revealing more than the contraband hydroponic marijuana-growing operation. Protected information, such as when the lady of the house was bathing, could also be revealed. Furthermore, the subjective privacy expectation was one that society would be willing to recognize. This latter conclusion was reached on the basis that thermal imagers are not devices commonly available to the public. Hence, the interiors of houses are off limits to any technology, no matter how unobtrusive the technology may be, if the technology is not in general use. This decision offers minimal or temporary protection to privacy advocates since new technology is a continuing phenomenon and more technology is being made available to the public.

Suggested Reading: Bolkcom, Christopher. *Unmanned Aerial Vehicles and Border Surveillance*. CRS Report for Congress. <http://www.fas.org/sgp/crs/homesecl/>

RS21698.pdf. Online, April 2006; FLIR Systems. *EPA Purchases New Infrared Camera to Detect Hazardous Air Pollutants That Cause Health Risks and Environmental Dangers; State Regulatory Agencies and Refineries and Other Industrial Corporations Follow Suit*. <http://www.flirthermography.com>. Online, April 2006; Schwab, Jay, "New Athens Chief Gets Training with Thermal Camera," *Belleville (Ill.) News Democrat* (September 28, 2005). <http://www.belleville.com/mld/newsdemocrat/12760442.htm>. Online, September 2005.

Jill Joline Myers

***Time, Inc. v. Hill*, 385 U.S. 374 (1967)**

On September 11 and 12, 1952, three escaped convicts held James Hill, his wife, and their five children hostage for 19 hours in their **home** in Whitemarsh, Pennsylvania. The convicts were subsequently involved in a highly publicized encounter with the police, and two of the three convicts were killed. The Hill family quickly became front-page news. James Hill stressed that none of them had been hurt, molested, or exposed to violence and discouraged any further coverage of their story. The family moved to Connecticut soon after.

In the spring of 1953, Joseph Hayes published a novel entitled *The Desperate Hours*, in which a family of four is held hostage by three escaped convicts in their suburban home. Unlike the Hill family's experience, the story's family is exposed to violence by the convicts. The father and son are beaten, and the daughter experiences verbal sexual insult. The book was later made into a play, also entitled *The Desperate Hours*.

Time, Inc.'s *Life* magazine printed an article about the play, calling it a reenactment of the Hill incident. The article appeared in *Life* in February 1955. It was titled "True Crime Inspires Tense Play," with the subtitle "The ordeal of a family trapped by convicts gives Broadway a new thriller, 'The Desperate Hours.'" The text of the article reads, "Three years ago Americans all over the country read about the desperate ordeal of the James Hill family, who were held prisoners in their home outside Philadelphia by three escaped convicts. Later they read about it in Joseph Hayes's novel, *The Desperate Hours*, inspired by the family's experience. Now they can see the story reenacted in Hayes's Broadway play based on the book."

The article also used photographs of scenes that had been staged in the Hill's former home. The pictures included a reenactment of the son being roughed up by one of the convicts, labeled "brutish convict"; a picture of the daughter biting the hand of a convict to make him drop a gun, captioned "daring daughter"; and one of the father throwing his gun through the door after a "brave try" to save his family is foiled. The appellee, James Hill, alleged that the *Life* article gave a knowingly false impression that the play was an accurate depiction of the Hill incident. Hill sued *Life* magazine for damages under a New York statute that provides a cause of action to a person whose name or picture is used by another without consent for purposes of trade or advertising. *Life* magazine, the appellant, claimed that the article was about a subject of general interest and was published in good faith.

The jury awarded James Hill \$50,000 compensatory and \$25,000 punitive damages. On appeal, the Appellate Division of the Supreme Court ordered a new trial



as to damages but sustained the jury verdict of liability. At the new trial on damages, a jury was waived, and the court awarded \$30,000 compensatory damages without any punitive damages. The court did not feel that James Hill's private life had been intruded on and did not feel that Time, Inc. published the article for financial gain. Time, Inc. was still found liable, but the court felt the damages awarded to Hill were excessive. The court declined to hold the New York "Right of Privacy" statute unconstitutional. The court concluded that the instructions to the jury were fatally defective because they failed to advise that a verdict for the plaintiffs could be predicated only on a finding of knowing or reckless falsity in the publication of the *Life* article. The court explained that absent a finding of such malicious intent on the part of a publisher, press statements are protected under the First Amendment, even if they are otherwise false or inaccurate.

See also: Associated Press v. Walker, 388 U.S. 130 (1967); *Bauer v. Kincaid*, 759, F. Supp. 575 (1991); *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975); *Journalism; Red & Black Publishing Co. v. Board of Regents*, 262 Ga. 848 (1993); *United States v. Caldwell*, 408 U.S. 665 (1972)

Suggested Reading: Barteo, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Goodale, James C. *Communications Law*. New York: Practising Law Institute, 1999; Sullivan, Kathleen M., and Gerald Gunther. *First Amendment Law*. St. Paul, MN: West, 1998; Tedford, Thomas L., and Dale A. Herbeck. *Freedom of Speech in the United States*, 5th ed. State College, PA: Strata, 2005.

Sarah K. Parkinson

Transaction-generated data

In the contemporary world of commerce, from grocery store to the **Internet**, all legal transactions between buyers and sellers are recorded. A transaction may be conceptualized as the exchange of one value for another (e.g., money in exchange for a good). In the marketplace, payment increasingly occurs through **credit cards** or **digital cash**, and record-keeping practices assume the form of electronic/digital data. Therefore, the consumer represents not only a potential buyer, but also a source of data. Practices of documentation constitute a form of consumer **surveillance** carried out by private, for-profit organizations—whether the organization is a third party or the actual seller. Data collection in seemingly simple exchanges “captures” **personally identifiable information** (e.g., telephone number, ZIP code) unnecessary for the purposes of the immediate transaction. Through the collection and collation of extensive personal information, private corporations can create consumer profiles to inform business strategy. In response to the burgeoning use of surveillance techniques in economic transactions, particularly with respect to e-commerce, Americans report in a number of surveys (e.g., 1997 Privacy and American Business Survey and a 2001 Harris Interactive Survey) that they feel as if they have lost control over the use of their personal information. They also interpret these practices as an encroachment on individual privacy.

The contemporary collection and collation of personal information through economic transactions is more extensive and intensive than in the past. The extensiveness

of this surveillance results from bureaucratic organizations formally tracking an increasing number and range of individual behaviors. In principle, the systematic record keeping of economic transactions represents one of the oldest practices of human civilization, preceding even literacy. For example, the Inca Empire used a system of knotted cords. The Roman Empire mastered systematic written record keeping, which the Church perpetuated in a less organized fashion through medieval Europe. With the rise of the nation-state and the expansion of capitalist markets, record keeping rationalizes economic transactions with more methodical accounting practices, and bureaucratic organizations control a greater proportion of daily life. The intensity of consumer surveillance is apparent in the expanding quantity and precision of data generated and integrated per transaction. In the United States, the sociohistorical roots of this mushrooming can be identified after World War II. Three conditions essential for the proliferation of personal data collection systems include new technologies, government policy, and market forces.

The role of computer and telecommunication technologies in introducing more intense surveillance technologies is widely recognized. The effect of **computers** on economic record keeping has been widely discussed in academic literature, public policy, and business circles since the early 1970s. Computers transform record keeping into data processing. The translation of personal information “captured” through exchange into an electronic format facilitates the collection, storage, analysis, retrieval, and mobility of consumer data: computer software automates record keeping for bureaucratic organizations. By the 1960s, automatic data processing had dramatically reduced the cost and revolutionized the possibilities of the record-keeping practices that had been used for thousands of years. Telecommunication technologies also facilitated the adoption of electronic exchange (e.g., credit cards and debit cards), which also supports consumer surveillance. A contemporary example illustrates the effect of new technologies on economic transactions. When a consumer calls a toll-free business number, software systems can automatically access a customer profile before the operator answers the phone. That profile can include data that are internal to the company (e.g., billing records) or external, such as “lifestyle data,” which might indicate the place of residence, estimations of home value, and annual income. Not only do such data open or close possibilities in the relationship between a particular customer and enterprise, but the outcome of the interaction feeds back into that profile to affect subsequent interactions.

U.S. government policy has helped facilitate the heightened surveillance of consumer behavior. In the postwar era, the federal government has consistently financed technological innovation from the earliest and crudest computers to the Internet. For example, the **United States Census** offers geographic and social data to myriad private companies for commercial exploitation. The ZIP Code Improvement Plan and the 911 emergency system standardized addresses, making residential information more user-friendly and marketing techniques, such as direct mailing (i.e., “junk mail”), more affordable. In the 1970s, the Claritas corporation capitalized on these federal subsidies by pioneering a data-processing method known as geodemographics, a body of analytic techniques that identify neighborhoods and households by lifestyle categories to predict consumer behavior and reach niche markets. Geodemographics merges spatial and demographic information with data from more than 500 million consumer purchases per year. This research classifies

the American public into 62 distinct lifestyle “clusters”—each associated with distinct tastes, values, and living arrangements.

Aside from subsidizing the cost of data collection, the rollback of the social safety net—witnessed in the United States and most industrialized nations since the 1960s—helps assign a greater value to personal information. Private providers, free from any burden of offering universal access (e.g., insurance companies), assume the responsibilities of public bureaucracies. These economic actors compile personal information to sort the profitable clients from the risky clients. This “risk society” further entrenches the drive to classify and categorize the population based on its revenue-generating capacity. In this sense, cuts to social entitlements aid in the creation of consumer data markets. In a more direct fashion, the government helps create these markets by purchasing the services of **data brokers** like Claritas. State agencies use “cluster” data to design and administer programs, such as antismoking campaigns. In total, more than 15,000 nonprofit organizations, government agencies, political parties, and private firms rely on the services of Claritas. The accumulation and organization of personal data foster the development of new campaigns, the introduction of new product lines and services, and the location and design of new facilities.

The collection and collation of personal information from economic transactions represents a growing sector in the economy. At the close of the twentieth century, the production and analysis of transaction-generated data had become a \$10 billion/year industry. The emergence of the data-brokering industry underscores the importance of market mechanisms in the intensification of consumer surveillance. In the marketplace, the demand for personal information stems from the need of businesses to acquire accurate information regarding the environments in which they act. Information that is more precise gives a firm a competitive advantage over others. In other words, knowledge of individual customers and potential customers serves the organizational goal of profitability. Thus, as the cost of data collection, storage, and analysis falls because of new technologies and federal subsidization, private firms seek greater quantities and better quality of personal information. Precise, reliable, and valid personal information enables companies to identify the most profitable clients and devise appropriate goods, services, and marketing strategies. Conversely, the collation of transactions into databases, such as “Consumer Return Databases,” allows retailers to isolate less attractive customers, such as those who chronically complain or return items, and develop methods of exclusion (e.g., “digital redlining”).

The strategic interests of private enterprises have spawned a market where data abstracted from the lives of individuals become a commodity. A handful of corporations dominate this industry and own unimaginable sums of personal information. A company called Acxiom has acquired personal data on virtually every consumer in Australia, the United Kingdom, and the United States. However, more traditional merchants participate in personal-data markets by selling their customers’ information for supplemental revenues. Publishing companies, who have sold magazine subscriber lists for decades, were among the first to realize this opportunity. More recently, financial institutions have learned of these income-generating possibilities. In search of these auxiliary revenues, traditional companies stress data

collection in what business observers call the “second exchange.” The “first exchange” consists of the transaction of a good or service for payment, and in the “second exchange” the consumer offers personal information for discounts or special offers. Mail-in warranties represent a typical second transaction, and one-third of U.S. households have filed such warranties. Supermarket loyalty cards constitute another form. With loyalty cards, consumers must disclose significant amounts of personal information to be eligible for store discounts, and retailers use such cards to track all purchases back to the person. While this arrangement may initially appear to be a fair deal since the consumer gains a reward for the loss of privacy, a 2003 study by the *Wall Street Journal* on loyalty cards demonstrates that they do not actually lower prices. They create the appearance of lower prices, but in reality, the discounts simply offset price hikes. In effect, consumers must foreclose more personal information to maintain pre-loyalty card prices.

The combination of more extensive economic transactions and more intensive record keeping engenders what legal scholar Arthur R. Miller calls a “data-mania.” Apologists of consumer surveillance celebrate the democratizing effect of systems like geodemographics, in which the cluster purportedly overcomes distinctions of race, gender, and class in the marketplace. These enthusiasts tout “data-mania” as a new era of efficiency and represent data collection and collation as a matchmaking process. Critics of “data-mania” point to the erosion of personal privacy. Accounts in the mainstream media discuss a limited set of implications that include identity theft and telemarketing annoyances, but scholarly critics call attention to social power. The asymmetrical flows of information immanent in these new record-keeping practices empower private corporations at the expense of the individual. When transaction-generated data permit companies to sort consumers into groups of assigned worth or risk, new forms of discrimination, such as “digital redlining,” become possible. Thus, the clusters and individual profiles compiled from abstract electronic data have very real effects on the life chances of flesh-and-blood persons.

See also: **Banking and financial records; Credit rating; Data mining**

Suggested Reading: Culnan, Mary J., and Robert J. Bies. “Consumer Privacy: Balancing Economic and Justice Considerations,” *Journal of Social Issues* 59 (2003): 323–342; Electronic Privacy Information Center. *Privacy Self-Regulation: A Decade of Disappointment*. epl.scu.edu/~stsvvalues/readings/decadedisappoint.pdf. Online, December 2005; Froomkin, A. Michael. “The Death of Privacy?” *Stanford Law Review* 52 (2000): 1461–1542; Gandy, Oscar H. “Legitimate Business Interest: No End in Sight? An Inquiry into the Statuses of Privacy in Cyberspace,” *University of Chicago Legal Forum* 77 (1996): 77–137; Harrow, Robert. *No Place to Hide*. Boston: Free Press, 2005; Lyon, David (ed.), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge, 2003; Turow, Joseph. *Breaking Up America: Advertisers and the New Media World*. Chicago: University of Chicago Press, 1997; Weiss, Michael J. *The Clustered World*. Boston: Little, Brown, 2000.

Brian Azcona

Trap and trace. *See* **Electronic surveillance; Pen register; Wiretapping**



Trespass

Trespass is the unauthorized entry onto or use of property, either real or personal. The legal concept of trespass was developed in English common law during the thirteenth century as a means of protecting the king's interest in land and was not considered a protection of privacy per se. Today trespass is most often used to describe an intrusion into or an infringement of one's rights to real property. While a trespass action is frequently filed to protect a property owner's privacy rights, the action is still grounded in the land-based property concerns of early England. For example, when a former U.S. congressman felt that reporters from the *Baltimore Sun* invaded his privacy by interviewing him in his nursing **home** room, his trespass action needed to be supplemented by an action for "intrusion upon seclusion" under Maryland law to address his privacy concerns (see *Mitchell v. Baltimore Sun Co.*, Md. Ct. Spec. App., No. 266, 9/29/05). It is more helpful to think of a trespass action as a tool to keep others from one's property so that one's privacy is protected rather than as a tool to protect one's privacy. In most jurisdictions, to succeed in a civil trespass action, one must prove actual damages, although the damages may be slight.

Criminal trespass is more difficult to explain because the laws vary from jurisdiction to jurisdiction. Under English common law, criminal sanctions were not appropriate unless the trespass was accomplished by violence or a breach of the peace. Today, some states make any entry onto another's land without authority a crime. If the trespass involves violence or injury to a person or property, it is usually considered criminal, although the resulting charges may not actually be for trespass itself. Many jurisdictions, but not all, require proof of criminal intent to prove criminal trespass. There are also jurisdictions that require proof that the trespasser had an unlawful purpose for entering into or remaining on the land to support a charge of criminal trespass. Still other jurisdictions will not find there has been a criminal trespass unless the trespasser was first warned, by either a sign or some other method, that trespassing is prohibited.

Generally, courts will hold trespassers responsible for the consequences of their actions, including unintended or unanticipated consequences. Thus, if a trespasser lights a fire to cook a meal but sets a forest on fire, the trespasser will be held liable to the landowner for damages to the timber, the costs of fighting the fire, and any other consequential damages. Absent specific statutes protecting privacy, courts will usually not award damages in trespass for violation of privacy.

One of the more interesting and challenging questions of trespass is how far above or below ground level the right to possession of land extends. In *United States v. Causby*, 328 U.S. 256 (1946), the Supreme Court held that airspace above land is like a public highway and ordinary airplane flights cannot commit trespass. Nevertheless, a construction boom moving building materials over land may constitute a trespass, as may a roof that hangs over another's property. A trespass may be committed by tunneling or mining under another's land, or by forcing water to flow under another's property. A trespass action in these circumstances, however, will generally be permitted only when there is damage to the surface land or interference with a landowner's use of the property.

The old English concept of trespass on chattels has found a new life in **computer** privacy litigation. Federal courts in several jurisdictions have held that the ancient

doctrine applies to the “trespass” by spyware on computers via the **Internet**. Companies like America Online, CompuServe, Intel, and eBay have successfully used the doctrine to battle spammers and hackers. The cause of action provides hope for private users as well in the battle to protect privacy when they can allege that unauthorized spyware tracks their Internet use, invades their privacy, and causes damage to their computers. In addition, states are adopting criminal laws to prevent “computer trespass.”

To understand the concept of trespass, it is helpful to understand the defenses to the charge whether in the civil or criminal arena. Generally, for example, public officials have no special rights allowing trespass. Nevertheless, building inspectors, health inspectors, and the like may have the authority to enter onto private property without an owner’s consent. The distinction is that the entry is with lawful authority.

Those who enter land to protect another’s property or to save a life will not be found guilty of trespass. Those with permission to enter property will not be guilty of trespass unless they violate the terms of the original grant of authority allowing them to enter. For example, generally a shopper in a store is not guilty of trespass, as the owner has authorized the shopper’s entry. If, however, the shopper entered the store to steal merchandise, the shopper may be guilty of trespass.

Property owners are limited in the actions they may take in response to trespassers. They may put up fences and post signs limiting access, but they may not set traps for unwary trespassers or shoot at them. Furthermore, landowners or tenants on the land have no duty to protect or warn trespassers from existing hazards, but they also cannot create situations to intentionally cause harm to those trespassers. Nevertheless, if a property owner knows that people regularly trespass at one or more locations on that owner’s land, the owner must take steps to keep trespassers out or take steps to prevent their injury.

See also: California v. Ciraolo, 476 U.S. 207 (1986); *Oliver v. United States*, 466 U.S. 170 (1984); *Payton v. New York*, 445 U.S. 573 (1980)

Suggested Reading: Connolly, Kevin J. *Law of Internet Security and Privacy*. New York: Aspen, 2004; Gordley, James. *Foundations of Privacy Law: Property, Tort, Contract, Unjust Enrichment*. New York: Oxford University Press, 2003; Lyons, Bruce. *A Constitutional and Legal History of Medieval England*. New York: Harper & Brothers, 1960; Smith, Robert Ellis. *Ben Franklin’s Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*. Ann Arbor, MI: Sheridan Books, 2004; Smith, Robert Ellis. *Compilation of State and Federal Privacy Laws*. Providence, RI: Privacy Journal, 1992; Turkington, Richard C., and Anita L. Allen. *Privacy Law: Cases and Materials*. St. Paul, MN: West, 2002.

David J. Brown

Two-way mirrors

Two-way mirrors, also referred to as one-way mirrors, are primarily used by police to observe criminal suspects or by retail employees to monitor customers for theft. Although two-way mirrors are famous for their placement in police interrogation rooms and shopping malls, they have become more readily available to the public and are increasingly used in businesses and even private **homes**. With the public’s increasing access to technology, two-way mirrors have become available to anyone who is interested. Websites advertise the advantages of two-way mirrors



on personal property as ways to keep an eye on babysitters and others doing work inside one's home. On the other hand, some voice concern at the availability of two-way mirrors since owners can place them inside dressing rooms, rental property, or hotel rooms to facilitate **voyeurism**. The harmful possibilities of two-way mirrors have increased the public outcry for privacy laws that would protect those who are unknowingly watched.

Two-way mirrors are an effective means of **surveillance** since those being watched are usually unaware of it. This is because of the way two-way mirrors are designed. Two-way mirrors are commonly misunderstood to be a mirror from one side and a window (letting light through) from the other side. Actually, the two-way mirror is only semitransparent because it is letting about half of the light through, and reflecting the other half of the light, from both sides. This effect occurs when one side is in the dark. When no light goes through from the dark side to the bright side, and almost no light is reflected back from the bright side to the dark side, it acts as a sort of window. Therefore, those on the dimly lit side can see through the mirror, while those on the brightly lit side see their own reflection.

Because of the properties of two-way mirrors, they are commonly used in police interrogation rooms. This allows law enforcement officials to observe the interrogation and questioning process and to monitor for misconduct by both the criminal suspect and those doing the interrogating. In addition to being used in interrogation rooms, two-way mirrors have been used to monitor activity within shopping malls, banks, post offices, and private businesses. Since two-way mirrors are semitransparent, surveillance cameras can be placed behind them to capture any activity within its viewing range. This is probably the second most popular use of two-way mirrors. With a camera placed behind the two-way mirror, employers can monitor not only customers, but their own employees as well. The placement of cameras behind two-way mirrors is an effective means of identifying and apprehending those breaking the law.

See also: **Landlord and tenant; Restrooms and dressing rooms**

Suggested Reading: Brinn, David. *The Transparent Society*. New York: Perseus, 1999; Calvert, Clay. *Voyeur Nation: Media, Privacy, and Peering in Modern Culture*. Boulder, CO: Westview Press, 2000; Rodriguez, Americo Pla. "The Protection of Workers' Privacy: The Situation in the Americas," *International Labour Review* 134 (1995): 297–313; Staples, William G. *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. Lanham, MD: Rowan & Littlefield. 2000.

Christina Dudzinski

U



United States Census

The U.S. Census has evolved a great deal since the first enumeration in 1790. As the population has grown, the task of collecting demographic information from every household in the country has become more complex and costly. Over time the survey itself has also changed, now including questions designed to elicit more sensitive information than originally intended. As technological advances have shaped census methodological and data dissemination practices, new privacy concerns have developed. Although privacy and **confidentiality** may be conceptually distinct, in the context of the U.S. Census, and in the minds of respondents, the two issues are intricately related. The Census Bureau's privacy and confidentiality practices are important factors in determining the agency's procedures for collecting and releasing household data. One of the primary concerns of the bureau is data protection, which requires minimizing intrusion and developing comprehensive measures to ensure that the data collected remain confidential. Reducing both real and perceived risk is essential for a successful enumeration. Because census results determine congressional redistricting and influence the distribution of billions of dollars in federal funds, government officials, policymakers, and the general public have an interest in the agency's ability to collect accurate information.

The Census Bureau's largest task is the decennial census. Although most of the agency's other projects rely on nationally representative sampling techniques, the goal of the decennial census is to account for every household in the country. This undertaking required a census employee to visit each household until 1970, when the agency implemented the "mail out-mail back" survey allowing the **United States Postal Service** to distribute the questionnaires and respondents to mail them back to local processing offices. Each household now receives either the short form (intended to collect only basic demographic and housing information such as **gender**, age, race, and home ownership/rental status) or the long form (which is sent to a sample of households and contains the short form plus additional questions). The content and length of the long form have varied historically; in the 2000 census it contained more than 50 questions eliciting information on such topics as English

language fluency, previous residences, the value of one's home and cost of utilities, whether a unit is covered by a second mortgage or homeowner's insurance, and the number of **automobiles** per household.

Participation in the decennial census is technically mandatory, but noncompliance is rarely penalized. Collecting household information inherently involves a level of intrusion. Because a successful enumeration requires the voluntary cooperation of respondents, addressing the public's privacy concerns is paramount to the bureau's success. Respondents have been particularly troubled by the perceived invasiveness of the long form. Growing intolerance for private market researchers, generally low levels of trust in the government, and greater fear of fraud and the unauthorized use of personal information create additional barriers to census participation. Political leaders have also expressed concerns. Prior to both the 1970 and 2000 censuses, Congress considered legislation to formally limit the questions that could be asked in the decennial census in order to reduce what was viewed as an undue burden and invasion of privacy imposed on the public.

In reaction to steadily declining response rates since the 1970 census, the bureau launched a research initiative in the 1990s to assess attitudes about census-related privacy concerns and their effects on individuals' willingness to provide information. They found that the public was not well informed about the bureau's privacy principles and that fears of data misuse were especially pronounced among historically underrepresented minority groups. To reverse participation trends in 2000, the bureau instituted a multi-million-dollar, professionally designed public relations campaign that included television, radio, and print ads. Hard-to-count populations were targeted, and the advertisements emphasized that individually identifiable census data are not subject to **disclosure** under the **Freedom of Information Act** and that even the **Internal Revenue Service (IRS)** and Supreme Court do not have access to **personally identifiable information** collected in the decennial census.

The agency saw the success of the 2000 census campaign as evidence of the importance of addressing the public's privacy concerns. In March 2005, the bureau appointed the agency's first formal Chief Privacy Officer, Gerald W. Gates, whose responsibilities included strengthening data protections and educating census employees and the public about privacy issues. After the 2000 census, the agency also updated its data stewardship website, increasing emphasis on the bureau's legal and ethical obligations to respect privacy and protect confidentiality. The new content stressed that personally identifiable information is never published and cannot be used against a person by any government agency or court, and that employees are sworn to uphold the privacy of respondents for life, pointing out that violating the census confidentiality oath carries severe fines of up to \$250,000 and/or maximum prison sentences of five years.

The website also highlighted the protection that specific federal laws provided respondents, as well as the agency's own privacy principles: the census collects only information that is necessary for federal programs; respondents have the right to know the purpose and uses of the survey or census they agree to participate in; the census is in full compliance with federal protections for research participants, and respondents have a right to respectful treatment, including reasonable limits and restrictions on the number of follow-up surveys; access to private information is restricted to sworn staff; and, statistical methodologies, computer technologies, and security procedures are in place to prevent identity disclosure.

When the first census enumeration was taken, there was very little concern for individual privacy. Until the 1850 census, local returns were openly posted and subject to public review. Citizens were allowed unrestricted access to original records until 1880. An important turning point in the privacy history of the U.S. Census occurred in 1952, when the statutory regulations of U.S. Code Title 13 were formalized. The provision establishes that census data may be used only for statistical purposes and cannot be published with individual identifiers such as name or **Social Security number**. The statute also restricts the use of information that contains personal identifiers to sworn census employees. Legal contests by the attorney general, the **Federal Bureau of Investigation (FBI)**, the Immigration and Naturalization Service, and municipal governments to release personally identifying census data or master address lists have consistently upheld the strict confidentiality standards set forth in Title 13.

One of the enduring tasks of the Census Bureau is to provide greater accessibility to data while protecting respondent confidentiality. Increasing use of the **Internet** and PCs, combined with technological advances, has led to an increased capacity for the dissemination of census data to nongovernment users while also generating new sources of privacy risk. In the late 1990s, the Census Bureau introduced the American FactFinder website, which gives users remote access to census microdata (disaggregated data at the respondent level without personal identifiers). To make data more easily available while limiting confidentiality risks, the bureau has developed a number of disclosure limitation procedures.

Prior to 1990, data suppression techniques were primarily used, leaving marginal totals in tables of aggregate data intact but suppressing small individual cell values in addition to other random cells, so that the missing values could not be calculated. Data-swapping techniques were introduced in the 1990 census and entail exchanging records for a sample of cases with a sample of households in neighboring areas that are matched on the basis of key variables within households. Public Use Microdata Samples (PUMS) may also be protected by introducing random noise (adding or multiplying the data by a random number), top- and bottom-coding (collapsing data that fall above or below a certain percentage of the distribution), and using population thresholds (prohibiting disclosure of geographic identifiers for areas with populations below 100,000). A disclosure review board reviews all requests for microdata files to assess disclosure risk before being released.

As the census and technology continue to evolve, new privacy concerns and solutions will also arise. For instance, in the 2000 census, respondents were allowed to indicate multiple race categories. Although intended to collect better race data, the change inadvertently increased disclosure risks because of the added race detail. In 2000, respondents were allowed to file their census short form over the Internet, requiring multiple firewalls, encryption, and authentication codes to protect the submitted data. The Census Bureau also is considering within-household privacy issues. In 1998, the Census Bureau implemented a respondent identification policy that requests permission to share limited information with other household members in future waves of panel studies. The bureau also has been testing the use of the American Communities Survey, based on a monthly random sample of U.S. households, which elicits information similar to that requested on



the long form. If successful, this could result in the elimination of the long form, which is perceived as especially invasive.

See also: **Privacy Act of 1974; Public records**

Suggested Reading: Anderson, Margo J. (ed.). *Encyclopedia of the U.S. Census*. Washington, DC: CQ Press, 2000; Duncan, George T., Thomas B. Jabine, and Virginia A. de Wolf (eds.). *Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics*. Washington, DC: National Academy Press, 1993; Hawala, Sam, Laura Zayatz, and Sandra Rowland. "American FactFinder: Disclosure Limitation for the Advanced Query System," *Journal of Official Statistics* 20 (2004): 115–124; Mayer, Thomas S. *Privacy and Confidentiality Research and the U.S. Census Bureau: Recommendations Based on a Review of the Literature*. Report prepared for the U.S. Bureau of the Census (2002). www.census.gov/srd/papers/pdf/rsm2002-01.pdf. Online, November 2005; Singer, Eleanor, John Van Hoewyk, and Randall J. Neugebauer. "Attitudes and Behavior: The Impact of Privacy and Confidentiality Concerns on Participation in the 2000 Census," *Public Opinion Quarterly* 67 (2003): 368–384; U.S. Bureau of the Census. *Census Confidentiality and Privacy: 1790–2002*. Report prepared for the U.S. Bureau of the Census (2003). www.census.gov/prod/2003pubs/conmono2.pdf. Online, November 2005; U.S. Bureau of the Census. *Data Protection and Privacy Policy*. www.census.gov/privacy/. Online, November 2005.

Elizabeth Miklya Legerski

United States Postal Service (USPS)

The Postal Service was created in 1775 by decree of the Second Continental Congress. The passage of the Postal Reorganization Act in 1970 restructured the Post Office Department into the independent division of the executive branch we have today. Presently owned and regulated by the executive branch, the USPS is the third largest employer in the United States. The duties of the USPS are to receive, sort, and make every reasonable attempt to deliver mail to citizens, organizations, and corporations in the United States. Because the USPS has access to **confidential** information, concerns about privacy infringement have been raised. Specifically, rental procedures for private mailboxes (PMBs), National Change of Address (NCOA) distribution, and mail **surveillance** have been cited as potential areas of privacy violation.

The ability of the USPS to regulate commercial mail receivers is a concern to privacy advocates. One reason to rent a PMB is to protect one's home address from public knowledge. Originally, PMB renters had the most **anonymity**. In the past, renting a PMB required only one form of identification and a completed Form 1583 (Application for Delivery of Mail Through Agent). However, on March 25, 1999, the USPS imposed new regulations on commercial mail-receiving agencies. Now the USPS requires two forms of identification from all PMB renters. Acceptable forms of identification must include proof of signature with picture and a serial number that is traceable to the applicant. The USPS requires copies of all PMB forms from commercial mail-receiving agencies, and it keeps those records on file in case of criminal investigation. The national database that stores this information, however, is publicly accessible. These new regulations have resulted in the collection of individuals' names, addresses, phone numbers, and **Social Security**

or otherwise traceable numbers. Public access to this private information may have serious consequences for lawful U.S. citizens.

Privacy advocates argue that this procedure violates the Fifth Amendment, which allows for protection of private information. Nondisclosure of private information is important because it impedes discrimination and fraud. The USPS justifies these new regulations as an attempt to reduce mail fraud. However, the USPS has yet to demonstrate that fraud is more prevalent among PMB renters compared with post office box holders. More alarming is that the personal information required on Form 1583 violates the privacy regulations of the USPS. Accessibility of this information may, in fact, enable criminal activity, not impede it. Access to home addresses and otherwise private information may be a personal liability, especially in instances involving identity theft, stalkers, and domestic-abuse victims.

The USPS privacy regulations state that all personal information disclosed should be in accordance with the **Privacy Act of 1974**. Examples of permissible grounds for **disclosure** include the individual's request or the request of the government, legal proceedings or process, licensure, or mailers if they have the old address on file. Nevertheless, loopholes in the Privacy Act allow for the unintended distribution of confidential information. For example, NCOA lists provide the USPS with new addresses that aid with mail forwarding when a person changes residences or businesses. However, the USPS does not actually execute the address corrections. The information collected on the NCOA forms is sold to licensed service providers of the USPS. These service providers make address corrections to existing mailing lists of individuals. In addition to address updates, however, these licensed service providers, which include junk mailers, direct marketers, and credit bureaus, often have other interests in an individual's private information. The consequences to private citizens are an increased risk of fraud or discrimination and receipt of unwanted mail.

The USPS argues that the distribution of NCOA lists decreases the volume of undeliverable mail, therefore cutting costs. Yet this procedure allows for private information to be passed on to authorized third parties for unauthorized uses. Privacy advocates argue that federal protection is needed—similar to protection from **telemarketers**—to incorporate safeguards from unwanted mail. The House Government Reform Committee, in conjunction with the House Government Affairs Committee, has recommended the establishment of national Do-Not-Mail lists, “No Junk Mail” stickers, and company-specific do-not-mail programs. In addition, these committees urged the 109th Congress to consider the unintended consequences of the NCOA program.

Besides the PMB and NCOA lists, the USPS affects Americans' civil liberties in another way. In response to the 2001 anthrax scares, the USPS proposed implementing a sender identification program. Sometimes referred to as “smart stamps,” intelligent mail would allow the U.S. government to track private mail. This would be accomplished by requiring and recording identification from individuals sending mail. The risks to civil liberties include the violation of **anonymity** and the unwarranted surveillance of private mail. In 2003 the USPS withdrew its proposal to implement sender identification; nevertheless, mail surveillance is still a concern.

Mail covers, or the enclosing materials of private mail, are considered public domain. Therefore, the U.S. government can inspect mail covers to protect national security or apprehend criminals. Moreover, the opening of private mail is an inherent



prerogative of executive authority in protecting national security. Mail covers indicating an international origination or destination are subject to inspection by Homeland Security or customs. In addition, a **search warrant** is not required for opening mail in instances of possible bomb mechanisms, illicit drugs, or a threat to national security. Information collected from mail covers includes sender identification, recipient identification, and the class under which the mail was sent. This information may lead to privacy violations of lawful U.S. citizens corresponding with addresses outside the United States.

Grounded in the Fourth and Fifth Amendments, nondisclosure of personal information and protection from search and seizure are considered constitutional rights. However, the USPS may infringe on Americans' rights to privacy. Areas of concern include PMB rental requirements, NCOA distribution, and mail surveillance. Although surveillance and disclosure are in accordance with the Privacy Act, these disclosures simultaneously permit government and nongovernment offices to collect and distribute private information of lawful U.S. citizens.

Suggested Reading: Electronic Privacy Information Center (EPIC). www.epic.org/privacy/postal/. Online, March 2006; Flaherty, David H. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill: University of North Carolina Press, 1992; Smith, Robert Ellis. *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*. Providence, RI: Privacy Journal, 2004; USPS. *Postal History*. <http://www.usps.com>. Online, April 2006.

Christine Schneider

United States v. Caldwell, 408 U.S. 665 (1972) (companion case to *Branzburg v. Hayes*)

In early 1970, a grand jury was investigating violations of federal law, including threats against the president, civil disorder, and mail fraud, by the Black Panther Party and other black militant groups. Earl Caldwell was a reporter for the *New York Times* and assigned to cover the activities of the Black Panther Party and similar groups. In February 1970, a subpoena was served on Caldwell ordering him to testify and produce documents and recordings concerning the activities of the Black Panthers. Caldwell objected to the scope of the order, and in March a second subpoena was issued ordering him to appear before the grand jury to testify; however, the order omitted the document requirement. Again, Caldwell opposed the scope of the subpoena, citing that his testimony would destroy his relationship with the Panthers and infringe on the First Amendment rights of speech and press.

In April, the district court denied Caldwell's motion to quash the subpoena but did issue a protective order, which allowed Caldwell to refrain from revealing **confidential** information, which is protect by the First Amendment. The court did stipulate, however, that such information must be revealed if the government could show a compelling national interest in obtaining his testimony that could not be served by any other means.

Caldwell refused to appear and was held in contempt until he complied with the court's order to testify. The court of appeals reversed the contempt order and held that requiring Caldwell to testify breached a qualified testimonial **privilege** for a reporter. Such a requirement would have an adverse impact on the flow of news to the public.

The Supreme Court granted certiorari and determined the issue to be whether reporters are immune to grand jury subpoenas and from answering questions relevant to the investigation of a crime. The Court reasoned that the First Amendment does not give the press the right to publish anything and everything it wills without consequence, as it is subject to liability for damages and subject to prosecution. Furthermore, grand juries serve a fundamental interest in securing the safety of the public, and thus, actions that infringe on personal rights are generally justifiable.

Therefore, the Court overturned the decision of the court of appeals and ordered Caldwell to testify. The Court found that requiring reporters to disclose to grand juries information that would be otherwise protected served a legitimate and compelling state interest and was not in violation of the First Amendment.

In the dissent, Justice **William O. Douglas** stated two principles that stemmed from his understanding of the First Amendment. The first is that the government should afford citizens the freedom and privacy of their own opinions and beliefs regardless of public sentiment. A corollary conclusion reached in the dissent is that an individual must also have absolute privacy of the information gathered and used in developing his or her own opinions and beliefs. The second principle is that self-government cannot succeed unless people are free of general suspicion as to their beliefs and able to participate in an undeterred flow of opinion and reporting. Thus, by requiring Caldwell to testify, the government not only infringed on inherent freedoms, but also impeded journalists' ability to gather and disseminate news.

Moreover, Justice Douglas points out that in his view no compelling need can be shown that refutes the reporter's immunity or forces him to testify, unless he is involved in a crime. The First Amendment, absent his involvement in a crime, protects him against appearance before a grand jury, and if he is involved in a crime, the Fifth Amendment protects him from self-incrimination. Therefore, in the view of Douglas, the reporter need not appear simply to invoke a right to every question posed by the grand jury. Thus, the reliance upon which the Court rested its opinion—that there was a compelling state interest in Caldwell's testimony and information—failed to withstand the constitutional rights of the First and Fifth Amendments guaranteed to Caldwell.

See also: Associated Press v. Walker, 388 U.S. 130 (1967); *Bauer v. Kincaid*, 759 F. Supp. 575 (1991); **Constitutional protections**; *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975); **Journalism**; *Red & Black Publishing Co. v. Board of Regents*, 262 Ga. 848 (1993); *Time, Inc. v. Hill*, 385 U.S. 374

Suggested Reading: Tedford, Thomas L., and Dale A. Herbeck. *Freedom of Speech in the United States*, 5th ed. State College, PA: Strata, 2005; Westin, Allan. *Privacy and Freedom*. New York: Atheneum, 1967.

Matthew M. Dwyer

***United States v. Dionisio*, 410 U.S. 1 (1973)**

The right to feel secure from unreasonable governmental searches and seizures is a fundamental **constitutional protection** founded on the Fourth Amendment. The question in *United States v. Dionisio* was whether Fourth Amendment protection extends to security of an individual's voice. The Supreme Court deliberated on the need to protect private citizens against governmental mandates to produce voice



samples in an investigation. The Court held that the voice is not included under the Fourth Amendment and that the order to produce a voice sample is not a significant seizure of an individual's voice or a violation of the **reasonable expectation of privacy**.

A grand jury convened in an attempt to investigate federal gambling crimes that had become an issue of governmental concern. The investigation produced multiple recordings of conversations containing evidence pertinent to the grand jury. In an attempt at **voice identification** with respect to the recordings, the grand jury subpoenaed roughly 20 people to submit voice samples. The respondent, Mr. Dionisio, was among the 20 individuals required to take part in the investigation.

Each participant was instructed to look over transcripts of the recordings and then report to the state's attorney's office for submission of a voice sample. They were all advised of their legal rights as well as their classification as possible defendants in the grand jury investigation. Mr. Dionisio refused to comply on the grounds that it violated his Fourth Amendment right of protection from unreasonable governmental seizures as well as his Fifth Amendment right to silence. When his arguments went before the district court, both constitutional assertions were rejected. He was ordered to comply with the grand jury's subpoena and to submit to the voice testing. Dionisio refused the court's mandate, and he was found in civil contempt. He was confined to police custody until either he submitted his voice sample to the state's attorney or the grand jury was dissolved.

After a reversal by the appellate court on the grounds that the subpoena did in fact violate the respondent's Fourth Amendment rights because of a lack of probable cause, the Supreme Court granted a writ of certiorari and reviewed the case. It reasoned that there was no Fifth Amendment violation because a voice sample is evidence that is physical in nature, much like other **biometric identifiers** such as **fingerprints** or handwriting. In this case, the voice samples were meant only to identify the voices on the recording as physical evidence. For the Fifth Amendment to apply to this case, the intentions for ordering the voice samples would have to involve testimonial or communicative purposes. In other words, what the investigation sought to do was no different from comparing the respondent's face to a photograph in order to determine his identity. The Court decided that the respondent's Fifth Amendment right to silence was not violated by the grand jury's order.

Concerning the Fourth Amendment assertion, the Supreme Court separated the respondent's argument into two parts. The first issue was whether it was a violation of the Fourth Amendment's protection against unreasonable seizures to require the respondent to physically appear before the grand jury. The Court quickly rejected this issue. Long ago, the courts deemed it to be in society's best interest to require an individual's contribution of evidence when it was requested by any legal fact-finding body. Second, Dionisio contended that the recording of his voice would be a Fourth Amendment violation of his expectation of privacy. The Court ruled that a seizure of Dionisio's voice is, likewise, not protected under the Fourth Amendment's privacy clause. A person does not have a reasonable expectation of privacy regarding his voice. A person's voice is produced in public on a daily basis for the benefit of everyone who can hear it. It is not reasonable for an individual who speaks in public to expect others not to recognize or familiarize themselves with his voice. Simply because a person wishes to keep his voice private does not mean that his expectation is reasonable if he exposes it in public. Likewise, it is not rea-

sonable for the respondent to expect his voice to remain private from the grand jury if, in the past, he has publicly produced it, without restraint, for the benefit of all to hear.

The Supreme Court concluded that there was no constitutional violation of the respondent's rights. The assertion that the Fifth Amendment right to silence would be violated was flawed. Since the request of the respondent's voice was made for evidentiary rather than testimonial purposes, the Fifth Amendment did not apply. The Court also decided that the Fourth Amendment claim was erroneous. Since the respondent could not reasonably expect his voice to remain private if it had been publicly used in the past, he could not expect it to remain private from the court.

See also: **Electronic surveillance**

Suggested Reading: Amsterdam, Anthony G. "Perspectives on the Fourth Amendment," *Minnesota Law Review* 58 (1974): 349–447; Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; Ramsland, Katherine. *The Origins of Voiceprints*. www.crimelibrary.com. Online, December 2005.

Sean M. Peek

United States v. Dunn, 480 U.S. 294 (1987)

Ronald Dunn owned nearly 200 acres of ranch property. Situated one-half mile off the public road, the ranch consisted of a **home** with a nearby greenhouse, two barns approximately 50 yards from the house, and a fence surrounding the property. The ranch had a series of interior fences as well. One encircled the home and greenhouse. A wooden fence surrounded the larger of the two barns, and another fence barred entry into the barn proper; both of these fences were surrounded by barbed wire. In 1980 the Drug Enforcement Administration learned that Robert Carpenter had purchased certain equipment and chemicals used in the manufacture of amphetamines, namely an electric hot stirrer plate and two drums of chemicals. DEA agents placed tracking devices on the stirrer and the drums and tracked two of them to the ranch house.

On November 5, 1980, law enforcement officials made a warrantless entry onto the ranch, drawn by their data, the smell of chemicals, and the sound of a motor running. Crossing several fences, the officers observed—without entering the barn—what they believed to be a drug laboratory. The following morning the officers obtained a **search warrant**, and it was executed two days later. The officers seized the equipment, chemicals, and drugs in the house and arrested Dunn.

The question before the Supreme Court was whether the barn fell within the **curtilage** of the house, and thus whether Dunn had a **reasonable expectation of privacy** in the barn and its contents. The Supreme Court held that the barn was not within the curtilage of the home, as it did not meet a four-factor test. The first of these factors to be considered was the proximity of the area to the home. In this case, the barn was nearly 50 yards away from the residence. In the eyes of the Court, this distance was sufficient to find that the barn was too far away from the



residence. The second factor was whether the area was within an enclosure surrounding the home. On Dunn's ranch, he had constructed several fences. However, the same fence did not encompass the home and the barns. The third factor considered was the nature and use of the area. The Court pointed out that the officers possessed independent and objective data indicating that the barn was not being used as part of the home. Therefore, the barn could not be placed under the same blanket of protection as the home, as it was being used for an independent purpose. The fourth factor considered was the steps taken by Dunn to protect the area from observation by others. The Court reasoned that although there were several fences, they were much like those used to corral livestock and not intended to block observation. Therefore, because the barn did not satisfy any of the four factors, it was not found to be within the curtilage of the home.

In the alternative, Dunn attempted to argue that the barn was essential to his business, and therefore he possessed a privacy interest in it. The Court was quick to point out that the officers never entered the barn. Rather, they conducted their observations over the ranch-style fences. As the Court has previously held, law enforcement may conduct observations from the surrounding open fields, and fences of this type do not create a constitutionally protected privacy interest. The **plain view** observation of an area is not unconstitutional, and even shining a flashlight into a darkened area does not violate any Fourth Amendment protected interest.

Therefore, the Court reversed its prior decisions and held that the barn was not within the protected curtilage of the home. All evidence that had been seized was admissible, and Dunn's conviction was upheld.

See also: California v. Ciraolo, 476 U.S. 207 (1986); *Chimel v. California*, 395 U.S. 752 (1969); *Payton v. New York*, 445 U.S. 573 (1980); *Trespass; Warden v. Hayden*, 387 U.S. 294 (1967); *Weeks v. United States*, 232 U.S. 383 (1914)

Suggested Reading: Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States; Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

Matthew M. Dwyer

***United States v. Kyllo*, 533 U.S. 27 (2001)**

Federal agents suspected defendant Kyllo of growing marijuana in his **home**, part of a triplex. Indoor marijuana production requires high-intensity heat lamps. In order to determine if such lamps were in use at Kyllo's home, agents used a **thermal** imager to determine the relative amount of heat emanating from Kyllo's triplex. The scan was done from the agent's car across the street and took only a couple of minutes. The scan revealed that the roof and one wall of Kyllo's garage were relatively hot compared with the rest of the home and the rest of the triplex. Based on tips from informants, utility bills, and the thermal scan, a **search war-**

rant was issued. More than 100 marijuana plants were discovered in Kyllo's home. He moved unsuccessfully to have the evidence from the thermal scan suppressed and was convicted, and he appealed. The Court of Appeals for the Ninth Circuit remanded the case to the district court to decide on the intrusiveness of the thermal scanning. The district court held that it was not intrusive because, *inter alia*, it did not reveal intimate details of the home. The district court upheld the warrant, and the defendant again appealed. The Ninth Circuit eventually affirmed the decision under the *Katz v. United States* test, holding that Kyllo had shown no subjective expectation of privacy in the amount of heat escaping from his home, and even if he had, there was no **reasonable expectation of privacy** in "amorphous 'hot spots' on the roof and exterior wall."

The United States Supreme Court granted certiorari and reversed the Court of Appeals for the Ninth Circuit. The Court held that where the government uses a device that is not in general public use to explore the details of a private home that would have been unknowable but for physical intrusion, the **surveillance** constitutes a "search" within the meaning of the Fourth Amendment. In an opinion delivered by Justice Scalia, the Court arrived at this conclusion by applying the *Katz* "reasonable expectation" test: an object is not protected from search by the Fourth Amendment unless the individual has a subjective expectation of privacy in the searched object, and society is willing to recognize that expectation as reasonable. The Fourth Amendment is most applicable to the protection of privacy interests in the home, but is extended to protect against searches of many things in which an individual has an expectation of privacy. Indeed, in *Katz* the Court found an impermissible search in the government's use of a "listening device" planted in a public phone booth. While the setting is not a home, and is not always particularly private because passersby may hear what is transpiring, an individual who shuts the door to a public phone booth has a subjective expectation of privacy in the conversation, and society is prepared to recognize that as reasonable.

While visual observation is not a search, this case involved more than naked-eye surveillance; it involved the use of technology. And whereas the Court had previously held that enhanced aerial photography of an industrial complex was not a search—primarily because it was not a home, where privacy expectations are heightened (*Dow Chemical Co. v. United States*)—here the Court drew the line. It held that any information obtained by sense-enhancing technology regarding the interior of the home, that could not have otherwise been obtained without physical intrusion, constitutes a search. The Court declined to adopt the argument that the type of information, intimate versus non-intimate, required a different conclusion. The Court ruled that all details of the home are intimate details. The Court affirmed that the Fourth Amendment draws a firm line at the entrance to the house, and that line must be not only firm but bright, requiring clear specification of what methods of surveillance are impermissibly intrusive without a warrant.

Justice Stevens, joined by Chief Justice Rehnquist and Justices Kennedy and O'Connor, dissented. The dissent in this case argued that there was an overlooked distinction between "through-the-wall surveillance" and "off-the-wall surveillance." It argued that the thermal scanning, which collected data exposed on the outside of the home, did not invade any constitutionally protected interest in privacy. Moreover, the dissent argued that the majority's holding was contrary to



established law: that what a person knowingly exposes to the public is not subject to Fourth Amendment protection. The dissent compared heat waves to aromas from a kitchen, a lab, or an opium den: they enter the public domain when they leave a building, and the expectation that they would remain private is not one that society would recognize as reasonable. The dissent likened this case to *California v. Greenwood* (1979), in which the court held that there is no reasonable expectation of privacy warranting Fourth Amendment protection in **garbage** discarded on the curb outside the home. Further, the dissent argued that the majority's limitation of Fourth Amendment protection to surveillance by technology not in the public use makes the holding meaningless because the protection dissipates as soon as the technology becomes publicly available. The dissent also faulted the majority for making their holding "home-specific," citing the proposition that the Fourth Amendment protects people, not places. The dissent concluded with an argument that while the Court was properly concerned about threats to privacy flowing from advances in technology, the duty to grapple with these issues belongs to the legislature.

See also: *California v. Ciraolo*, 476 U.S. 207 (1986); *Curtilage*; *Oliver v. United States*, 466 U.S. 170 (1984); *Payton v. New York*, 445 U.S. 573 (1980); **Trespass**

Suggested Reading: Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996.

Larkin R. Evans

United States. v. Scheffer, 523 U.S. 303 (1998)

In April 1997, Edward Scheffer, an airman in the United States Air Force, failed to appear to work, could not be located on base, and was declared absent without leave from the service. During a routine traffic stop, an Iowa state police officer identified Scheffer and placed him under arrest, holding him until he could be returned to the base. A **urine analysis** revealed the presence of methamphetamines. Scheffer sought to introduce polygraph results during his general court-martial, which indicated he had not lied when denying drug charges and use while in the service. However, Military Rules of Evidence, specifically Rule 707, prohibit the use of polygraph results in court-martial proceedings. The Supreme Court granted certiorari to determine whether the exclusion of polygraph results violated the defendant's Sixth Amendment right to present a fair defense.

The Court determined that state and federal authorities have a legitimate interest in the admission of only reliable evidence at trial. The impression given by the Court was that polygraph evidence has poor reliability and that even advocates of such tests admit the existence of erroneous results. While the defendant has the right to present relevant evidence, that evidence is subject to reasonable restrictions. Courts can make rules restricting admission of evidence as long as they are not arbitrary or disproportionate to the purposes served. In the Court's eyes, Rule

707 creates a balance, excluding both favorable and unfavorable results. Exclusion of unreliable evidence is a principal objective of evidentiary rules. Finally, the Court determined that the ultimate determination of truth and credibility lies, and should remain, in the hands of juries and not machines. A fundamental premise of the American criminal trial system is that the jury determines credibility. In essence, the jury serves as its own lie detector. Polygraphs diminish the jury's role, and unlike **fingerprints**, which are solid evidence and fact, a polygraph is another opinion as to whether a witness or defendant is telling the truth.

See also: Automobile; Sobriety checkpoint

Suggested Reading: Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

Matthew M. Dwyer

***United States v. Steagald*, 451 U.S. 204 (1981)**

In early 1978, an anonymous informant contacted an agent of the Drug Enforcement Administration (DEA) and indicated he might help the agency locate Ricky Lyons, a fugitive wanted on drug charges. The informant provided a telephone number in Atlanta, Georgia, where Lyons could be reached during the next day. The DEA contacted agent Kelly Goodowens and relayed the information. Goodowens contacted the phone company and obtained an address for the telephone number. Goodowens also learned that Lyons had a six-month-old arrest warrant.

Within a short amount of time, Goodowens and 11 other officers drove to the address. When they arrived, the agents noticed two men standing outside the **home**. The officers drew their guns, frisked the two men, and determined that neither was Lyons. The men were identified as Hoyt Gaultney and the petitioner, Gary Steagald. When the agents approached the home, Gaultney's wife answered the door. The agents placed her in a guarded position and searched the house. During the search, an agent discovered what he allegedly believed to be cocaine. Goodowens sent an officer to obtain a **search warrant** and proceeded with a second search of the house. Pursuant to the search warrant, a third search occurred, and the officers discovered 43 pounds of cocaine. Steagald was arrested and indicted on federal drug charges. At the suppression hearing, Goodowens testified he believed the arrest warrant for Lyons justified the entry and search, and that nothing prevented him from obtaining a search warrant.

The Supreme Court has consistently held that entry to a home to search or make an arrest is unconstitutional unless done pursuant to a warrant, or in the existence of consent or exigent circumstances. Thus, the question before the Court in this case was whether an arrest warrant is adequate to protect the Fourth Amendment

rights of those not named in the warrant when their homes are searched without consent and there are no exigent circumstances.

In this case, the warrant issued authorized the agents to seize Lyons. However, the Court viewed the agents' actions as overstepping the legal parameters established in the warrant. The Court determined that the arrest warrant protected only Lyon's interest in being free from an unreasonable seizure, but not Steagald's interest in being free from an unreasonable search of his home. Therefore, the Court viewed the search of Steagald's home as no more reasonable than if it had been conducted in the absence of a warrant.

The Court felt that a contrary conclusion would give police with an arrest warrant the freedom to search an individual's home, *and* the homes of that individual's friends and acquaintances. Therefore, since the agents did not possess a search warrant upon first entry and only an arrest warrant for Lyons, and because no exigent circumstances existed to justify the infringement of Steagald's Fourth Amendment rights to be secure in his home, the Court ruled that the search of the home was unconstitutional.

The dissent by Justice Rehnquist and Justice White stated that incidental infringements of Fourth Amendment rights might be reasonable in the course of executing a valid warrant. To support this reasoning, the dissent pointed out that requiring a search warrant for each house, given the inherent mobility of a fugitive, would impede the interest of the government and the public in the apprehension of fugitives. The dissenters noted that in *Dalia v. United States* (1979), the Court rejected the argument that a separate search warrant was required before police could enter a business office to install an eavesdropping device when a warrant authorizing the eavesdropping itself had already been obtained. The Court stated in *Dalia* that when executing a warrant, police often find it necessary to infringe on other privacy issues or rights not explicitly covered or considered by the judge issuing the warrant. The same situation was applicable in *Steagald*, according to the dissent. Although the arrest warrant was issued for Lyons, Steagald's privacy interest was incidental to the execution of a valid arrest warrant, and therefore under a reasonableness standard, the government's interest in the warrantless entry of a third-party dwelling to execute an arrest warrant was compelling. Moreover, an arrest warrant is limited in its scope of applicability to a third person's home. It ensures that person that the police are there on official business, and that they may search for the limited purpose of arresting the subject of the warrant. The contraband discovered by the search for Lyons was incidental to the arrest warrant, and not the product of a search warrant.

See also: California v. Ciraolo, 476 U.S. 207 (1986); **Constitutional protections; Curtilage; Oliver v. United States**, 466 U.S. 170 (1984); *Payton v. New York*, 445 U.S. 573 (1980); **Reasonable expectation of privacy; Stop and frisk; Trespass; Weeks v. United States**, 232 U.S. 383 (1914)

Suggested Reading: Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Bodenhamer, David J., and James W. Ely, Jr. (eds.), *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*.

Durham, NC: Carolina Academic Press, 2005; LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*. 3rd ed., 5 vols. St. Paul, MN: West, 1996; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

Matthew M. Dwyer

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)

On October 26, 2001, President George W. Bush signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), P. L. No. 107-56, 115 Stat. 272 (2001). The massive, 342-page act amended at least 15 existing laws, and it expanded the investigative and **surveillance** authorities of federal agencies in pursuit of law enforcement and counterterrorism ends. The Patriot Act quickly became a lightning rod for supporters and critics of the Bush administration's "global war on terrorism," and much hyperbole has surrounded public discourse about the act and its provisions. Although the Patriot Act was, by any measure, a reaction to the terrorist attacks of September 11, 2001, nearly all of the authorities created by Congress in 2001 were later re-authorized as permanent legislation in February 2006.

Background

The Department of Justice introduced antiterrorism bills in the House and Senate less than one week after the September 11 attacks. The department had already prepared draft legislation expanding law enforcement and counterterrorism investigative authorities, so the bills were readily and quickly assembled. In the rush to do something in response to September 11, and prodded by the anthrax letter attacks and the fear that other such attacks could be in the planning stages, the bills were passed with little debate in either house, and no Senate, House, or conference report was produced that could aid interpretation of its provisions after enactment. Although the original administration proposal contained several provisions that significantly expanded existing investigative and surveillance authorities, the only important concession made during the consideration of the act was the addition of so-called sunset provisions (providing that sections of the act expire automatically after a fixed period of time, unless explicitly renewed by Congress) attached to several of the most controversial new provisions.

The act is complex, and many of its provisions are controversial. The act has generated spirited debate throughout its history, centering on whether the broad powers granted the government in ways that could interfere with the rights of ordinary Americans have sufficient safeguards to protect basic liberties. Is the loss of personal liberty worth the gain in security? More than five years later, there is no clear answer to the policy debate or constitutional questions presented by some portions of the Patriot Act; nor is it clear whether the act has met the announced goal of making it more difficult for criminals and would-be terrorists to operate inside the United States.

Summary of the Act

The Patriot Act expands the authority of federal officials to track and intercept communications for law enforcement and foreign intelligence gathering purposes.



The act creates new crimes and penalties, and it streamlines in some ways the procedures for prosecution. The act also provides the Secretary of the Treasury with new powers to regulate corruption of U.S. financial institutions with respect to foreign money laundering, while it adds restrictions tightening immigration and border crossing laws and facilitates the detention and removal of suspected terrorists already inside the United States. Some of the most controversial expansions of governmental authority were made subject to a four-year sunset provision. After considerable debate and short-term extensions of the act in late 2005 and early 2006, all but two of those provisions were made permanent in 2006. Two others, discussed next, were renewed subject to a new, multi-year sunset provision. This discussion focuses on the portions of the Patriot Act most likely to impact privacy.

Provisions Affecting Privacy Interests

The most controversial provisions of the Patriot Act are those that most directly affect privacy interests. These parts of the act provide law enforcement and intelligence agencies a range of new **surveillance** and other investigative powers intended to thwart terrorism and other crimes. While some new authorities have been widely accepted, several others continue to generate controversy. The most significant new powers include

- “Sneak and peek” searches, which make it easier for law enforcement and intelligence agents to conduct secret searches of private homes and businesses without prior notice.
- Enhanced power for intelligence investigators to demand access to personal records held by libraries, health insurance companies, bookstores, schools, businesses, and civil or nonprofit organizations.
- Expanded **wiretapping** authorities, which permit law enforcement agents to monitor personal **Internet** usage, including inbound and outbound **electronic mail** traffic and sites visited on the Internet. Court orders may be implemented nationwide (“roving wiretaps”).
- Eased restrictions on foreign intelligence gathering in the United States and greater access for intelligence investigators to information obtained during criminal investigations.
- Greater authority to bypass court approval and obtain personal records from financial institutions, telephone companies, and Internet service providers.
- Creation of a new crime of “domestic terrorism” that may be capable of targeting nonviolent domestic groups, such as **abortion** protesters and environmental activists.

“Sneak and Peek” Searches

The Fourth Amendment normally requires that police obtain a warrant from a magistrate or judge before searching someone’s **home** or business. The police also must notify the person before conducting the search (known as “knock and announce”). In theory, notice serves as a check against government excesses; government must operate in the open, and targets of a warrant could challenge it if the search exceeded the scope of the warrant or if, for example, the police came to the wrong home or business. Lacking prior notice, the target does not know of the war-

rant or the search until after the search has been completed. Exceptions to prior notice have been limited to situations where evidence of a crime was likely to be destroyed or where notice presented grave danger of physical harm to the investigators.

Under the Patriot Act, government agents may “sneak and peek” without notice if notification of a search “may have an adverse result” on law enforcement. The act allows notice to be delayed for a “reasonable period.” The Justice Department claims that delayed notice gives them time to gather evidence of terrorist activity and then arrest terrorists before they can attack. Critics point out that investigators already had authority for secret surveillance to gather intelligence about suspected terrorists, and the new law enforcement authority was not needed. In addition, the “sneak and peek” authority extends to all federal law enforcement activity, not just terrorism. This authority was not subject to the sunset in 2005.

Personal Records

Since at least the 1970s, federal courts have held that the government may collect personal information that has been voluntarily provided to various categories of third parties, such as banks, telephone companies, and schools. However, according to legislation concerning domestic criminal investigations, a subpoena for banking records, for example, required the bank to give notice to the target of the subpoena, who then could challenge the subpoena in court before the bank turned over information to the government. In gathering foreign intelligence, there would be no notice to the target, but the government had to demonstrate to a court probable cause to believe that the target was an agent of a foreign power.

Under these two schemes, the government could access a limited range of personal information—financial records and records from airlines, car rental agencies, and other travel businesses. As modified by the Patriot Act, any kind of business or nonprofit is required to produce “any tangible thing” that the government demonstrates is relevant to “an authorized investigation to protect the United States from international terrorism.” The requests, like prior ones related to foreign intelligence, are made by a special court created by the **Foreign Intelligence Surveillance Act of 1978 (FISA)**, where no notice or opportunity for the target to contest the request is available and the court has no discretion to reject the government’s request so long as the application is technically complete. The showing of a connection to a foreign power is no longer required, and the information may be sought from an unlimited range of businesses or nonprofits, including **credit card** companies, health management organizations, video rental stores, libraries and bookstores, and advocacy organizations. In addition, once a firm is presented with a demand for “any tangible thing,” the act forbids the firm from disclosing the request to the target or to any other person.

The act does forbid the government from basing a request for records solely on the First Amendment activities of a U.S. citizen or resident alien. Moreover, the Justice Department has claimed no interest in the reading or shopping habits of ordinary Americans. Instead, the department has maintained that the expanded authority might help uncover terrorist plots, such as learning about the purchase of bomb-making materials from a feed or hardware store or a chemical or pharmaceutical plant. Still, libraries and other groups lobbied hard to allow the records provi-



sion to lapse by its sunset at the end of 2005. In the 2006 re-authorization, the records sunset will be extended for a period of years, and a proposal to require the government to show that the target of the request is connected to terrorism or espionage before obtaining his records faces an uncertain outcome in Congress.

Monitoring Internet Use

Before the Patriot Act, government investigators had authority to use **pen registers** and trap-and-trace devices to record the numbers of outgoing and incoming telephone calls at a particular phone. Law enforcement investigators could obtain a court order so long as they simply certified that the pen register or trap-and-trace device was “relevant” to an ordinary criminal investigation. Because these devices do not capture actual conversations, and are thus viewed as less of a privacy threat than traditional wiretaps, the law did not require that the target be a suspect in the investigation.

Under the Patriot Act, the pen register and trap-and-trace order may be extended to cover “dialing, routing, and signaling” information, enabling the government to monitor Internet use. Although the act forbids the monitoring of the “content of any communication,” critics of the provision note that a log of any person’s e-mail or Internet transmissions can reveal the websites visited and the kinds of documents viewed or downloaded at those sites. In addition, the Patriot Act expanded the reach of a pen register or trap-and-trace order to follow the target anywhere in the United States, not just within the jurisdiction where the court issued the order. These nationwide or “roving” orders save time, according to the government, and the expanded authority to monitor Internet use is a necessary part of countering terrorist threats. Critics tend to concede the need for Internet surveillance, but they argue that because the authority in the act is not limited to terrorism investigations, the “relevant” standard should be tightened to limit its application to those actually suspected of aiding terrorism. In the end, Congress voted to extend the sunset provision on “roving wiretaps.”

Expanded Foreign Intelligence Gathering within the United States

Since 1978, when Congress created the Foreign Intelligence Surveillance Court (FISC) in the Foreign Intelligence Surveillance Act, the government has been permitted to come to the secret court and obtain permission to install wiretaps and conduct searches without notice to the target and without showing probable cause of a crime. The purpose of the surveillance or search had to be to gather foreign intelligence, and not to solve domestic crimes. Because the targets were agents of foreign powers and there was no domestic law enforcement purpose to the surveillance or search, the traditional requirements of notice to the target and demonstration to a magistrate that there was probable cause of criminal conduct were not viewed as essential for these intelligence-gathering activities.

In the Patriot Act, an apparently simple and inconsequential change in wording—from “the purpose” to “a significant purpose”—has been construed by the Justice Department and a FISA review court to permit the government to use the secretive and less protective FISC and FISA to get warrants, even where the overriding purpose for the surveillance is to obtain foreign intelligence information. As the Justice Department and other supporters of the change point out, national secu-

rity crimes—particularly terrorism crimes—have mushroomed in recent years. Thus, the search for intelligence related to security and terrorism and investigations of criminal conduct are intertwined to such an extent that requiring separate procedures and separate investigative teams was hindering effectiveness.

The effect of this Patriot Act amendment on FISA was widely perceived as tearing down “the wall” separating law enforcement and intelligence gathering. Intelligence information can be shared with criminal investigators, and law enforcement information can be given to intelligence investigators. This sharing of information was reinforced by a related Patriot Act provision that makes information sharing an express power.

National Security Letters

When citizens provide private information to third parties—banks, and telephone and Internet companies, for example—courts have held that there is no privacy interest that stands in the way of the third party transferring that information to the government. Before the Patriot Act, the government had authority to issue “national security letters” (NSLs) to force financial institutions and telephone companies to release information concerning their customers. However, the government had to have “specific and articulable facts” to show that the customer whose records were sought was an agent of a foreign power. Under the Patriot Act, the factual predicate was loosened considerably, so now to obtain an NSL the government merely has to show that the credit reports, banking records, or telephone and e-mail logs are “relevant” to an authorized intelligence investigation. The NSL is issued by the FBI, and no court approves in advance or certifies afterward that the legal requirements have been met.

Although the NSL provision was not subject to the 2005 sunset, Congress amended the NSL provision in 2006 to rescind a requirement that the recipient of a NSL not communicate with anyone, even a lawyer, about its receipt. In addition, Congress may provide the NSL recipient with an opportunity to seek judicial review of the NSL before complying with its terms to determine that the request meets the “relevance” standard and does not otherwise violate the rights of the recipient.

The Crime of “Domestic Terrorism”

For the first time in our nation’s history, Congress provided through the Patriot Act a law enforcement means for charging citizens thought to be engaged in terrorist activity. The crime of “domestic terrorism” includes “acts dangerous to human life” that otherwise violate federal law and that “appear to be intended . . . to influence the policy of a government by intimidation or coercion” and occur primarily inside the United States. Critics of the new crime assert that government could use the law to justify investigations and prosecutions of political activists and nonprofit organizations that are opposed to government policies. They worry that civil disobedience and nonviolent protest could be construed as acts that “appear to be intended . . . to influence . . . government by intimidation or coercion” and that are “dangerous to human life.” Government supporters answer that these fears are misplaced, and that peaceful groups who do not otherwise break laws will not be perceived as committing the new crime. Although the



new crime was one of those provisions due to expire at the end of 2005, it was made permanent in the 2006 legislation.

See also: **Banking and financial records; Constitutional protections; Disclosure; Library records; Search warrant**

Suggested Reading: American Civil Liberties Union. *Reform the Patriot Act—Don't Expand It!* <http://action.aclu.org>. Online, April 2006; Heritage Foundation. *The Patriot Act and Related Provisions: The Heritage Foundation's Research*. www.heritage.org/Research/VHomelandDefense/wm612.cfm. Online, January 2006; Perrine, James B. "The USA Patriot Act: Big Brother or Business as Usual?" *Notre Dame Journal of Law, Ethics & Public Policy* 19 (2005); Schulhofer, Stephen J. *Rethinking the Patriot Act: Keeping America Safe and Free*. New York: Century Foundation Press, 2005; Soma, John T., Maury M. Nichols, Stephen D. Rynerson, Lance A. Maish, and Jon David Rogers. "Balance of Privacy v. Security: A Historical Perspective of the USA Patriot Act," *Rutgers Computer & Technology Law Journal* 31 (2005): 285; Wood Michael J. "Counterintelligence and Access to Transactional Records: A Practical History of USA Patriot Act Section 215," *Journal of National Security Law & Policy* 37 (2005).

William C. Banks

Upskirting. *See* **Surveillance cameras; Voyeurism**

Urine analysis

Drug testing programs operate in two general contexts: to deter drug use, or punish it; and, to assist in treatment and rehabilitation. Programs may administer urine tests periodically, randomly, or only in response to accidents or incidents in which drug use is suspected. Privacy interests differ between settings, but their combined effect is a generalized form of social control that is based on everyday **surveillance** of bodily fluids once thought to be private. Positive tests in workplace drug testing programs may lead either to job loss or disciplinary action, or to enrollment in employee assistance programs. Consequences are especially negative in social services or criminal justice settings, where the results of a positive toxicology screen may lead to loss of child custody or even of liberty itself.

Urine testing is currently the most widely accepted and practiced form of testing used to determine whether individuals have recently ingested illegal drugs. More than 90 percent of drug testing is accomplished via urine testing as opposed to one of the "alternative" testing modes (saliva, sweat, or hair analysis). Civil libertarians resist urine testing on privacy grounds, citing both the act of urine testing itself and the use of findings as incursions into the protected **zone of privacy**. Despite their concerns, urine testing has been institutionalized throughout several major social institutions in the United States, bringing the habits of millions of people under surveillance. Two conditions enabled urine testing to become widespread in the United States: judicial acceptance of the results and administrative changes. Testing is most common in a few economic sectors, most notably transportation, which exhibits the highest rates of random urine testing.

Since its humble beginnings in the 1970s, urine testing has become a \$5.9 billion industry. Individual tests currently cost \$25 to \$32. The industry has spawned a professional association, the Drug and Alcohol Testing Industry Association,

with more than 1,200 members and an allied industry to analyze the results. Laboratories that analyze the results of urine tests are subject to regulation by the National Institutes of Drug Abuse (NIDA), which operates a national certification program to ensure that laboratories comply with mandatory guidelines. The industry's largest customer is the federal government, seeking to comply with its own drug-free workplace regulations.

Urine tests establish the presence of metabolites, not the presence of drugs themselves. Its scientific basis was established in the late 1960s, but not until the early 1980s was EMIT, an enzyme-based assay still in use today, accurate enough for organizations to risk court challenges in response to its use. Accurate urine testing requires two steps. First, preliminary screening through radioimmunoassays, enzyme immunoassays, fluorescence polarization immunoassays, and/or thin-layer chromatography is used to identify samples that may be positive. The second step uses a more specific methodology: gas chromatography with mass spectrometry (GC/MS), which confirms or disconfirms the results of the first step. Thus, there is room for error and interpretation. Enzyme-based urine testing often yields false positives, and there is always the possibility of environmental contamination, tampering, or human error. Urine tests are generally used to test for marijuana, cocaine, methamphetamine, PCP, and opiates. They are generally not used to screen for legal drugs such as alcohol or tobacco. Drug tests cannot document habitual drug use or impairment on the job. The window during which episodic drug use remains detectable varies by drug and by the testing technology used. The validity of the results also varies. However, the technology itself has become less cumbersome and expensive over time. Today, urine testing kits are relatively easy to use and accurate compared with their antecedents. Their ease of use has enabled the extension of surveillance even further into the population.

Although urine testing began in drug treatment settings in the late 1960s and early 1970s, the U.S. Armed Forces first scaled it up. The military turned to mass testing due to problems with heroin addiction in combat units during the Vietnam conflict. Veterans' organizations and unions challenged the Army Drug and Alcohol Abuse Prevention Program in a series of cases in the mid-1970s. The first court challenges led to recognition that urine tests were a form of "search and seizure" that implicated the Fourth Amendment of the U.S. Constitution. Fourth Amendment cases concern "warrantless" searches. Urine testing programs are considered constitutional, despite the routine testing of individuals who are under no suspicion of drug use (and where there is no "probable cause"). The Supreme Court enabled broader testing of workers after accidents in *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602 (1989). The courts implemented "balancing tests" to ensure that testing is conducted for purposes other than criminal prosecution (which would contradict the presumption of innocence). These tests seek to "balance the individual's privacy expectations against the government's interests" (*National Treasury Employees Union v. Von Raab*, (1989)). Government interests were found to outweigh individual privacy interests in *Von Raab*, which involved U.S. Customs Agents.

The principal at issue in cases of this kind is whether a greater social good outweighs an individual's **reasonable expectation of privacy**. Urine tests are considered legally "reasonable" infringements on the privacy of some groups, such as

U.S. Customs employees, who have a “diminished expectation of privacy in respect to the intrusions occasioned by a urine test” (*National Treasury Employees Union v. Von Raab*, 489 U.S. 669 (1989)). Opinions in these cases generally interpret urine testing as a way of detecting fitness for duty and soundness of judgment.

Military urine testing programs survived their earliest court challenges, so the stance behind them was later extended to the federal workplace under the direction of Reagan administration drug czar Carlton Turner. Eventually, urine testing programs made their way into transportation, health care delivery, and educational settings. In 1986, President Ronald Reagan issued Executive Order 12564, which required federal agencies to urine-test with the goal of guaranteeing a “drug-free federal workplace.” Urine testing became commonplace in federally regulated U.S. workplaces and educational institutions, and later in medium to large private-sector organizations. When the American Management Association (AMA) first surveyed its members’ corporate drug policies in 1987, only 21 percent had testing programs. Despite the expense of testing, that figure rose to 81 percent of major U.S. firms by 1996. Additionally, school districts began urine testing programs, and they also have survived challenges.

In 1997, for the first time, the U.S. Supreme Court demarcated a boundary between permissible and impermissible urine-testing programs (*Chandler v. Miller*, 117 U.S. 1295 (1997)). Permissible searches are those that are based on individual suspicion as opposed to subjecting an entire “suspect class” to blanket testing. Lack of clarity about what was permissible, and the overall expense of programs that have relatively low rates of success at identifying drug users, have deterred some employers and school districts from continuing their urine testing programs. The effects of urine testing programs on workplace safety and productivity have been negligible. Despite its presence in the military and the schools, the bulk of urine testing continues to occur in workplace settings due to federal support and subsidies for testing programs there.

Workplace drug testing may take place at several points: during the hiring or, “pre-employment” phase; once an individual is on the job, particularly if there is an accident or safety-related incident that provokes a higher level of scrutiny; or, through random testing once on the job. The criminal justice system is another locus for urine testing, especially for individuals involved in community corrections programs and drug courts, where urine testing has become increasingly common. Medical institutions also have begun to extend routine urine testing beyond diagnosis and monitoring for infection to testing for illegal drugs in the case of pregnant women. The city of Charleston, South Carolina, developed a program that led to pregnant and recently postpartum women being charged with drug crimes based on a single positive urine test conducted in the routine course of their medical care. The Charleston Police Department had never arrested a male patient and charged him with possessing drugs on the basis of a single positive urine test. The U.S. Supreme Court, however, ruled that urine-testing pregnant women without their knowledge or consent constituted an unlawful search and seizure that violated the Fourth Amendment (*Ferguson v. City of Charleston*, 532 U.S. 67 (2001)). The outcome of this case suggests that there are times when privacy interests outweigh state interests.

See also: **Blood testing; *United States. v. Scheffer*, 523 U.S. 303 (1998); Workplace privacy**

Suggested Reading: American Civil Liberties Union. *Drug Testing: A Bad Investment*. New York: ACLU, 1999; Gilliom, John. *Surveillance, Privacy, and the Law: Employee Drug Testing and the Politics of Social Control*. Ann Arbor: University of Michigan Press, 1994; Massing, Michael. *The Fix*. New York: Simon & Schuster, 1998; Normand, Jacques. *Under the Influence? Drugs and the American Workforce*. Washington, DC: National Academy Press, 1994; Staples, William G. *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. Lanham, MD: Rowman & Littlefield, 2000; Tunnell, Kenneth. *Pissing on Demand*. New York: New York University, 2004.

Nancy D. Campbell

V



Vernonia School District v. Wayne Acton, 515 U.S. 646 (1995)

In the late 1980s, the Vernonia (Oregon) School District perceived an increase in drug and alcohol use among its students and quickly took measures to address the problem. The district implemented drug education classes and used drug-sniffing canines to help detect the presence of drugs on school campuses. Acting on the administrators' claim that student athletes were heavily involved in the drug culture, the district held a parent meeting to discuss a new drug policy that would require athletes to submit to a **urine analysis** at the beginning of every sport season. The proposal also required an additional submission, once a week, by 10 percent of the athletes chosen at random. In addition, athletes would be required to provide a doctor's authorization for any medication they were taking at the time of a drug exam. To maintain personal privacy, the urine samples of male athletes would be collected while they were fully clothed, with back turned, and at a distance of 12 to 15 feet from a monitor of the same sex. Female athletes produced their samples inside an enclosed bathroom stall while being monitored audibly by a person of the same sex from outside the stall. The sample would then be sent to a laboratory and analyzed for the presence of marijuana, amphetamines, and cocaine. The parents unanimously agreed to the new policy.

In the fall of 1991, the respondent, James Acton, was denied the right to play football because he and his parents refused to sign the new policy's consent forms. An action was filed against the district claiming that the policy violated the Fourth and Fourteenth Amendment protection against unreasonable searches and seizures. The district court quickly struck down the claim. Upon appeal, the Ninth Circuit reversed the district court's decision, holding that the policy was, in fact, a breach of Fourth and Fourteenth Amendment protection from searches and seizures without due process.

The United States Supreme Court granted a hearing of this case under a writ of certiorari. The Court argued that the protection given by the Fourth Amendment, and ratified to the states through the Fourteenth Amendment, is only given for searches and seizures that are unreasonable. To determine whether a particular search is unreasonable, the Court must balance the extent of Fourth Amendment



intrusion against society's benefit or need. Typically, probable cause is required to establish the reasonableness of a particular search. However, under certain circumstances, the Court has allowed searches to be conducted without probable cause if the circumstances were exigent or special in nature.

The Court held that the interests of public schools exist in an area of law where the special needs of the school outweigh the need for probable cause before conducting searches. The Court has long held that because public schools have been given the temporary custody of children, they have also been given the responsibility and authority to protect the well-being of those children. In normal circumstances the submission of urine analyses would be deemed unconstitutional if requested at random and without any probable cause. However, schools have the authority to require rules of conduct and to maintain a degree of control that would not be allowed in normal circumstances.

The Court decided that the expectation of privacy is naturally diminished when athletes choose to participate in a sport. Locker and dressing room activities, as well as preseason physical exams, automatically reduce athletes' **reasonable expectation of privacy**. Because the submission of a drug sample is conducted in such a way as to limit the further intrusion of privacy, the policy was an acceptable means to the ultimate intention of the district's policy. The Court viewed the submission of samples by both male and female athletes as nearly identical to the conditions that students are exposed to every day while using the public **restrooms**. Therefore, the way in which the submissions were conducted was not unreasonable and did not violate the students' Fourth Amendment rights.

The Court also found that requiring the proof of medical authorization for the use of prescription drugs was, likewise, not a violation of the students' Fourth Amendment rights. The policy did permit student athletes to provide the required information directly to the laboratory in a sealed envelope, thus maintaining the same standard of medical privacy that the student is provided under everyday protection.

In this case the Court balanced the randomness of the searches, the intrusiveness of the searches, and the expectation of medical privacy against the district's need to halt a rising drug epidemic and decided that the policy only slightly intruded on the students' rights under the Fourth Amendment. The Court ruled that the policy's slight intrusion into the privacy of athletes was greatly outweighed by the need for the district to ensure the safety of students.

See also: **Blood testing; Drug testing; Family; Privacy, definition of; Private parts; Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 (1989); Surveillance; United States v. Scheffer, 523 U.S. 303 (1998); Workplace privacy**

Suggested Reading: American Civil Liberties Union. *Drug Testing: A Bad Investment*. New York: ACLU, 1999; Staples, William G. *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. Lanham, MD: Rowman & Littlefield, 2000; Tunnell, Kenneth. *Pissing on Demand*. New York: New York University Press, 2004.

Sean M. Peek

Video Privacy Protection Act of 1988

After a list of Robert Bork's video rentals was published in a newspaper during his failed Supreme Court confirmation hearings in 1988, Congress took swift action and

passed the Video Privacy Protection Act of 1988 (VPPA), 18 U.S.C. §2710. The act prohibits videotape service providers from knowingly disclosing information regarding a consumer's rental or purchase of "prerecorded videocassette tapes or similar audiovisual materials." **Disclosure** of the names and addresses of customers is permissible under the act if the customer is given the chance to prevent such disclosure (the opportunity to "**opt out**"). Disclosure of rental or purchase habits is permissible if the customer consents; in such cases, it is not sufficient for the videotape service provider to obtain consent via a membership sign-up form or some other document that was signed by the customer prior to the request for disclosure. Rather, the customer's consent must be given at the time the disclosure is requested.

An important exception to these general prohibitions on disclosure is that videotape service providers may disclose the subject matter of a customer's videos if it is for the exclusive use of marketing goods and services directly to the consumer. In other words, the renting habits of customers may be shared with other companies for marketing purposes.

Videotape service providers may also disclose customer records to law enforcement officials pursuant to a warrant, a grand jury subpoena, or a court order. If law enforcement officials seek disclosure pursuant to a court order, they are required to give the customer prior notice; moreover, they must show that there is probable cause to believe that the information they seek to obtain is relevant to a law enforcement inquiry.

In civil proceedings where a person seeks the disclosure of video rental or purchase information by court order, the individual whose information is at issue is afforded certain protections: he or she must be given reasonable notice by the person seeking disclosure and must be given an opportunity to appear in court to challenge that person's claim.

All records pertaining to a customer's purchase or rental habits generally must be destroyed one year after the information is no longer necessary for the purpose for which it was collected. This has been construed to mean one year after a customer terminates his or her account. Individuals whose privacy has been violated by transgression of the act may bring a federal civil action for damages. However, prevailing in such an action would likely prove difficult because the customer must show that the videotape service provider *knowingly* made improper disclosures.

Moreover, because the remedy for violations of the act is a private remedy, customers must self-police the privacy practices of videotape service providers. Such self-policing is difficult because there is no provision in the VPPA that requires videotape service providers to disclose information regarding their handling of a customer's information if a customer makes a request for such information. However, a number of states have passed videotape privacy statutes that are more stringent than the federal VPPA.

Although it is unclear whether the act applies to DVDs and video games, most commentators agree that the language of the statute extends the act's scope to both DVDs and video games. An unsettled question is how the VPPA interacts with the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)**, which allows law enforcement officials to obtain individuals' purchasing information if it is "in the course of an ongoing investigation"; this represents a much lower standard than the requirement for issuance of a warrant: probable cause.

See also: *Camfield v. City of Oklahoma City*, 248 F.3d 1214 (2001); **Search warrant; Surveillance**

Suggested Reading: Electronic Privacy Information Center. www.epic.org; Solove, Daniel J. "The Origins and Growth of Information Privacy Law," *Practicing Law Institute* 828 (2005): 23–67.

Marcy E. Peek

***Village of Bella Terre v. Borass*, 416 U.S. 1 (1974)**

In *Village of Belle Terre v. Borass*, the United States Supreme Court upheld a village zoning ordinance targeting nontraditional residences consisting of more than two unrelated people. The lower courts reached contradictory results based on the challenge to the ordinance under the constitutional right to privacy. After applying the rational basis test, Justice **William O. Douglas**'s majority opinion found that the ordinance was rationally related to a legitimate government interest. Upholding the ordinance, he determined that it did not infringe upon any constitutionally protected fundamental right.

The village of Bella Terre lay on the north shore of Long Island, New York. At the time of the lawsuit before the Court, the village's total land mass of less than one square mile held about 220 homes and 700 people. By ordinance, the village restricted land use "to one-family dwellings excluding lodging houses, boarding houses, fraternity houses, or multiple-dwelling houses." The term "**family**" included "one or more persons related by blood, adoption, or marriage, living and cooking together as a single housekeeping unit, exclusive of household servants. A number of persons but not exceeding two (2) living and cooking together as a single housekeeping unit though not related by blood, adoption or marriage shall be deemed to constitute a family."

The owners of the house, the Dickmans, leased the house to six college students at nearby State University at Stony Brook. None of the six was related to the other through blood, adoption, or marriage, as the ordinance required. Upon finding this out, the village served the Dickmans with an "'Order to Remedy Violations' of the Ordinance." As a result, the Dickmans and three of their six tenants brought an action under 42 U.S.C. §1983 demanding an immediate injunction and judgment to declare the village ordinance unconstitutional.

Upon hearing the challenge, the United States District Court for the Eastern District of New York upheld the ordinance as constitutional (367 F. Supp. 136), but the Court of Appeals, Second Circuit (476 F.2d 806), reversed that decision. The village appealed to the United States Supreme Court, which heard the case in 1971 and rendered its decision reversing the Court of Appeals.

Justice Douglas's majority opinion began by examining several recent zoning ordinance cases that had come under scrutiny before the Supreme Court. Because of the importance of remaining consistent with its earlier decision, the Court attempted to analogize the similarities or explain the differences of earlier cases in line with this one. Given that this ordinance was not identical in its restrictions to any other ordinance previously before the Supreme Court, Justice Douglas had to engage in a fresh analysis of the constitutional challenges to the Village of Bella Terre's housing ordinance.

The majority opinion began by addressing the challenges to the ordinance. Justice Douglas identified the following challenges made against the constitutionality of the

ordinance: that it interferes with a person's right to travel; that it interferes with the right to migrate to and settle within a state; that it bars people who are uncongenial to the present residents; that it expresses the social preferences of the residents for groups that will be congenial to them; that social homogeneity is not a legitimate interest of government; that the restriction of those whom the neighbors do not like trenches on the newcomers' rights of privacy; that it is of no rightful concern to villagers whether the residents are married or unmarried; and that the ordinance is antithetical to the nation's experience, ideology, and self-perception as an open, egalitarian, and integrated society.

Upon examining each of these challenges, Justice Douglas found that none applied to the ordinance. Citing earlier cases decided by the Supreme Court, he found that the ordinance was not aimed at transients and that it did not target a "fundamental" right guaranteed by the Constitution, such as voting, free association, access to the courts, "or any rights of privacy."

The majority's most powerful argument focused on the role of the courts in seeking to invalidate laws enacted by legislative bodies. The Court accepted that the "line drawn" against more than two unrelated people living in a house together might seem arbitrary or random. The Court entertained the question of why not three or four or more people. However, the Court responded that "every line drawn by a legislature leaves some out that might well have been included. That exercise of discretion, however, is a legislative, not a judicial, function." Thus, the Supreme Court was reluctant to second-guess a legislature in making a judgment call. Although the line drawn seemed arbitrary, the Supreme Court decided that every line had to be drawn somewhere.

Finally, the Court ruled that the ordinance was rationally related to a legitimate government interest. This is the hallmark formulation of the so-called rational basis test. It is the easiest form of constitutional scrutiny for a government regulation to meet, and in this case the Supreme Court upheld the zoning ordinance under this very permissive standard. The majority declared, "A quiet place where yards are wide, people few, and motor vehicles restricted are legitimate guidelines in a land-use project addressed to family needs." Because the Supreme Court did not find that the village's zoning ordinance infringed upon the right of privacy, the right of **freedom of association**, or any other constitutionally protected right, the ordinance survived the Court's scrutiny.

See also: **Constitutional protections; Home; Privacy, philosophical foundations of; Reasonable expectation of privacy**

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Hall, Kermit L. *Conscience, Expression and Privacy: The Supreme Court in American Society*. New York: Garland, 2000.

Ryan C. Hudson

Voice identification

Alexander Graham Bell's father envisioned that a person could be identified by the sound of his or her voice. The concept was to create a visual representation of the spoken word based on subtle differences in pronunciation. In 1941, Bell Telephone in New Jersey produced a sound spectrograph for mapping a voice on a



graph by analyzing sound waves based on frequency, intensity, and time. The original purpose was to assist in enabling deaf people to speak. During World War II, the government began using the technology to identify enemy voices on telephones and radios. Currently the **National Security Agency** uses the software to assist in electronic espionage.

Biometric identification using speech is particularly appealing because it is minimally intrusive. As with **fingerprints**, a suspect's voice can be compelled for the purpose of comparison without violating his or her Fifth Amendment rights (see *United States v. Dionisio*, 410 U.S. 1 (1973)). An individual's voice contains enough individually unique characteristics to distinguish it from others through analysis. In court situations, the standard for admissibility of an opinion as to the identity of a speaker is merely that the identifier has heard the voice of the alleged speaker at any time. The spectrogram assists the process by graphically displaying sound in three dimensions: pitch, resonating characteristics, and rate of speech.

However, use of the spectrogram presents several challenges. Voiceprints, unlike fingerprints, are not static. Fingerprint ridge details exist from cradle to grave. The human voice, however, changes with factors such as age, stress, and health. Additionally, the process suffers when transmission quality is poor or when ambient noise is present. The accuracy of voice identification depends on the conditions under which the voice samples are made, the characteristics of the equipment used, and the skill of the examiner. Although there is disagreement within the scientific community on the accuracy of voice verification authentication, today's voiceprint technology has advanced to the degree that several circuit courts now allow comparisons of the spectrogram of an unidentified speaker with that of an identified speaker in order to find similar patterns as admissible scientific evidence.

See also: **Electronic surveillance**

Suggested Reading: Ramsland, Katherine. *The Origins of Voiceprints*. www.crimelibrary.com. Online, December 2005.

Jill Joline Myers

Voyeurism

Voyeurism is deriving sexual pleasure by secretly peering into the private affairs of another individual, often while the other individual is disrobing or engaging in a sexual act. Clinically, voyeurism is considered a type of paraphilia, a disorder in which an individual has difficulty controlling certain sexual impulses that are considered antisocial.

A central trait of voyeurism is that the observer or "voyeur" achieves sexual gratification by seeking out opportunities secretly and furtively to observe another person. In essence, a voyeur spies on an unsuspecting victim to fulfill a sexual fantasy, which often may be accompanied by autoeroticism. The more severe and compulsive these impulses are, the more likely they are to lead to difficulty functioning normally within society.

Typically, the victim of voyeurism has not consented to being observed and often is unaware that his or her privacy is being surreptitiously invaded. For this reason, voyeurism is considered to be inappropriate, even deviant, conduct and is often illegal. Voyeurism may also involve **trespassing** and/or creating video or

audio recordings of the spied-on individual. Typically, voyeurism is most often associated with males in their 20s and 30s. Examples of paraphilias other than voyeurism include fetishism, exhibitionism, sadomasochism, bestiality, and pedophilia.

Although there is no uniform definition of privacy, it is generally accepted that it includes the desire to shield one's body, including genitalia or **private parts**, as well as certain activities—ranging from engaging in sexual conduct, to bathing, to trying on clothing in a retail dressing room—from the **plain view** of others. For example, people ordinarily seek and expect privacy when entering their own **home**, when closing a bathroom or bedroom door, or when taking any other, similar measures to limit the access of other people to their body and personal space. Notions of sexual conduct, nakedness, and certain bodily functions innately invoke a sense of privacy; in fact, their public display is often considered taboo.

Voyeurism is considered to be antisocial because it violates this expectation of privacy. The classic term for a voyeur is “peeping tom.” A peeping tom is an individual who hides and spies on another person with the intent to invade the victim's privacy, typically by watching that person while he or she is naked, undressing, or exposing his or her genitalia.

The phrase “peeping tom” has its origins in English mythology. During the eleventh century, a beautiful noblewoman, Lady Godiva, lived in the city of Coventry. According to legend, she became engaged in a dispute with her husband, Leofric, the Earl of Mercia, over an oppressive tax he levied on the people of Coventry. According to the story, Lady Godiva rode naked on horseback through the city streets in protest of this tax. Although the townspeople were ordered to stay indoors and not to look upon Lady Godiva, one man, named Tom, disobeyed this proclamation. Apparently, Tom peered at the naked Lady Godiva through a hole he carved in his window shutters. As the legend has it, the tax was lifted, but Tom, forever branded as Peeping Tom, was blinded as punishment.

While a voyeur, or peeping tom, typically does not come into direct physical contact with his victim, the act of peeping, without consent to do so, into another person's private affairs is generally considered to be invasive. It often causes feelings of shame, humiliation, distrust, and violation in the victim. For this reason, voyeurism has long been prohibited by laws regarding secret peeping, window peeking, indecent viewing, or eavesdropping. These statutes seek to protect an individual's right to privacy from unauthorized infringement by a voyeur, and often they give rise to both criminal and civil liability.

As a general matter, criminal law seeks to protect the greater public by prohibiting certain antisocial behaviors, such as voyeurism, and by establishing a system of punishment for breaking the law. As a companion measure, civil law seeks to provide a tort remedy through which a victim of voyeurism may seek compensation and redress against an infringing voyeur. Both criminal and civil law generally hold that the right to privacy is compromised when a voyeur intentionally and nonconsensually peers upon another person's body or intimate bodily acts.

Unlike Lady Godiva, most victims of voyeurism never anticipate that their body, their genitals, or their sexual acts will be viewed by an interloper. Voyeurism, by its very nature, is a form of spying and is designed to pierce the veil of protection that a victim has implemented to protect his or her body from disclosure to the outside

world, whether that barrier is clothing, a closed bedroom door, a drawn shower curtain, or a privacy fence. Voyeurism is considered offensive because a voyeur seeks to circumvent these privacy barriers. For example, a voyeur often may trespass to peer inside a window, may use binoculars to view a victim from a distance, or may employ a **cellular telephone** camera to capture images under or through a victim's clothing as he or she walks along a public street.

In fact, with the proliferation of video **surveillance** and micro-camera technology, the impact and the incidence of voyeurism have magnified. Video voyeurism is voyeurism involving the filming or recording of another person by use of a camera or other image-recording device. With the aid of modern technology, the video voyeur has the means to create a permanent record of the voyeuristic invasion, one that is capable of repeated viewing and is easily disseminated to others across the **Internet**.

Video voyeurs frequently use compact, hidden video surveillance equipment to record surreptitious images of unsuspecting victims, typically women. For example, the Internet is well populated with "up-skirt" and "down blouse" images, video images taken up a woman's skirt to view her underwear or down a woman's blouse to view her unclothed upper body. Unlike the traditionally solitary act of voyeurism, the video voyeur can broadcast these privacy intrusions to a potentially wide audience.

The term "voyeurism" has also been used more generally within popular culture to describe the act of deriving pleasure, but not necessarily sexual pleasure, from peering into the affairs of others. The affairs may or may not be private, and the peering may or may not be secretive. This derivative understanding of voyeurism is commonly used to describe such societal behaviors as watching reality television, reading **gossip** news stories, observing 24-hour Internet webcams, and being fascinated with the lives of the rich and famous. Voyeurism in this context is generally used to describe an interest in sensational, but not necessarily sordid, topics. Because of the proliferation of video surveillance technology and the acceptance of its legitimate uses in the mainstream of society, particularly in the news media, this alternative usage of the term "voyeurism" has increased.

See also: **Manners; Privacy, definition of; Restrooms and dressing rooms; Surveillance cameras**

Suggested Reading: Alderman, Ellen, and Caroline Kennedy. *The Right to Privacy*. New York: Alfred A. Knopf, 1995; Aries, Philippe, and Georges Duby. *A History of Private Life, Volumes I–V*. Cambridge, MA: Belknap Press, 1992; Ku, Alan Kato. "Talk Is Cheap, but a Picture Is Worth a Thousand Words: Privacy Rights in the Era of Camera Phone Technology," *Santa Clara Law Review* 45 (2005): 679; McClurg, Andrew. "Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places," *North Carolina Law Review* 73 (1995): 989; *Paraphilias*. www.webmd.com. Online, April 2006; Vitale, Antonietta. "Video Voyeurism and the Right to Privacy: The Time for Federal Legislation Is Now," *Seton Hall Legislative Journal* 27 (2003): 381.

Lance E. Rothenberg

W



***Warden v. Hayden*, 387 U.S. 294 (1967)**

In March 1962, an armed robber entered the Diamond Cab Company in Baltimore, Maryland. The robber made off with several hundred dollars but was followed by two cab drivers to a house on Cocoa Lane. One driver radioed a description to the company dispatcher, who then relayed the information to the police. Within minutes, the police arrived at the **home**, knocked on the door, and announced their presence. Mrs. Hayden answered the door and offered no objection to a search when the police asked to search the house for the robber. The officers spread throughout the house in search of the robber and found him in an upstairs bedroom. During the search for the robber, officers in other parts of the house uncovered several items of evidence. One officer discovered a shotgun and pistol in a toilet tank; another officer found a jacket and trousers matching the robber's description in the washing machine; and another found ammunition and a cap under Hayden's mattress. All of the items recovered were introduced against Hayden at trial. The officers testified that they were looking for either the man or the money in their respective searches of the house.

In Hayden's habeas corpus petition, relying on *Harris v. United States*, **331 U.S. 145 (1947)**, the petitioner contended that the clothing seized was improperly admitted into evidence because the items had "evidential value only" and therefore were not lawfully subject to seizure. In *Harris*, the principal issue was whether a search could be regarded as incident to lawful arrest when the suspect was already in custody before the search was made and any evidence had been seized.

The question before the Court was whether the seizure of the clothes violated the Fourth Amendment because the items are considered to be mere evidence. In its analysis, the Court distinguished Hayden's case from the *Harris* case. In the case at hand, the searches occurred prior to or contemporaneous with the arrest of Hayden. The Court reasoned that the police acted reasonably when they entered the house and began looking for the suspect and for any weapons he had used in the robbery or that he might use against the police. The Fourth Amendment does not require the police to halt an investigation if, in doing so, they would gravely endanger their

lives or the lives of others. The Court reasoned that the search conducted by the police was the only way to ensure that the suspect was alone and that the police had control of all the weapons that could be used against them or for an escape. The Court rejected arguments that the officer who seized the clothing in the washing machine was not looking for the suspect or weapons. Instead, the Court made the logical inference that the officer was in search of weapons.

The Court then turned to the distinction between seizure of items of evidential value and seizure of instrumentalities, fruits, or contraband. The Court found that the language of the Fourth Amendment provided for no distinction between the notion of **mere evidence** and that of instrumentalities, fruits, and contraband; the requirements of the Fourth Amendment secure the same protection of privacy for both. The Court did acknowledge that there must be a nexus, or common set of facts, events, or circumstances, provided in the case of seizure of fruits, instrumentalities, or contraband between the item to be seized and criminal behavior. Therefore, in the case of “mere evidence,” probable cause must be examined in terms of cause to believe that the evidence sought will aid in a particular apprehension or conviction; thus the purposes of a police search must be considered. In this particular case, the clothes found in the washing machine matched the description given to the police and thus could be used to help police identify the suspect.

Launching into a history of warrants in both English and American jurisprudence, the Court dismissed the distinction between the two types of seizure, stating that it was unsupported by language in the Fourth Amendment. To the Court, the right of privacy is disturbed to the same degree in both instances, and thus the clothing seized in Hayden’s house was admissible, regardless of the purpose for which it was seized.

The dissent, given by Justice **William O. Douglas**, viewed the question before the Court differently. The question, in the eyes of Douglas, was whether the government could lawfully seize testimonial evidence pursuant to a proper **search warrant**, to be used at a trial, where otherwise the Fifth Amendment would bar such evidence. Douglas viewed the evidence of the clothing as testimonial because it identified the suspect, and the suspect should be free from such evidence viewed as self-incriminatory.

See also: California v. Ciraolo, 476 U.S. 207 (1986); *Chimel v. California*, 395 U.S. 752 (1969); **Constitutional protections**; *Curtilage*; *Oliver v. United States*, 466 U.S. 170 (1984); *Payton v. New York*, 445 U.S. 573 (1980); **Reasonable expectation of privacy**; **Trespass**; *United States v. Dunn*, 480 U.S. 294 (1987); *Weeks v. United States*, 232 U.S. 383 (1914)

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black’s Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Hall, Kermit L. *Conscience, Expression and Privacy: The Supreme Court in American Society*. New York: Garland, 2000; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

Matthew M. Dwyer

Warrantless search. See Search warrant***Washington et al. v. Glucksberg et al.*, 521 U.S. 702 (1997)**

Glucksberg was a doctor in the state of Washington. Along with several other physicians, a few terminally ill patients who later died, and a nonprofit organization, Glucksberg brought suit challenging the state's ban on physician-assisted suicide.

The question before the Court was whether the state's ban on physician-assisted suicide violated the Fourteenth Amendment Due Process Clause by denying terminally ill adults the right to choose death over life. Using a two-part analysis, the Supreme Court held that the statute was constitutional. The Court interpreted the statute using a historical, contextual test as well as a rationality test. Both parts of the analysis achieved the same result.

Washington's suicide assistance statute made it a felony to knowingly cause or aid another person to attempt suicide. In its examination of the history surrounding suicide assistance statutes, the Court stated that for over 700 years Anglo-American common law has disapproved or punished suicide or the assistance thereof. However, such prohibitions have never been considered in light of those people near death. But in recent years this incongruity has been re-assessed, culminating with the presidential signing of the Federal Assistance Suicide Funding Restriction Act in 1997. The law prohibited the use of federal funds to perform or support physician-assisted suicide. Therefore, the Court reasoned that suicide has been prohibited in Anglo-American law and saw no constitutional purpose in deviating from that historical norm.

The next step of the Court's two-part analysis was a rationale test. The Due Process Clause was intended to protect fundamental rights and liberties. Given the historical perspective of suicide, the Court reasoned that there existed no right to assistance in committing suicide. To suggest the alternative would violate America's traditions and values. It would reverse hundreds of years of practice and doctrine, and it would go against the commonly accepted policy choice of a majority of the states.

In order for Washington's law to pass constitutional muster, it must be substantially related to a governmental interest. The primary interest served by this statute is to preserve human life. Other interests fulfilled include protecting the integrity of the medical profession, preserving the role of doctors as healers rather than killers, preventing the problem of suicide in society, and shielding vulnerable groups and persons from outside pressures to end their lives.

Previous case law, namely *Cruzan v. Director, Missouri Dep't of Health*, 497 U.S. 261 (1990), and *Planned Parenthood of Southeastern Pa. v. Casey*, had no stare decisis effect in the Court's opinion. *Cruzan* focused on the right to refuse hydration and nutrition as the right to refuse medication. Any person may refuse lifesaving treatment at any time as an exercise of his or her personal rights. *Casey* also recognized that many rights, liberties, and interests protected by due process are grounded in the notion of personal autonomy: the notion that individuals are in control of their own bodies and can make personal decisions regarding how they use their bodies. However, the case at hand is distinguishable from these cases.

Glucksberg embraces the dignity of human life. Other cases speak to the right to accept or refuse medication, the right to use birth control, or other such matters. None of the cases relied on by the petitioners deal with the alleged right to end one's life. Granted, refusing lifesaving medication is in fact a means to end one's life; however, it is medication that is being refused, not an affirmative action taking place that would directly result in the termination of human life. Using this reasoning, the Court upheld the constitutionality of the Washington statute that made it a felony to assist in the suicide of another person.

See also: **Right to die**

Suggested Reading: Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Colby, William. *Long Goodbye: The Deaths of Nancy Cruzan*. Carlsbad, CA: Hay House, 2002; Colby, William. *Unplugged: Reclaiming Our Right to Die in America*. New York: AMACOM Books, 2006; Webb, Marilyn. *The Good Death: The American Search to Reshape the End of Life*. New York: Bantam Books, 1997;

Matthew M. Dwyer

***Watkins v. United States*, 354 U.S. 178 (1957)**

In 1954 John Watkins, a labor organizer, appeared in front of the Subcommittee of the Committee on Un-American Activities of the House of Representatives in compliance with a subpoena. The purpose of the committee was to investigate and, in some cases, expose, the activities of members of the Communist Party.

Watkins had either been a member of, or was associated with, several organizations connected with the Communist Party. Between 1935 and 1953, Watkins had been an employee of the International Harvester Company. During the last 11 of those years, he served as an official to the Farm Equipment Workers International Union, later the United Electrical, Radio, and Machine Workers. He later rose to the position of president of District No. 2 of the Farm Equipment Workers. In 1953 he became a labor organizer for the United Automobile Workers International Union. The committee had obtained his name through the testimony of two prior witnesses.

Appearing in front of the committee, Watkins agreed to describe his connections with the Communist Party and to identify its current members. However, he refused to give information concerning individuals who had left the party or who had fallen into disassociation. Watkins argued that such inquiries were beyond the scope and authority of the committee, that they served no public purpose, and that the committee was engaged in a program of exposure for the sake of exposure.

The question before the Court became whether the activities of the **House Un-American Activities Committee (HUAC)** was an unconstitutional exercise of congressional power. The answer the Court gave rests on the principles of the power of Congress and the limitations upon that power. The Court reasoned that every indulgence of legality must be given to the actions of the federal government but that flexibility must give way to unreasonable infringements of constitutional freedoms. The Court further reasoned, however, that there are instances, particularly in pursuit of public need or welfare, when Congress may encroach upon an individual's rights, but these instances must be justified by a specific legislative need. Without such justification, Congress possesses no general authority to expose the private affairs of individ-

uals. Any inquiry made by Congress must be made in relation to a legitimate aim of Congress and not for the sole purpose of public exposure.

Therefore, the Court determined that the committee's actions exceeded the scope of congressional power and that Watkins was within his rights to refuse the inquiries regarding those individuals no longer associated with the Communist Party, because he had not been given enough information revealing the aims of the committee.

The dissent by Justice Clark considered the notion that Watkins was not protecting his won rights under the Fifth Amendment but rather was protecting the private affairs of other individuals, namely his former associates. Because Watkins had already admitted his own involvement, he should not have been allowed to invoke the constitutional rights of another.

Furthermore, Clark pointed out that in his view the committee was acting with complete clarity. To illustrate his point, Clark stated that the purpose and charter of the committee authorized investigation into subversive activity—its extent, character, objects, and diffusion. However, in his analysis Clark ignored the “plain meaning” interpretation given to most statutory language and insisted on a more contextual interpretation. Words such as “un-American” or phrases like “principle of the form of government” may be vague, but still these are fairly well-understood terms, and Clark stated that the Court should give them meaning if it could. In addition, the Court should presume that a legislative body had a legitimate purpose if the language giving it authority could be interpreted to do so. In Clark's view, the chairman of the committee made explicit comments regarding the functions and purposes of the committee. Thus, Watkins should not be exempt from testimony simply because he claimed he was not informed of the committee's intentions.

See also: Confidentiality; Constitutional protections; Disclosure; Federal Bureau of Investigation (FBI); McCarthyism

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Hall, Kermit L. *Conscience, Expression and Privacy: The Supreme Court in American Society*. New York: Garland, 2000; Smith, Robert Ellis. *Compilation of State and Federal Privacy Laws*. Providence, RI: Privacy Journal, 1992.

Matthew M. Dwyer

Web bugs. *See Internet*

Webster v. Reproductive Health Services, 492 U.S. 490 (1989)

This case follows a long line of cases that have been decided since *Roe v. Wade*, 410 U.S. 113 (1973). In 1986 the state of Missouri passed legislation placing restrictions on **abortions** performed in the state. The preamble to the statute stated that life begins at conception, and it put into effect the following limitations: public employees and public facilities were not to be used in performing or assisting abortions unnecessary to save the mother's life, encouragement and counseling to have



abortions were prohibited, and physicians were required to perform viability tests on women who were in their twentieth week of pregnancy or later.

On appeal from the Eighth Circuit, the question before the Supreme Court was whether the Missouri statute restrictions infringed upon the right of privacy or the Equal Protection Clause of the Fourteenth Amendment.

The Supreme Court stated that it need not decide any matters relating to the preamble of the statute. Previous case law stated that no state could justify any abortion regulation otherwise prohibited by *Roe v. Wade* because it embodied that state's view as to when life begins. The preamble, in and of itself, is not regulatory in nature, nor does it state any restrictions in the abortion practice. Rather, the Court held that the language of the preamble was nothing more than a "value judgment." Nothing in prior case law, including *Roe v. Wade*, had barred a state from expressing itself, and until the state applied the preamble to a situation or case, the Court felt it would be inappropriate to address or interpret its meaning.

The Court also considered the subsequent language of the statute. The statute prohibited the use of public employees and facilities for the performance or assistance of abortions. The Court reasoned that the Due Process Clause prevents the state from depriving anyone of life, liberty, or property interests, but it does not give citizens any affirmative right to governmental aid or place any duty upon the state to give it (*DeShaney v. Winnebago County Dept. Social Services*, 489 U.S. 189 (1989)). In other words, this particular provision does not prevent a woman from receiving an abortion; rather, it leaves her with the same choices as if the state had chosen not to run any hospitals. It simply restricts her ability to obtain an abortion from a physician working for a public hospital. The Court simply stated that nothing in the Constitution forces a state to enter or remain in the business of abortion.

For the second part of the statute, the Court used the same reasoning. However, the appellees in the case no longer sought relief under this part of the statute, and therefore the court of appeals was instructed to vacate the district court's judgment with prejudice pertaining to this part of the statute.

The third part of the statute requires a physician, before performing an abortion on an unborn child of 20 gestational weeks or more, to determine if the unborn child is viable. The Court considered this part to be constitutional. The Court determined that the state had a permissible interest in protecting potential human life. The section of the Missouri statute expressly states that Missouri had chosen viability as the point at which its interest in potential life must be protected. Although medical evidence clearly shows that a 20-week-old fetus is not viable, the evidence also clearly showed that there might be a 4-week error in estimating gestational age. Thus, the language of the statute requiring testing at 20 weeks was to compensate for any error in estimating gestational age. Therefore, the last part of the Missouri statute was found to be constitutional.

See also: Constitutional protections; Gender; Privacy, definition of; Reproductive rights; Women and privacy

Suggested Reading: Allen, Anita L. *Uneasy Access: Privacy for Women in a Free Society*. Totowa, NJ: Rowman & Littlefield, 1988; Allen, Anita L. *Why Privacy Isn't Everything: Feminist Reflections on Accountability for Private Life*. Lanham, MD: Rowman & Littlefield, 2003; Allen, Anita, and Erin Mack. "How Privacy Got Its Gender," *Northern Illinois University Law Review* 10 (1990): 441–

454; Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993; Garrow, David J. *Liberty and Sexuality: The Right to Privacy and the Making of Roe v. Wade*. Berkeley: University of California Press, 1998.

Matthew M. Dwyer

***Weeks v. United States*, 232 U.S. 383 (1914)**

Fremont Weeks was indicted for unlawful use of the mails for transporting lottery tickets in violation of federal statute. He was arrested, without a warrant, by a police officer in Kansas City, Missouri, at his place of employment. Other officers had gone to Weeks's house; a neighbor told them where he kept his key, and the officers entered his house. They searched Weeks's room and seized evidence. They turned this evidence over to a United States marshal. Later that same day, the officers returned with the marshal to search for more evidence. The door was answered by a boarder, and the marshal searched Weeks's room again, this time seizing various papers and envelopes. Neither the officers nor the marshal had obtained a **search warrant**. These articles were provided to the district attorney and were offered as evidence against Weeks at his trial. Just before trial, Weeks filed a petition arguing that this property had been seized in violation of the Missouri and the United States Constitutions. He urged the court to order that this property be returned. The trial court ordered the return of all property unrelated to the charges, but it denied his request as to property pertinent to the crimes charged. At trial, Weeks again moved the court to return his property, and again it denied the motion.

The case was eventually appealed to the United States Supreme Court, which delivered an opinion authored by Justice Day. It set out to analyze the case under the Fourth Amendment's guarantee against unreasonable searches and seizures. The Court recited the history of the amendment and its attendant jurisprudence, relying on the 1886 case of *Boyd v. United States*, 116 U.S. 616 (1886). The Court stated that the purpose and effect of the Fourth Amendment is to limit and restrain courts and federal officials from exercising power and authority in violation of its edict: to secure the people, their persons, houses, papers, and effects against unreasonable searches and seizures under the guise of law. The Court noted that this protection extends to all, whether accused of a crime or not, and that courts should not support any tendency of officers and officials to obtain convictions by means of unlawful seizures and forced confessions.

The Court then set out the issue in this case by stating that this case is not an assertion by the government of a right "to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime." Nor is it a case concerning the admissibility of evidence found upon a person and within his control at his otherwise lawful arrest. Rather, the Court held, this case involves the right of a court to retain as evidence the letters and personal correspondence of the accused, seized in his house in his absence and without his authority, by a marshal without a warrant for the search or for the arrest. The Court held that if evidence



could be seized and held in this manner and used against the accused, then the protection of the Fourth Amendment was of no value and may as well be stricken from the Constitution. The efforts of courts, officers, and officials to bring criminals to justice are praiseworthy. These efforts may not, however, sacrifice the fundamental laws of the country in doing so. Here, a warrant was necessary, and the invasion of the sanctity of Weeks's **home** under these circumstances violated Weeks's most basic constitutional rights. Because the evidence used against Weeks would not have come into the possession of the district attorney but for the unlawful search and seizure, the Court reversed the decision and remanded the case for proceedings in accord with its opinion.

See also: California v. Ciraolo, 476 U.S. 207 (1986); *Chimel v. California*, 395 U.S. 752 (1969); **Constitutional protections**; *Curtilage*; *Harris v. United States*, 331 U.S. 145 (1947); *Payton v. New York*, 445 U.S. 573 (1980); **Reasonable expectation of privacy**; **Trespass**; *United States v. Dunn*, 480 U.S. 294 (1987); *Warden v. Hayden*, 387 U.S. 294 (1967)

Suggested Reading: Barteo, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Black, Henry C. *Black's Law Dictionary*, 7th ed. St. Paul, MN: West, 1999; Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000; Hall, Kermit L. *Conscience, Expression and Privacy: The Supreme Court in American Society*. New York: Garland, 2000; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; Pettifor, Bonnie, and Charles E. Petit. *Weeks v. United States: Illegal Search and Seizure*. Berkeley Heights, NJ: Enslow, 2000.

Larkin R. Evans

WHOIS database

WHOIS is the popular label for a variety of **Internet** directories that allow users to find information on individual owners of specific domain names and Internet Protocol (IP) addresses. As the only tool of its kind, it provides fairly limited information (e.g., address, Internet service provider names); however, the program still has been the source of much debate. The WHOIS system is frequently cited in discussions of the relative importance of the First Amendment, intellectual property rights, and privacy on the Internet.

Initially developed during the 1980s as a centralized system to query domain names and other information, the program has grown and changed with the Internet. Today, the WHOIS system primarily operates with information that domain name registrars gather from registrants. While the system is not directly regulated, the providers of its information are; the more than 150 registrars are all accredited and monitored by the Internet Corporation for Assigned Names and Numbers (ICANN). (Regardless of the ICANN standards in place, the veracity of the information found within a WHOIS database is still at times questioned.)

The technology's advocates present the WHOIS database as a highly effective means of fighting fraud, piracy, and trademark infringement on the highly unregulated Internet. It is cited as a source of consumer protection, free information, and accountability. Its critics, however, argue that by readily providing personal infor-

mation on website operators, the WHOIS database may threaten political speech, free expression, and **anonymity** on the Internet. They also note that the WHOIS system has been a lucrative source of information for **electronic mail**, physical mail, and phone solicitors.

Like many contemporary technologies, the WHOIS system faces a pressing challenge to respect the privacy of individuals while also providing open, accurate information to the public.

See also: **Computers; Confidentiality; Public records**

Suggested Reading: Computer Professionals for Social Responsibility. www.cpsr.org. Online, March 2006; Electronic Privacy Information Center. www.epic.org. Online, March 2006; Internet Corporation for Assigned Names and Numbers (ICANN). <http://gnso.icann.org>. Online, March 2006.

Steve Munch

Wiretapping

Law enforcement uses a variety of tools to perform its functions, including conducting investigations and using wire and net taps, called trap-and-trace devices, to monitor or eavesdrop on suspected criminals. Use of such tools raises questions about privacy and the use of information acquired under a wiretap.

Generally, there are three kinds of devices used by law enforcement to eavesdrop: wiretaps, net taps, and Data Collection System 2000, formerly **Carnivore**. A full-content wiretap allows the government to intercept, listen to, and record telephone calls. A net tap is similar to a telephone wiretap, except that the government is intercepting data transmitted over wire or through the air. Net taps can access and record both the **pen register**, which is used to identify which telephone has been called by another phone, and the full content of the data being transmitted. Net taps rely on a variety of filters to search and find targeted information.

Carnivore, renamed Data Collection System (DCS) 2000, is another type of wiretap that the **Federal Bureau of Investigation (FBI)** uses but has not disclosed much about. Carnivore is a packet-filtering program that allows someone to filter and intercept **electronic mail**. Carnivore has “sniffers” that search a computer network for usernames and **passwords**, using sophisticated filters to sift through packets of data and siphon out the relevant information from the irrelevant. Carnivore has both pen register and full-content wiretap capabilities but must be physically installed at the site, usually that of an Internet service provider (ISP).

The right to privacy or the “**right to be let alone**” is a civil liberty that protects a person from unreasonable searches and seizures by the government. This right is protected by the Fourth Amendment to the U.S. Constitution. Statutory privacy protections generally apply to government action, which means that private companies have much more latitude in what they can do without implicating privacy protections. There are also state rights to privacy and state and federal civil rights statutes that can be enforced to protect privacy interests.

The existence of a recognizable privacy interest turns on whether and the degree to which a person has a reasonable protection of privacy in the place or thing being seized or searched. The U.S. Supreme Court relied on a two-pronged test in the landmark case *Katz v. United States*, **389 U.S. 347 (1967)**, to establish a privacy interest: (1) Does the person have a subjective expectation of privacy in the area

that is being searched, and (2) Is the expectation of privacy one that society is prepared to recognize as being reasonable? While there is a **reasonable expectation of privacy** in some types of communications, such as in letters and telephone calls, courts have generally held that there is no reasonable expectation of privacy in e-mail messages or in activities that occur at school or at the **workplace**, despite the use of a password.

Electronic monitoring at the workplace is common and permissible as long as employees are given advance notice or there are exigent circumstances, such as if the employer has reason to believe the company's interests are in jeopardy. Most employers should have a stated policy on randomly monitoring telephone calls for quality assurance, accessing and reading employees' e-mails, and owning **computer** files of employees. Notice can be provided in employee manuals or other documents that are given or made available to employees. Electronic monitoring and eavesdropping at the workplace have been justified because many workplace crimes, including computer crimes, are committed by employees. Employers are required to post their privacy policy on company websites.

The basic statute regulating wiretaps and **electronic surveillance** is the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §2511, also known as the **Electronic Communication Privacy Act of 1986** (ECPA). ECPA provides broad statutory privacy protection for wireless, wire, and electronic communications and storage of digitized text information, such as e-mail. ECPA prohibits government agents and third parties from intercepting voice and e-mail, accessing and reading e-mail or computer files, and accessing customer records from service providers without the authorization of one of the parties or a court order. Each intrusion is considered separately and therefore requires an independent justification.

Failure to get the required order means that the fruits of the illegal search may be inadmissible in a criminal prosecution. ECPA also authorizes recovery of civil damages for violations of the act. However, if the information is not used for prosecution, there may be no effective remedy for persons whose rights are violated. This issue becomes critical when one is trying to access information for investigation or interrogation purposes that could lead to other information that would be admissible in a criminal prosecution.

To get protection under ECPA, a person must show not only that messages are private, but also that the expectation of privacy is reasonable. ECPA covers only state action and does not cover interception of business e-mail by private persons, often used in commercial espionage. There are three exceptions to ECPA protection: (1) when one party consents; (2) when the provider of the communication service can monitor communications; and (3) when the monitoring is done in the ordinary course of business. ECPA protects both the sender and receiver of public mail and online services and has been extended to electronic communications, bulletin boards, and remote computer services. Statutory damages are limited to \$1,000 for most offenses by government officers.

To conduct a wiretap or net tap, the government is required to show probable cause of criminal activity or probability that a crime will be found. An interception order requires more justification than a **search warrant** because the level of intrusion into a person's privacy is greater. A search warrant is required to access a physical space, a computer, or other device and to read e-mail or the contents of a

communication. Application to the court requires the government to (1) identify who is requesting the order; (2) state the circumstances justifying the order, including the offense and the nature and location of the facilities where the communication is intercepted; (3) state other methods that have been tried and that have failed, or state why they have appeared to fail or seem too dangerous; and (4) specify the period of interception. The typical period of a wiretap is 30, 60, or 90 days. However, courts provide greater scrutiny the longer the period.

Law enforcement also has the right to conduct **surveillance**, including electronic eavesdropping, wiretapping, physical searches, and pen trap and trace, to collect foreign intelligence under the **Foreign Intelligence Surveillance Act of 1978 (FISA)**. Under FISA, law enforcement may collect foreign intelligence to detect espionage, sabotage, terrorism, and related hostile intelligence upon a finding of probable cause that the surveillance target is a foreign power or an agent of a foreign power. The effect is that FISA created a limited exception to the probable cause rule if the government is gathering foreign intelligence. There is a special court that reviews FISA applications.

The passage of the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)** broadened existing law enforcement tools, particularly in the area of surveillance and the **Internet**, and amended several sections of existing statutes related to computer crimes, money laundering and asset forfeiture, immigration, and the collection of evidence. The act also allowed broader use of information obtained from grand juries and wiretaps by law enforcement and government officials.

The Patriot Act has neutralized some of the protections in ECPA by making it easier for law enforcement to get customer records from service providers. The FBI and other agencies can demand that service providers provide access to customer records with a statement certifying that the information pertains to an investigation, without a court order. The Patriot Act also permits voluntary disclosures and cooperation by private companies with law enforcement.

Under Sections 216, 219, and 220 of the Patriot Act, law enforcement has nationwide authority to conduct search warrants for e-mail and to expand voice wiretaps so that suspicion of a crime is sufficient cause to get a wiretap of any telephone, computer, or cell phone used by a target in an investigation. This is known as a “roving wiretap” and only requires the identification of the target. The national scope of the act was intended to minimize the jurisdictional boundaries of investigating a crime and allow investigators to go through the same process for collecting warrants, but only once.

The Patriot Act also amended FISA to permit secret wiretaps without authorization whenever law enforcement says that its investigation also has a “significant foreign intelligence purpose.” This major change means that wiretapping for foreign intelligence purposes only requires showing that the target is an agent of a foreign power. It is not necessary to show that the target has engaged in criminal activity. A U.S. citizen is an agent if he or she knowingly engages in espionage for a foreign power or intelligence service and is about to violate any U.S. laws. The effect of this amendment allows the government to initiate wiretaps under FISA’s lower standard when the investigation’s primary purpose is to collect criminal evidence. Such information can then be shared with other government agencies, and the target may never know



about it because notification is not permitted, even though targets of criminal searches and wiretaps must be notified eventually of the search. Many critics have argued that the Patriot Act amendments to FISA have blurred the distinctions between spying on foreign agents and spying on U.S. citizens.

The Patriot Act has been criticized by civil libertarians as eroding Fourth Amendment protections against unreasonable search and seizures. The government has defended the act as being necessary to fix certain problems in existing statutes that treat access to wire and wireless communications differently from electronic communications and to expand certain investigators' tools to address the threat of terrorism.

Civil libertarians argue that the act reduces the search warrant requirements and allows law enforcement to gather U.S. and foreign intelligence and use illegally obtained information abroad in domestic prosecutions. The concern is over lack of appropriate reporting requirements and checks and balances to ensure against misuse and abuse that encroach upon the rights of U.S. citizens.

The effect is that investigators' powers are broadened without the same level of judicial review as previously provided to U.S. citizens. The fear is that these expanded powers will enable the government to conduct massive surveillance and detain Americans without proving they are terrorists, similar to the government's response during the **McCarthy** era to the threat of Communism.

Such suspicions seem to have some credibility, following **disclosure** that in 2001 President George W. Bush secretly authorized the **National Security Agency** to electronically spy on U.S. citizens placing calls overseas. Some credit this disclosure as being responsible for Congress authorizing only a five-week extension of selected provisions of the Patriot Act that were due to expire on December 31, 2005, under the act's sunset provisions. Among the most controversial of these provisions are the roving wiretap and informational sharing between the FBI and the **Central Intelligence Agency (CIA)**. In the end, however, Congress voted to extend the sunset provision on "roving wiretaps." Yet despite this action, whether such provisions will be extended and for how long is unclear. However, it is clear that the debate over balancing privacy concerns with effective law enforcement tools will continue for the foreseeable future.

Suggested Reading: Dash, Samuel, Richard Schwartz, and Robert Knowlton. *The Eavesdroppers*. New Brunswick, NJ: Rutgers University Press, 1959; Dempsey, James X. "Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy," *Albany Law Journal of Science and Technology* 8 (1997): 70–71; Diffie, Whitfield, and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press, 1999; Electronic Privacy Information Center. *Clipper Chip*. <http://www.epic.org/crypto/clipper/>. Online, March 2006; Flaherty, David H. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill: University of North Carolina Press, 1992; Goldberg, Carole. *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security*. New York: W. W. Norton, 2002; Smith, Robert Ellis. *Compilation of State and Federal Privacy Laws*. Providence, RI: Privacy Journal, 1992; Turkington, Richard C., and Anita L. Allen. *Privacy Law: Cases and Materials*. St. Paul, MN: West, 2002.

Andrea L. Johnson

Women and privacy

Women's **reasonable expectations of privacy** are often infringed upon differently than those of men. Privacy most fundamentally means the right and ability to keep others out. Women, like men, have longed for and sought freedom from unwanted intrusion and forced intimacy. However, only recently have such forms of privacy become realities for many women. Certain invasions into private bodily spaces are uniquely female, including unwanted pregnancies and nonconsensual sexual intercourse. Through the availability of effective contraceptives, women now can often control whether and when to become pregnant. Through changes in laws, men who rape women they know (who are the group that sexually assault women much more frequently than do strangers) are now subject to criminal prosecution.

Women in the United States have greater control over what kind of privacy they choose to have and choose to reject than women in many other cultures. In particular, **reproductive rights** and freedom have played a large role in increasing American women's privacy by allowing them to decide when to have children and how many to have. Four important constitutional privacy cases of the late twentieth century are *Griswold v. Connecticut*, 381 U.S. 479 (1965), and *Eisenstadt v. Baird*, 405 U.S. 438 (1972), which held that the ability to obtain and use contraceptives involves the fundamental right to privacy; and *Roe v. Wade*, 410 U.S. 113 (1973), and *Planned Parenthood v. Casey* (1992), which based the right to **abortion** on the constitutional right of privacy.

Invasions of privacy are often **gender** specific. Women are denied the right to safely walk alone on public streets and beaches or in parks or forests. They continue to have to consider the time of day or night and what they are wearing when alone in public. These rights of privacy in public spaces are denied women because strangers threaten them with a serious risk of intrusion on their private space and bodily integrity. Similarly, **cellular telephones** with webcams that film up women's skirts, street harassment such as catcalls and whistles, cyber stalking, peeping toms, and obscene phone calls are violations of the right of privacy that women endure much more frequently than men.

Sexual violence, when it involves nonconsensual sexual intercourse, is a stark example of a sex-based invasion of privacy. The act of rape in many cases creates the risk of the further intrusion of an unwanted pregnancy. If a woman reports her rape, she will likely be subjected to an invasive physical examination to confirm that she was raped. She will also be subjected to intrusive questioning by law enforcement officers and prosecutors. The victim may also experience unwanted and embarrassing publicity concerning the rape and her conduct that led up to it. Finally, if the case goes to trial, the rape victim will likely be subjected to prying, hostile, and humiliating questioning by the accused's attorney, described by many sexual assault victims as being raped again. While there are more legal protections concerning publicity and questioning today than in the past, the criminal justice system remains highly invasive of a rape victim's privacy.

Privacy remains double-edged for women. In 1890 **Louis Brandeis** and Samuel Warren wrote the first scholarly article in which a legal right to privacy was asserted. The privacy they argued for was the "**right to be left alone.**" They asserted that every man needs a place of solitude, a retreat from the hustle and bustle and competition of public life. While women value the right to be left alone as

much as do men, social norms have traditionally relegated women to the private world of home and childrearing, where they experience little personal privacy. The darkest side of privacy for some women still is isolation in violent homes where they are subject to sexual and physical violence.

In 1929 Virginia Woolf's book, *A Room of One's Own*, explained why women, like men, needed a private space to engage in intellectual creativity and achieve self-fulfillment. Woolf's demand that women have privacy in order to flourish has been partially answered by enforcement of laws enacted in the late nineteenth century giving women rights over their own finances and property. More recently broad public support for enforcing laws against domestic violence has provided women greater security in private spaces. In addition, date, acquaintance, and marital rape are all violent intrusions on women's most intimate spaces that, like stalking and **sexual harassment**, have only been legally and socially recognized in the United States since the 1980s.

America's recognition of a legal right to privacy began with *DeMay v. Roberts*, an 1881 case involving the privacy expectations surrounding childbirth. On a stormy night a doctor brought along a unmarried man to help him carry his medical equipment to a childbirth at a private home. When the doctor and the young man entered the home, the doctor failed to explain that the young man was not a medically trained assistant. During a paroxysm of pain, the laboring woman flailed uncontrollably and the doctor yelled "catch her" to the young man, who grabbed her hand briefly and then returned to a corner by the fire. After the child was delivered and the doctor left, the woman discovered that the man who held her hand during childbirth was not medically trained. She sued for this misrepresentation and its intrusion. The court in *DeMay* was the first to permit someone to sue for an injury based on the interference with her right of privacy.

While the facts of *DeMay* are somewhat dated, the concept of a woman's reasonable expectation of privacy during childbirth remains. Women expect to be informed of and have control over who attends them when they are in labor. Invasion of this right is something that a man can never experience.

Recent cases that rely on the *DeMay* case as precedent for women's right of personal privacy also involve specifically feminine privacy interests. In a 1984 case, *Harkey v. Abate*, a court held that a hidden viewing device in a public women's restroom at a skating rink violated women's rights of privacy. In *Lewis v. LeGrow* (2003), a court held that three ex-girlfriends could sue the defendant for invasion of privacy for secretly videotaping his consensual sexual encounters with them. In *Sanchez-Scott v. Alza Pharmaceuticals* (2001), a breast cancer patient was allowed to sue a male drug salesperson for invading her privacy by his attending a breast exam given by her oncologist.

A 2006 Kansas case demonstrates further how certain kinds of invasions of privacy are specifically targeted at women or more often affect them. In *Alpha Medical Clinic v. Anderson*, the Kansas Supreme Court invalidated a demand by the Kansas attorney general that clinics provide him with the names of all their patients who had late-term abortions. The attorney general demanded the names because he alleged that some of these patients might have committed the crime of child abuse by terminating their pregnancies without legal justification. Holding that this demand was an unconstitutional invasion of the women's privacy, the court found that three rights of privacy were at issue: the right to maintain the privacy of certain personal informa-

tion; the right to obtain confidential health care; and a woman's right to obtain an abortion without the government imposing an undue burden on that right.

Feminist theorists have argued that women have a greater need and preference for connection and intimacy than do men. Carol Gilligan's book *In a Different Voice*, published in 1982, has been the basis of claims that women see the world through a connection lens while men value separation from others. Robin West, in her article *Jurisprudence and Gender*, asserts that men value separation and fear connection while women value connection and fear separation. Even if there is factual basis for such claims, it is only chosen connection and intimacy that women value; often connection and intimacy are imposed on women instead.

Anita Allen in her 1988 book *Uneasy Access* examines the lack of meaningful privacy for women. She discusses how women's positive values, such as caring, connection, selflessness, and intimacy, often conflict with their ability to experience the kind of privacy that men assume as their right. The economic realities for women, especially battered women and single mothers, often continue to make decisional privacy and a room of her own very hard to achieve.

Women in the United States today often have far more chosen privacy than women had in the past. Nevertheless, they continue to confront certain invasions of privacy that affect them much more than they affect men.

See also: **Constitutional protections; Health privacy; Privacy, definition of; Privacy, philosophical foundations of; Public/private dichotomy**

Suggested Reading : Alderman, Ellen, and Caroline Kennedy. *The Right to Privacy*. New York: Alfred A. Knopf, 1995; Allen, Anita L. *Uneasy Access: Privacy for Women in a Free Society*. Totowa, NJ: Rowman & Littlefield, 1988; Allen, Anita L. *Why Privacy Isn't Everything: Feminist Reflections on Accountability for Private Life*. Lanham, MD: Rowman & Littlefield, 2003; Gilligan, Carol. *In a Different Voice*. Cambridge, MA: Harvard University Press, 1982; West, Robin. "Jurisprudence and Gender," *University of Chicago Law Review* 55 (1988): 1–72.

Caroline Forell

Workplace privacy

The field of workplace privacy involves a vast number of disparate topics and is governed by a wide range of different laws, from the United States Constitution to state and local laws in a number of jurisdictions. Accordingly, the law of workplace privacy varies from state to state and jurisdiction to jurisdiction. What issues of workplace privacy have in common is a focus on the regulation or limitation of the activities of employers that threaten to violate the interests of employees in keeping personal information and personal activities private from their employers and in safeguarding their individual dignity and autonomy.

The United States Constitution restricts the actions that public-sector employers can take with respect to the privacy interests of their employees. The two primary protections for the workplace privacy interests of public-sector employers are found in the Fourth Amendment's protection against unreasonable searches and seizures and the Ninth Amendment's more general right to privacy. The Fourth Amendment generally restricts physical intrusions upon employees' privacy interests, such as the right to be free from the searches caused by employer **drug testing**,



medical and **genetic** testing, employer searches of the person and property of employees, and employer **surveillance** and monitoring of employee activities and communications. In addition, the constitutional right to privacy restricts employer intrusions of a less tangible or physical nature, such as employer interference with employees' interests in making certain personal decisions and in avoiding the **disclosure of personally identifiable information**.

The Fourth Amendment protects against unreasonable searches and seizures. An action constitutes a search or seizure if it intrudes upon an individual's subjective expectations of privacy that society is prepared to accept as objectively reasonable. That is, a public-sector employer's action will implicate the Fourth Amendment if it invades an employee's **reasonable expectation of privacy**; if the employee's expectation of freedom from intrusion is not deemed to be reasonable, no constitutionally regulated search or seizure has occurred. Although traditional Fourth Amendment analysis would find a search or seizure to be unreasonable if not conducted pursuant to a warrant issued upon probable cause, an exception to these requirements has been recognized in the case of intrusions upon privacy that occur in the context of the workplace. In the workplace context, courts have allowed searches and seizures to be justified based on "special governmental needs" not tied to law enforcement. When that special needs test is met, the courts have allowed a workplace search or seizure to be justified based on a balance between the interests of the governmental employer in conducting the search and the degree of intrusion upon the privacy interests of the affected employee.

Accordingly, the courts, including the United States Supreme Court, have upheld public-sector employer drug testing programs against Fourth Amendment challenge when those drug testing programs have been deemed necessary to safeguard public or employee safety. On the other hand, when the employer has been found to have adopted a drug testing program based on less compelling circumstances, such as a general interest in employee productivity or efficiency or a symbolic desire to demonstrate the integrity of employees by showing that they are drug free, the courts have generally refused to uphold such programs. In addition, in applying the balancing test to employer use of drug testing, courts have considered whether the method of drug testing is particularly invasive, such as whether it involves direct observation of the act of urination in providing a test sample or whether the drug test measures largely off-duty, as opposed to on-duty, activities.

While Fourth Amendment challenges in the employment setting may occur most commonly in the context of drug testing, similar challenges have been made to other forms of employer activities, such as employer use of video, **computer**, and **electronic surveillance**. Because the intrusions deemed to be caused by such employer actions are generally considered less invasive than that occasioned by drug testing, employers have generally been required to provide less justification for those types of actions. In addition, the existence of an employer policy informing employees of the potential or certainty of such monitoring has been deemed to decrease the reasonable expectations of employees that they will not be subject to such monitoring.

Ninth Amendment right-to-privacy challenges have been brought when public-sector employers have sought disclosure of, or made employment decisions on the basis of, sensitive personal information about employees. For example, these types

of challenges have been brought when current or prospective employees have been questioned—in polygraph examinations, honesty or psychological examinations, or just employment interviews—about intensely private information, such as information about sexual practices, religious beliefs, or stigmatized medical conditions. As in the Fourth Amendment area, these challenges have been resolved by balancing the employer's interest in and need for the requested information with the privacy interests of the employee or job applicant. The more private the information, the stronger the employer's interest in the information needs to be.

There are also a number of federal statutes that have implications for employer actions that threaten the privacy interests of employees. For example, the federal Employee Polygraph Protection Act of 1988 limits the ability of private-sector employers, but not public-sector employers, to conduct polygraph examinations and other lie detection tests of employees and job applicants. In general, pre-employment polygraph testing is allowed of job applicants in very limited circumstances, specifically when employers are involved in providing security services or in manufacturing or distributing controlled substances. With respect to current employees, private-sector employers can conduct polygraph examinations only in connection with an ongoing investigation of economic loss or injury to the employer and then only of employees with access to the property at issue and for whom there is reasonable suspicion of involvement in the loss or injury.

Another federal statute that places some restrictions on the actions of employers that may implicate employee privacy rights is the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the **Electronic Communication Privacy Act of 1986**. This act, known generally as the federal Wiretap Act, places restrictions on the ability of employers to intentionally intercept or attempt to intercept oral, wire, or electronic communications of employees. Accordingly, recording oral communications and conversations of employees can violate the act if the employees have a reasonable expectation that their conversations will not be overheard. Similarly, the federal Wiretap Act can be violated when employers listen in on or record the telephone conversations—a wire communication—of employees, unless the employer can justify that monitoring by either implied or express consent of the employee or can show a business-related justification for the monitoring. In general, while employers are allowed to monitor the business telephone calls of employees, they are not authorized to monitor personal telephone calls, at least no longer than is necessary to determine if the call is in fact business or personal. The federal Wiretap Act, however, has been interpreted to provide little protection to electronic communications, such as voice mail and **electronic mail**. In general, employers have not been found liable for intercepting those types of employee communications unless the communication was intercepted at the moment of transmission; accessing those communications while they are in storage has generally been held to fall within an exception to the act's prohibitions.

Other federal restrictions on employer actions that threaten employee privacy rights arise not directly from an effort to protect privacy interests but indirectly from an effort to prohibit employer discrimination against members of protected groups. Accordingly, while the Americans with Disabilities Act of 1990 may restrict the ability of employers to seek private medical information from their employees and job applicants, the purpose of that statute is to prohibit discrimination on the



basis of disability. Similarly, when some courts have sought to protect employees from discrimination and harassment on the basis of sexual orientation or status as a transsexual, the focus of those courts has been on whether the employer's action constitutes discrimination on the basis of sex under Title VII of the Civil Rights Act of 1964, not whether the employer's action violates a private right to not have to disclose information or to not have employment decisions made on the basis of personal information.

A number of states have enacted state legislation to protect the privacy rights of employees, filling gaps left in federal protection for privacy. Indeed, these state statutes may be the only protection that most employees and job applicants have with respect to their privacy interests. These state statutes seek to regulate a number of different types of employer actions that may implicate employee privacy rights. For example, a large number of states have enacted drug testing statutes. While some of these statutes seem motivated by a desire to clear the way to allow employers to conduct such drug testing of employees and job applicants, a number of provisions of these statutes—restricting the manner in which the tests are conducted and the circumstances under which they can be conducted—appear to be drafted with employee privacy interests in mind.

Similarly, many states have adopted statutes regulating employer use of polygraph tests, and many of these statutes are more restrictive than the federal act. Among the provisions of such statutes are requirements that certain types of questions not be asked of employees, apparently out of concern for employee privacy interests. Other statutes restrict the ability of employers to conduct psychological testing of employees; their intent is to ensure that employers do not use these tests without a proper justification and that the use of such tests is not more intrusive than is needed to serve the employer's legitimate interests. States have also enacted legislation to protect the privacy interests of employees in the areas of sexual orientation, genetic testing, and employer efforts to regulate the off-duty activities of employees.

Employer actions that threaten employee privacy can also be challenged as a violation of the common law right of privacy, which is recognized as a claim in the employment setting in a number of states. Although there are several types of "invasion of privacy" claims that have been recognized, the common law privacy claim that is most likely to be applicable in the employment setting is the claim that an employer's action is an "unreasonable intrusion upon the seclusion of another." In general, the ability to make out a claim under this theory requires that the employee establish that the employee has suffered an intrusion that is offensive to a reasonable person and that the reason for the intrusion does not justify that intrusion. Employees have relied on the common law right of privacy, with some success, to challenge drug tests, polygraph examinations and psychological tests, physical searches of the persons and property of employees, electronic and video monitoring of employees, and attempts by employers to regulate the off-duty conduct of their employees. As with the similar challenges that are brought under the constitutional right to privacy, the success that employees have had in asserting common law right of privacy claims depends both on the degree to which the employer's actions intrude upon privacy interests that the courts are willing to accept as reasonable and the legitimacy and gravity of the employer's interest in and need for the requested information.

This brief summary of the various laws that touch on issues of privacy in the workplace illustrates the lack of comprehensive regulation of employee privacy. The patchwork of federal and state constitutional, statutory, and common law indicates that the protection of one's privacy interests depends on the particular type of employer activity that threatens those interests and the particular jurisdiction in which one is employed. This state of affairs has led some commentators to argue for comprehensive federal legislation that would protect the privacy rights of employees. While some would oppose such comprehensive legislation on the ground that such issues are better left to the states, those arguments have not been sufficient to prevent the enactment of other comprehensive federal legislation dealing with workplace issues. These same kinds of arguments were made, and rejected, when the various federal anti-discrimination laws—Title VII of the Civil Rights Act of 1964, the Age Discrimination Act of 1967, and the Americans With Disabilities Act of 1990—were enacted. Nor have these arguments been sufficient to defeat other federal legislation relating to the workplace, such as the Employee Polygraph Protection Act of 1988.

The law of employee privacy would, in the opinion of this commentator, best be regulated by comprehensive federal legislation that imposed uniform minimum standards for the protection of the privacy rights of employees. All individuals would then be entitled to have some basic protection from employer intrusion into their off-duty activities and personal characteristics that are unrelated to their ability to perform the duties of their jobs. As in other areas of the law, such as the anti-discrimination field, states could continue to be given the authority to provide more protection than the federal minimum, but they would not be allowed to enforce state standards that were not as protective as the federal minimum. Although this approach would likely further restrict employers' actions that threaten privacy rights, employers would also gain some certainty about the validity of any actions taken in compliance with the proposed federal standard.

Although congressional legislation dealing with specific types of employer actions might be beneficial, it might also pose difficulties, particularly if Congress cannot keep up with new technologies that might threaten employee privacy interests. Although not without its problems, more legislation would likely be needed to address the full range of possible employer activities. Prohibiting regulation of off-duty conduct that does not adversely affect an employee's job performance would be a critical aspect of any proposed federal legislation, as would prohibiting inquiries about private off-duty conduct and other private information irrelevant to job performance. Finally, any proposed federal legislation should also regulate the manner in which employers seek private information that is sufficiently job-related so as not to be prohibited; such inquiries should be made in the least intrusive manner, and employers should be required to safeguard the **confidentiality** of any private information obtained. More specific rules on limiting or regulating employer activities would presumably be left to the courts or to an administrative agency charged with enforcement of the statute.

While there would presumably be employer opposition to more regulation of their activities relating to privacy, the existence of scattered federal and state legislation relating to privacy demonstrates that legislatures continue to be concerned about these issues. Comprehensive federal legislation is necessary if significant protection is to be given to employee privacy rights.



See also: **Background checks; Constitutional protections; Industrial espionage; Privacy, definition of; Wiretapping**

Suggested Reading: Bryant, Susan. "Electronic Surveillance in the Workplace," *Canadian Journal of Communication* (1995). www.cjc-online.ca. Online, February 2006; Decker, Kurt H. *Privacy in the Workplace: Rights, Procedures and Policies*. Horsham, PA: LRP, 1994; Finkin, Matthew W. *Privacy in Employment Law*. Washington, DC: Bureau of National Affairs, 2003; Hébert, L. Camille. *Employee Privacy Law*. Eagan, MN: Thompson West, 1993, and annual supplement 2006; Hébert, L. Camille. "Toward the Comprehensive Regulation of Employee Privacy Rights." In Bruno Stein (ed.), *Proceedings of New York University 46th Annual National Conference on Labor*, pp. 141–178. New York: Little, Brown, 1994; Hubbart, Phillip A. *Making Sense of Search and Seizure Law: A Fourth Amendment Handbook*. Durham, NC: Carolina Academic Press, 2005; Regan, Priscilla. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press, 1995; Staples, W. *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. Lanham, MD: Rowman & Littlefield, 2000; Tunnell, Kenneth. *Pissing on Demand*. New York: New York University, 2004; Turkington, Richard C., and Anita L. Allen. *Privacy Law: Cases and Materials*. St. Paul, MN: West, 2002.

L. Camille Hébert

World Wide Web (WWW). *See* **Internet**

X



X-ray devices

Discovered in 1895 by W. C. Roentgen, x-rays are a form of invisible, highly penetrating electromagnetic radiation. Because of their ability to pass through most material, x-rays are used in a variety of applications, including security settings. Since the events of September 2001, the U.S. government has been investing enormous amounts of money and effort in technology to prevent future terrorist attacks, especially in U.S. transportation systems.

Currently, the Transportation Security Administration (TSA) is field-testing a noninvasive x-ray system known as a “backscatter portal” that can see items hidden on a person’s body, concealed in vehicles, or secretly stashed in cargo containers. The system’s signals interact with explosives, plastics, and metals, revealing their shape and form and thereby making them easy to visually identify.

The backscatter technology works by measuring the solar radiation reflected by the person or object under scrutiny. The system is sensitive enough to detect metal objects, plastic explosives and weapons, nonmetallic handguns, and drugs. In vehicle inspections, the driver briefly exits while the screening van slowly passes by the target, screening for contraband. When a person is screened, the individual steps into the refrigerator-sized machine, and the technology performs a virtual **strip search**, which provides inspectors with a clear view of what is underneath the person’s clothes—skin or weapons. Whether the technology is used to screen a vehicle or a person, TSA claims that the process takes less than a minute and asserts that the technology is physically harmless; however, critics purport that generating such a realistic image of an individual’s naked body violates privacy rights.

The TSA is aware of the revealing nature of the images. It is working with companies to create software that would substitute a generic body but leave in place the outlines of the suspected contraband. The TSA’s proposed goal for using this technology is to reduce the long queues in airports and to reduce security threats posed by vehicles containing explosives.

The devices are currently used by U.S. Customs agents at 12 airports to screen suspected drug smugglers, at London’s Heathrow Airport, and in London’s underground subway tube since the July 2005 bombings. Furthermore, the backscatter technology is being used as part of the Secure Automobile Inspection Lanes



(SAIL) test project, which screens for explosives on **automobiles** boarding the Cape May-Lewes Ferry in Cape May, New Jersey, the Golden Gate Ferry in San Francisco, California, and several other designated locations.

See also: **Air travel; Biometric identifiers; Surveillance; Thermal sensors**

Suggested Reading: Electronic Privacy Information Center. *Backscatter X-Ray Screening Technology*. www.epic.org. Online, November 2005; Times Online. *Body Scan Machines to Be Used on Tube Passengers*. <http://technology.timesonline.co.uk/article/0,,20409-1686151,00.html>. Online, November 2005; Transportation Security Administration. *Secure Automobile Inspection Lanes Pilot (SAIL)*. www.tsa.gov. Online, November 2005; USA Today. *Air Travelers Stripped Bare with X-Ray Machine*. www.usatoday.com/travel/news/2005-05-15-xray-inside_x.htm. Online, November 2005.

Jill Joline Myers

Z



Zone of privacy

In *Griswold v. Connecticut*, 381 U.S. 479 (1965), William O. Douglas, who wrote the majority opinion, argued that the choices made by married couples with respect to **family** planning are contained within a “zone of privacy” into which the government should not intrude. Acknowledging that the right to privacy is not specified anywhere in the Constitution, Douglas maintained that specific guarantees in the First, Third, Fourth, Fifth, and Ninth Amendments provide ways in which citizens can make autonomous decisions pertaining to married life. Douglas’s reasoning has drawn heavy criticism, not only from opponents of free access to **birth control** products and **abortion**, but also from legal theorists who favor strict adherence to the text of the Constitution. According to these strict constructionists, the problem with *Griswold* is not that it enabled married couples to make choices about reproduction, but that its notion that zones of privacy could be created under the cover of various amendments went too far beyond the Bill of Rights.

The language Douglas used to support the recognition of zones of privacy has been characterized as needlessly confusing, but it draws from a relatively established legal vocabulary. According to Douglas, certain protections included in the Bill of Rights give off “penumbras,” which are partial or incomplete shadows produced by “emanations,” that is, implications that are vital to those protections. In other words, particular guarantees in different amendments create rights that are implied but not explicitly specified. Although it might be too much to suggest that these concepts are sufficiently well defined to amount to a “penumbral theory,” the term “penumbra” was applied to provisions within the Bill of Rights in earlier cases, most notably by Justice Oliver Wendell Holmes in his dissent in *Olmstead v. United States*, 277 U.S. 438 (1928). There, commenting on the “penumbra” surrounding the Fourth and Fifth Amendments, Holmes suggested that it is not wise to adhere too closely to the actual wording of a law if doing so would obviate its policy implications.

Although Douglas discussed multiple zones of privacy—indicating that there may be various types—the area he focused on most intently in *Griswold* was the family **home**. Thus, he cited *Boyd v. United States*, 116 U.S. 616, 630 (1886),



which held that the Fourth and Fifth Amendments specifically protect “the sanctity of a man’s home and the privacies of life.” Moreover, he conjured up the image of the police barging into the “sacred precincts of marital bedrooms” to stress the home as deserving of special consideration. In his concurring opinion, Justice Arthur Goldberg reinforced this perspective, quoting Justice John Marshall Harlan’s dissent in *Poe v. Ullman*, 367 U.S. 497 (1961), which emphasized that the home is so central to family life that it falls under the protection of several explicitly stated constitutional rights.

With the highly significant exception of *Roe v. Wade*, 410 U.S. 113 (1973), which underscored *Griswold*’s stipulation of a constitutional “guarantee of certain areas or zones of privacy,” the Court has generally tended to adopt Goldberg’s approach. In *Stanley v. Georgia*, 394 U.S. 557 (1969), for example, the Court affirmed important aspects of *Griswold* but dropped the term “zone” and simply pointed to broad social and legal agreement on the need to respect the “privacy of the home.” Similarly, *Payton v. New York*, 445 U.S. 573 (1980), acknowledged that privacy might be protected in other environments, but noted that the “zone of privacy” is nowhere “more clearly defined than when bounded by the unambiguous physical dimensions of an individual’s home.” Later, in *United States Department of Defense v. Federal Labor Relations Authority* (1994), the Court described the privacy of the home as a settled principle within constitutional law: “We are reluctant to disparage the privacy of the home, which is accorded special consideration in our Constitution, laws, and traditions.”

Justice Anthony Kennedy, who wrote the majority opinion in *Lawrence v. Texas*, 539 U.S. 558 (2003), focused more on liberty than on privacy in overturning *Bowers v. Hardwick*, 478 U.S. 186 (1986). However, he cited *Griswold* as the starting point for *Lawrence* and, rather than adopting the phrase “zone of privacy,” echoed the pronouncements made in previous cases by starting off with the declaration that “liberty protects the person from unwarranted government intrusions into a dwelling or other private places.” Thus, without decisively rejecting Douglas’s concept of “zones of privacy,” or ruling out privacy protections in other areas, the Court has located the right to privacy most consistently within the home.

See also: Constitutional protections; Health privacy; Privacy, definition of; Public/private dichotomy; Reproductive rights; Women and privacy

Suggested Reading: Bartee, Alice Fleetwood. *Privacy Rights: Cases Lost and Causes Won before the Supreme Court*. Lanham, MD: Rowman & Littlefield, 2006; Garrow, David J. *Liberty and Sexuality: The Right to Privacy and the Making of Roe v. Wade*. Berkeley: University of California Press, 1998; Johnson, John. *Griswold v. Connecticut: Birth Control and the Constitutional Right of Privacy*. Lawrence: University of Kansas Press, 2005; Turkington, Richard C., and Anita L. Allen. *Privacy Law: Cases and Materials*. St. Paul, MN: West, 2002.

Susan E. Gallagher

Resource Guide

Suggested Reading

This is a list of key books on privacy. For more selections, see the “Suggested Reading” list at the end of each encyclopedia entry.

- Agre, Philip E., and Marc Rotenberg (eds.). *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT Press, 1997.
- Alderman, Ellen, and Caroline Kennedy. *The Right to Privacy*. New York: Alfred A. Knopf, 1995.
- Allen, Anita L. *Why Privacy Isn't Everything: Feminist Reflections on Accountability for Private Life*. Lanham, MD: Rowman & Littlefield, 2003.
- Aries, Philippe, and Georges Duby. *A History of Private Life*. Cambridge, MA: Belknap Press, 1992.
- Bennett, Colin J., and Rebecca Grant (eds.). *Visions of Privacy*. Toronto: University of Toronto Press, 1999.
- Bennett, Colin J., and Charles D. Raab. *The Governance of Privacy: Policy Instruments in Global Perspective*. Aldershot, UK: Ashgate, 2003.
- Bodenhamer, David J., and James W. Ely, Jr. (eds.). *The Bill of Rights in Modern America after 200 Years*. Bloomington: Indiana University Press, 1993.
- DeCew, Judith Wager. *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*. Ithaca, NY: Cornell University Press, 1997.
- Etzioni, Amitai. *The Limits of Privacy*. New York: Basic Books, 1999.
- Feinman, Jay M. *Law 101: Everything You Need to Know about the American Legal System*. New York: Oxford University Press, 2000.
- Flaherty, David H. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill: University of North Carolina Press, 1992.
- Gandy, Oscar. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press, 1993.
- Garrow, David J. *Liberty and Sexuality: The Right to Privacy and the Making of Roe v. Wade*. Berkeley: University of California Press, 1998.
- Goldberg, Carole. *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security*. New York: W. W. Norton, 2002.
- Kersch, Ken I. *Constructing Civil Liberties: Discontinuities in the Development of American Constitutional Law*. Cambridge, UK: Cambridge University Press, 2004.



- Lyon, David (ed.). *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. London: Routledge, 2003.
- Regan, Priscilla. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press, 1995.
- Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House, 2000.
- Rössler, Beate (ed.). *Privacies: Philosophical Evaluations*. Stanford, CA: Stanford University Press, 2004.
- Smith, Jeff H. *Managing Privacy: Information Technology and Corporate America*. Chapel Hill: University of North Carolina Press, 1994.
- Solove, Daniel J. *The Digital Person, Technology and Privacy in the Information Age*. New York: New York University Press, 2004.
- Staples, William G. *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. Lanham, MD: Rowan & Littlefield, 2000.
- Westin, Allan. *Privacy and Freedom*. New York: Atheneum, 1967.

Websites

Economics of Privacy,

<http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm>

This page provides links to resources on the economics of privacy, financial privacy, and the economics of anonymity—papers, people, related conferences, and other resources.

Health Privacy Project,

<http://www.healthprivacy.org/>

The Health Privacy Project is dedicated to raising public awareness of the importance of ensuring health privacy in order to improve health care access and quality, both on an individual level and on a community level.

Online Privacy Alliance,

<http://www.privacyalliance.org/>

This is a business group supporting self-regulatory initiatives to protect privacy online and in electronic commerce.

State of California Office of Privacy Protection,

<http://www.privacy.ca.gov/>

California is the first state to have an agency dedicated to promoting and protecting the privacy rights of consumers. Created by legislation enacted in 2000, the Office of Privacy Protection opened in 2001

Supreme Court Multimedia,

<http://www.oyez.org>

This site is a Northwestern University Project offering access to Supreme Court case summaries and more than 2000 hours of Supreme Court audio files.

United States Federal Trade Commission, *Privacy Initiatives*,

<http://www.ftc.gov/privacy/>

This is a federal government initiative to educate consumers and businesses about the importance of personal information privacy, including the security of personal information.

Organizations

American Civil Liberties Union
125 Broad Street, 18th Floor
New York, NY 10004
Phone: 212-549-2519
<http://www.aclu.org/>

An independent organization that focuses on defending the individual rights and liberties guaranteed under the Constitution and laws of the United States. This site has information on current ACLU activities and legal actions, including privacy-related initiatives.

Center for Democracy and Technology
1634 Eye Street NW #1100
Washington DC, 20006
Phone: 202-637-9800
<http://www.cdt.org>

A nongovernmental organization, the Center for Democracy and Technology works at the intersection of law, technology, and policy and is “dedicated to building consensus among all parties interested in the future of the Internet and other new media.”

Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110-1914
Phone: 415-436-9333
<http://www EFF.org>

The Electronic Frontier Foundation is a donor-funded nonprofit dedicated to “digital rights,” including “free speech, privacy, innovation, and consumer rights.” Though its efforts are primarily focused in the courts, it also advises policymakers and educates the media and the public.

Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
Phone: 202-483-1140
<http://www.epic.org>

EPIC is a public interest research center that focuses on emerging civil liberties debates, privacy protection, and constitutional issues. This site offers extensive information on current and past privacy-related issues.

Privacy Foundation
2255 E. Evans Ave.
Suite 435
Denver, CO 80208
Phone: 303-871-6295
<http://www.privacyfoundation.org>

The Privacy Foundation is a policy research center associated with the Sturm School of Law at the University of Denver. The foundation focuses primarily on research, particularly on the analysis of communications technologies and services that may pose a threat to personal privacy.



Privacy International
6–8 Amwell Street
London EC1R 1UQ
United Kingdom
+44-7947 778247
<http://www.privacyinternational.org>

A self-described privacy “watchdog group,” Privacy International is based in London but has an office in Washington, D.C. PI focuses on issues of cybercrime, freedom of information, ID cards, digital money, outsourcing, wiretapping, encryption, and video surveillance.

Privacy Rights Clearinghouse
3100 5th Ave., Suite B
San Diego, CA 92103
Phone: 619-298-3396
<http://www.privacyrights.org/>

This organization offers consumers fact sheets on a range of privacy-related issues to provide practical advice and information for users about securing their privacy. Some of the topics included in these fact sheets are telemarketing, financial privacy, identity theft, and employment background checks.

Films

These films deal with a range of privacy and surveillance issues.

Feature Films

Brazil (Terry Gilliam, 1985). A bureaucrat in a future world tries to correct a small administrative error and becomes an enemy of the state.

The Conversation (Francis Ford Coppola, 1974). A surveillance expert is obsessed with his own privacy.

EDtv (Ron Howard, 1999). Everyman video store clerk Ed agrees to have his life filmed by a camera crew for a TV network, and his supposedly mundane life reveals family secrets.

Gattaca (Andrew Niccol, 1997). This film is a portrait of a fictional world where genetic engineering and DNA are the primary factors determining social position.

Minority Report (Steven Spielberg, 2002). In the future, a special unit is assigned to track down criminals before their planned crimes are committed, but one of the officers in the unit is accused of such a crime and sets out to prove his innocence.

Nineteen Eighty-Four (Michael Radford, 1984). Adaptation of George Orwell’s novel of a totalitarian future society in which a man whose daily work is rewriting history tries to rebel by falling in love.

The Truman Show (Peter Weir, 1998). An insurance salesman/adjuster discovers that his entire life is actually a TV show.

Documentaries

Cyberstalker: Hard Lessons of Internet Safety (Films for the Humanities and Sciences, 2005). This CBS News program explores the dangers of personal information posting and dating on the Internet.

Internet Shopping: Interactive or Invasive? (Films for the Humanities and Sciences, 1999). Correspondent Jeffrey Kaye seeks to understand the dynamics of, and the ethical issues surrounding, strategic online marketing. From cookies to banner ads, the gathering and leveraging of consumer data are viewed as the key to making e-commerce viable.

No More Privacy: All About You (Films for the Humanities and Sciences, 1993). A camera crew stood on a freeway overpass and picked a car license number at random. This documentary shows what they were able to learn in half a day by searching public records and spending \$13 to build a dossier on two people they had never met.

Peter Jennings Reporting: No Place to Hide (Films for the Humanities and Sciences, 2005). ABC News examines high-tech monitoring methods that promise greater safety and security but threaten personal privacy.

Security Threat: Terrorism, Surveillance, and Civil Liberties (Films for the Humanities and Sciences, 2003). This program weighs the pros and cons of real-time profiling systems, closed-circuit cameras in public places, smart ID cards, thermal-imaging polygraphs, and other anti-terror technologies.

Whatever Happened to Privacy? (Films for the Humanities and Sciences, 2005). This film examines the effect of technology on the right to privacy in America.

Who Gets to Know? Genetics and Privacy (Films for the Humanities and Sciences, 2003). When it comes to genetic testing, how much should a patient be told? And could—and if so, should—such privileged information be made available to employers, insurance companies, and others? This seminar moderated by Harvard Law School's Arthur Miller offers a compelling discourse on the far-reaching ethical, social, legal, and economic implications of genetic testing.

About the Editor and Contributors

ANITA L. ALLEN is Henry R. Silverman Professor of Law and Professor of Philosophy at the University of Pennsylvania. Allen is the author of *Uneasy Access: Privacy for Women in a Free Society* (1988), *Why Privacy Isn't Everything* (2003), *Privacy Law: Cases and Materials* (2002), and *The New Ethics* (2004).

BRIAN AZCONA received an MA in sociology at the University of New Orleans and has taught sociology at Xavier University of New Orleans. He is currently completing his Ph.D. at the University of Kansas with a concentration in economic sociology, historical sociology, and social theory.

WILLIAM C. BANKS is Laura J. and L. Douglas Meredith Professor of Law and Director of the Institute for National Security and Counterterrorism at Syracuse University. Banks is the co-author of *National Security Law* (2006) and *Constitutional Law: Structure and Rights in Our Federal System* (2005).

TORI BARNES-BRUS is a graduate student in sociology at the University of Kansas. Her areas of interest include culture, gender, and historical methods. She is currently exploring the perpetuation of social inequality in late-nineteenth-century discourses on pregnancy.

TOD J. BEAVERS received his BA from the University of Northern Iowa in 1985, his JD with honors from Hamline University School of Law, and an ML specializing in taxation from the University of Missouri at Kansas City.

BARBARA BELBOT is Associate Professor of Criminal Justice at the University of Houston–Downtown. She served as a federal monitor in the Texas prison reform lawsuit *Ruiz v. Estelle*, appointed by Judge William Wayne Justice. Her current areas of research include prisoners' rights and prison reform movements.

STEFAN BRANDS is an expert on modern cryptology, secure access control, and privacy-preserving technologies. He is affiliated with Credentica, a Montreal-based IT security company. Dr. Brands is also Adjunct Professor of Computer Science at McGill University.



MAYA A. BERNSTEIN, JD, is the Privacy Advocate of the U.S. Department of Health and Human Services. She previously served as the Privacy Advocate of the IRS and as a Senior Policy Analyst at the Office of Management and Budget, where she was responsible for oversight of the Privacy Act of 1974.

DAVID J. BROWN is Managing Attorney of The Law Offices of David J. Brown, LC, in Lawrence, Kansas. He writes on legal ethics, legal rights for gays and lesbians, family law, asset protection, and privacy law.

NAOMI CAHN is Professor of Law at George Washington University, where she teaches family law. She has published widely in the area of family law and privacy issues, and is a co-author of the textbook *Contemporary Family Law* (2006) and the co-editor of *Families by Law: An Adoption Anthology* (2004).

MICHAEL CALOYANNIDES is a Senior Fellow at Mitretek Systems Corp. and Adjunct Professor in Computer Science at Johns Hopkins and George Washington universities. He has published two books and numerous papers on computer privacy and is an associate editor of *Security and Privacy* magazine.

ELLEN CAMPBELL is Deputy Director of the Family Policy Compliance Office of the U.S. Department of Education. She has been instrumental in bringing to the educational community a better understanding of the rights that parents and students are afforded by the Family Educational Rights and Privacy Act.

NANCY D. CAMPBELL is Assistant Professor in the Department of Science and Technology Studies at Rensselaer Polytechnic Institute. She is author of *Using Women: Gender, Drug Policy, and Social Justice* (2000) and *Science Says: The Laboratory Logics of Addiction Research* (forthcoming).

EVELYN A. CLARK is a graduate student in sociology at the University of Kansas. Her areas of interest are globalization, social inequalities, and political sociology. She is currently exploring social inequalities and neoliberal policies in Chile.

WILLIAM H. COLBY is senior fellow and national spokesperson for the National Hospice and Palliative Care Organization. He argued the first right-to-die case before the U.S. Supreme Court and is the author of *Unplugged: Reclaiming Our Right to Die in America* (2006) and *Long Goodbye: The Deaths of Nancy Cruzan* (2002).

MIHAEL COLE is a law student at the University of Ottawa Law School. He has an MA in Criminology from the University of Ottawa.

SIMON A. COLE is Assistant Professor of Criminology, Law & Society at the University of California–Irvine. He is the author of *Suspect Identities: A History of Fingerprinting and Criminal Identification* (2001), which won the Rachel Carson Prize for a book-length work of social or political relevance in the area of science and technology studies.

MARY J. CULNAN is Slade Professor of Management and Information Technology at Bentley College. She has interests in information privacy, online communities, and critical infrastructure protection as related to information security. Her research has appeared in numerous marketing and management journals.

JUDITH WAGNER DECEW is Professor and Chair of Philosophy at Clark University. DeCew is the author of *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (1997) and *Unionization in the Academy: Visions and Realities* (2003), and co-editor of *Theory and Practice* (1995).

LANE DENICOLA is a doctoral candidate in the Department of Science & Technology Studies at Rensselaer Polytechnic Institute. His research interests include the social and political dimensions of modeling and simulation, information technologies, and space industrialization.

BRIAN L. DONOVAN is Assistant Professor of Sociology at the University of Kansas. His work focuses on the role of legal institutions and moral reform activism in shaping social inequality. He is the author of *White Slave Crusades: Race, Gender and Anti-Vice Activism, 1887–1917* (2005).

CHRISTINA DUDZINSKI is a graduate student in the sociology program at the University of Kansas. She is currently pursuing her master's degree concentrating in the areas of culture, media, and social inequality.

DENISE M. DUDZINSKI is Assistant Professor in Medical History & Ethics at the University of Washington. She has written about the ethical dimensions of topics ranging from assisted reproductive technologies and transplantation to graduate medical education in ethics and professionalism.

GREGORY M. DUHL is Visiting Assistant Professor of Law at Southern Illinois University. He researches and writes in the areas of property and commercial law, with an emphasis on examining long-term relationships between legal actors from a sociolegal perspective.

MATTHEW M. DWYER holds a BA in History and a BA in English with Honors, from the University of Kansas. He received his Juris Doctorate from the University of Kansas in 2005.

ADA EMMETT is an academic librarian at the University of Kansas and serves as bibliographer for chemistry and molecular biosciences. She teaches a one-credit course on chemical information resources and has an ongoing interest in innovative projects that address current issues in scholarly communication.

LARKIN R. EVANS holds bachelor's degrees in English and in Studio Art from Southern Methodist University. She received her JD from the University of Kansas in 2004. She is currently employed as a research attorney for Justice Carol Beier of the Kansas Supreme Court.

D'LINELL FINLEY is Assistant Professor of Political Science and Public Administration at Auburn University, Montgomery. His research interests are privacy and Fourth Amendment rights, changing attitudes toward civil rights since 1954, and faith-based initiatives and the role of the church.

CAROLINE FORELL is Clayton R. Hess Professor of Law at the University of Oregon School of Law in Eugene. She is the author, with Donna Matthews, of *A Law of Her Own: The Reasonable Woman as a Measure of Man* (2000).



SUSAN FREIWALD is Professor of Law at the University of San Francisco. Freiwald received her JD from Harvard Law School, where she was Books and Commentaries Editor of the *Harvard Law Review*. She is the author of “Online Surveillance, Remembering the Lessons of the Wiretap Act,” which appeared in the *Alabama Law Review* (2004).

RICHARD FYFFE is Director of Libraries at Grinnell College. His 2003 article “Technological Change and the Scholarly Communications Reform Movement: Reflections on Castells and Giddens” won the American Library Association’s Blackwell Scholarship award.

SUSAN E. GALLAGHER is Associate Professor of Political Science at the University of Massachusetts–Lowell and specializes in media studies, gender studies, and legal studies. She also develops digital scholarly resources for students, faculty, and the general public and is currently completing a series of multimedia essays on the history of privacy in the United States.

ROBERT GELLMAN is a privacy and information policy consultant. He served for 17 years on the staff of the House Subcommittee on Government Information with responsibilities related to privacy, freedom of information, and other information policy issues.

BETH GIVENS is founder and Director of the Privacy Rights Clearinghouse, a nonprofit consumer education and advocacy organization. She has written and spoken extensively on identity theft and other consumer privacy issues and has contributed testimony for state and federal legislative and regulatory proceedings.

BRIAN GRAN is Assistant Professor in the Department of Sociology and Law at Case Western Reserve University. His interests include comparative social policy, sociology of law, and methodology. His current research focuses on comparative social policy as it is formed at the intersection of the public and private sectors.

LAURA GURAK is Professor of Rhetoric and Scientific and Technical Communication and Head of the Department of Rhetoric at the University of Minnesota. She is the author and editor of numerous books, including *Persuasion and Privacy in Cyberspace* (1997) and *Cyberliteracies* (2001).

L. CAMILLE HÉBERT is the Carter C. Kissell Professor of Law at the Michael E. Moritz College of Law at The Ohio State University. She has written and spoken extensively on issues of employee privacy law and is the author of *Employee Privacy Law* (1993 and Supp. 2006).

ELIZABETH BLANKS HINDMAN is Associate Professor at the Edward R. Murrow School of Communication at Washington State University. Her research centers on legal and ethical obligations of the news media. She is the author of *Rights vs. Responsibilities: The Supreme Court and the Media* (1997).

JAMES G. HODGE, JR., JD, LL.M., is Associate Professor at Johns Hopkins Bloomberg School of Public Health, Adjunct Professor of Law at Georgetown University Law Center, and Executive Director of the Center for Law and the Public’s Health at Georgetown and Johns Hopkins universities.

MARCIA HOFMANN is Director of the Open Government Project and Staff Counsel at the Electronic Privacy Information Center in Washington, D.C. Hofmann leads EPIC's efforts to understand emerging policies in the post-9/11 period and serves as lead counsel in several of EPIC's Freedom of Information Act cases.

CHRIS JAY HOOFNAGLE is Senior Counsel to the Electronic Privacy Information Center and Director of its West Coast Office in San Francisco.

LARRY HOYLE is Associate Scientist and Director of Computing for the Policy Research Institute at the University of Kansas. He was an early implementer of database-driven websites for census and other demographic data such as the Kansas Data Archive (at <http://www.ipsr.ku.edu/ksdata/>).

RYAN C. HUDSON holds a BA in political science and JD from the University of Kansas. He is currently a law clerk for Chief Judge John W. Lungstrum of the United States District Court in the District of Kansas.

ANDREA L. JOHNSON is Professor of Law and Director of the Center for Intellectual Property, Technology and Telecommunications for the California Western School of Law.

IAN R. KERR holds the Canada Research Chair in Ethics, Law and Technology at the University of Ottawa Faculty of Law. He has written on ethical and legal aspects of privacy online. His current research focuses on the impact of information and authentication technologies on identity and anonymity.

JENNIFER KEYS is Assistant Professor of Sociology at North Central College in Naperville, Illinois. She received her Ph.D. from the State University of New York at Albany. Her research interests center around the movement-counter movement dynamics of the abortion debate and women's abortion experiences.

SHELLEY L. KOCH is a doctoral candidate in sociology at the University of Kansas. Her research interests include political economy, gender, and food.

SUSAN LANDAU is Distinguished Engineer at Sun Microsystems Laboratories. Landau previously was a faculty member at the University of Massachusetts and Wesleyan University. She is the author, with Whitfield Diffie, of *Privacy on the Line: The Politics of Wiretapping and Encryption* (1998).

ELIZABETH MIKLYA LEGERSKI is a doctoral candidate in sociology at the University of Kansas. Her interests include gender, work, family, and social movements. Her current work is focused on understanding how economic restructuring affects working-class families.

OPHRA LEYSER is a Ph.D. candidate in sociology at the University of Kansas. Her research interests include families, medical sociology, and gender.

CHRISTINE BERRY LLOYD is Assistant Professor of Economics at Western Illinois University. Her interests are in labor and public economics, privacy, and information-related topics.

WILLIAM C. LOWE is Professor of History and Dean of the College of Arts and Sciences at Ashford University, where he teaches American constitutional history.



He is the author of *Blessings of Liberty: Safeguarding Civil Rights* (1992), a text for middle-schoolers.

KUORAY MAO is a graduate student in sociology at the University of Kansas. His areas of interests include deviance, culture, race, and ethnicity. He is currently exploring the formation of ethnic identity for immigrant youths in Southern California.

JOSE L. MARTINEZ is a graduate student in sociology at the University of Kansas. He has research interests in issues of race, gender, and class.

GARY T. MARX is Professor Emeritus at MIT and the author of books and articles on surveillance and social control. Additional information is available at garymarx.net.

JASON MAZZONE is Assistant Professor of Law at Brooklyn Law School. His areas of academic work have been in constitutional law and history, criminal law and procedure, and federalism. Among his recent works are “The Security Constitution” in the *UCLA Law Review*.

TORIN MONAHAN is Assistant Professor of Justice & Social Inquiry at Arizona State University. His research focuses on the design of information technology infrastructures and their political and social ramifications. He is the author of *Globalization, Technological Change, and Public Education* (2005).

STEVE MUNCH received his BA in history and sociology from the University of Kansas in 2006.

WENDY J. MURPHY, JD, is Adjunct Professor at the New England School of Law, where she teaches a seminar on sexual violence. She writes and lectures widely on violence against women and children, privacy, and the criminal justice system and is a CBS News legal analyst, trial attorney, and impact litigator.

JILL JOLINE MYERS is Assistant Professor of Law Enforcement and Justice Administration at Western Illinois University. Prior to joining the faculty at WIU, she served as a prosecutor in Baltimore, Maryland, for 20 years. Professor Myers concentrates in the area of technological developments by examining their application to law enforcement investigations. On occasion, she serves as a script advisor for the popular HBO series *The Wire*.

MAITHILI NARASIMHA is a Ph.D. student in the School of Information and Computer Sciences at the University of California–Irvine. Her research interests focus on system and network security.

JAMES P. NEHF is Professor and Cleon H. Foust Fellow at the Indiana University School of Law–Indianapolis. Nehf has published widely on consumer law and information privacy. He also serves as the U.S. representative on the executive board of the International Association for Consumer Law.

ANN MARIE NEIR received her JD degree from the University of Kansas in 2006.

PATRICIA OSLUND is a Research Economist for the Policy Research Institute at the University of Kansas.

SARAH K. PARKINSON received bachelor's degrees in psychology and sociology at the University of Kansas. She is currently working on her master's at the University of Kansas with a focus on gender, race, and Asian American studies.

SHAUN PARKMAN is a graduate student in the Department of Sociology at the University of Kansas and has interests in economic sociology, environmental sociology, and social theory. He is a co-editor of *Social Thought and Research*.

APRIL PATTAVINA is Assistant Professor of Criminal Justice at the University of Massachusetts–Lowell. She studies the impact of information technology on the criminal justice system and spatial analytic techniques in the study of crime. She is the editor of *Information Technology and the Criminal Justice System* (2004).

MARCY E. PEEK is Assistant Professor of Law at Whittier Law School. Peek earned her JD from Harvard Law School. Her most recent article is "Passing Beyond Identity on the Internet: Espionage, Counterespionage, and Intersectionality in the Internet Age," which appeared in the *Vermont Law Review*.

SEAN M. PEEK holds a BA in Political Science from the University of Washington. He has spent significant time working in London and studying Spanish at the University of Guadalajara, Mexico. He is currently attending the Thomas M. Cooley School of Law in Lansing, Michigan.

MARK PERRY is Professor on the Faculty of Law and the Faculty of Science at the University of Western Ontario. He is a Barrister and Solicitor of the Law Society of Upper Canada, a Faculty Fellow at IBM's Center for Advanced Studies, and a correspondent for the *Computer Law and Security Report*.

UROS PETROVIC is a graduate student in the Department of Sociology at the University of Kansas and has interests in theory, culture, nationalism, and race and ethnicity.

MICHAEL PETRUNIK is Associate Professor of Criminology at the University of Ottawa. He has written extensively on legislation and policy for dangerous offenders.

ROSS D. PETTY is Professor of Marketing Law at Babson College. He is the author of *The Impact of Advertising Law on Business and Public Policy* (1992) and the recipient of the Thomas C. Kinnear Award for the best article published in the *Journal of Public Policy & Marketing* (2005).

TIANA MARIE PLATZ is a Research and Teaching Assistant at the University of Massachusetts–Lowell. She is involved in research examining the prevalence of dual arrest in intimate-partner cases funded by the Department of Justice.

PETER RAVEN-HANSEN is Glen Earl Weston Research Professor of Law at George Washington University Law School. He is a co-author of *National Security Law* (4th ed., 2006) and has written extensively on topics of national security law.

LESLIE ANN REIS is Director of the Center for Information Technology and Privacy Law and Adjunct Professor of the John Marshall Law School. Professor Reis supervises the law school's distinguished *Journal of Computer and Information Law*.



SADIQ REZA is Professor of Law at New York Law School. He writes and teaches on American criminal law and procedure, comparative criminal procedure, and criminal law and procedure under Islamic law (Sharia) and in countries of the modern Muslim world.

NEIL M. RICHARDS is Associate Professor of Law at Washington University in St. Louis. He writes on privacy law, First Amendment law, and legal history.

CHRISTINE M. ROBINSON is Assistant Professor of Sociology and Interdisciplinary Liberal Studies at James Madison University. Her research focuses on the social control of deviance, deviant communities, subcultures, and countermovements.

PATRICIA A. ROCHE is Assistant Professor of Health Law at the Boston University School of Public Health. Her areas of research and writing include patient rights, particularly rights to privacy; the protection of research subjects; and the impact of genetic technologies on individual rights.

MARC ROTENBERG is Executive Director of the Electronic Privacy Information Center and Adjunct Professor of Law at Georgetown University. He frequently testifies before Congress on privacy issues. He has received the World Technology Award for Law and the ABA Cyberspace Law Excellence Award.

LANCE E. ROTHENBERG is an associate with Fulbright & Jaworski, LLP. He is the recipient of the Laura E. Turley Award for his article “Re-Thinking Privacy: Peeping Toms, Video Voyeurs and the Failure of Criminal Law to Recognize a Reasonable Expectation of Privacy in the Public Space” (2000).

VINCENT J. SAMAR is Adjunct Professor of Law at Chicago-Kent College of Law and Adjunct Professor of Philosophy at Loyola University in Chicago. He is the author of *Justifying Judgment: Practicing Law and Philosophy* (1998) and *The Right to Privacy: Gays, Lesbians and the Constitution* (1991).

ELIZABETH J. SAMUELS is Associate Professor at the University of Baltimore School of Law. She has written extensively on the history and current status of adoption records and the laws governing birth parent consent to adoption. In 2004 she was named an “Angel in Adoption” by the Congressional Coalition on Adoption Institute.

CHRISTINE SCHNEIDER is a graduate student in sociology at Case Western Reserve University. Her research interests are in the field of medical sociology.

RIC SIMMONS is Assistant Professor at the Moritz College of Law at The Ohio State University. He is a former prosecutor in New York City and has written numerous articles exploring the relationship between the Fourth Amendment and emerging technologies.

DANIEL J. SOLOVE is Associate Professor at the George Washington University Law School. He is the author of *The Digital Person: Technology and Privacy in the Information Age* (2004) and *Information Privacy Law* (2006) (with Marc Rotenberg and Paul M. Schwartz).

DAVID E. SORKIN is Associate Professor of Law at the John Marshall Law School in Chicago and is affiliated with the school's Center for Information Technology and Privacy Law. His work focuses on Internet law and policy, informational privacy, consumer protection, and dispute resolution.

SUE E. SPIVEY is Associate Professor of Social Science at the Center for Liberal and Applied Social Sciences at James Madison University. She has written on issues of inequality, specifically regarding race, class, gender, and sexuality as they pertain to sociology, political science, and economics.

THOMAS G. STACY is Professor of Law at the University of Kansas. He has written on constitutional criminal procedure, constitutional protections of autonomy and religion, constitutional federalism, and substantive criminal law. His articles have appeared in the *Columbia Law Review* and the *Cornell Law Review*.

IAN W. STAPLES is currently a political science major and Legislative Director of the Student Senate of the University of Kansas. His interests include the American political system and public policy.

WILLIAM G. STAPLES is Professor and Chair of Sociology at the University of Kansas, the oldest sociology department in the United States. Staples received his Ph.D. from the University of Southern California and was a Postdoctoral Fellow at UCLA. His books include *Castles of Our Conscience: Social Control and the American State, 1800–1985* (1991); *Everyday Surveillance: Vigilance and Visibility in Postmodern Life* (2000); and *Power, Profits, and Patriarchy: The Social Organization of Work at a British Metal Trades Firm, 1791–1922* (with Clifford L. Staples) (2001).

DOREEN STARKE-MEYERRING is Assistant Professor of Rhetoric and Scientific and Technical Communication at McGill University in Montreal. She has written on rhetoric and persuasion in technology-related policy discourse, digital literacies, and the link between globalization, technology discourse, and social change.

DWIGHT L. TEETER, JR., is Professor in the School of Journalism & Electronic Media at the University of Tennessee. He is the co-author of two textbooks, *Law of Mass Communications* (11th ed., 2004, with Bill Loving), and *Voices of a Nation: A History of Mass Media in the United States* (2002, with Jean Folkerts).

ATHAN THEOHARIS is Professor of History at Marquette University and the author of *Chasing Spies: How the FBI Failed in Counterintelligence but Promoted the Politics of McCarthyism in the Cold War Years* (2002) and *The FBI and American Democracy: A Brief Critical History* (2004).

ALEXANDER TESISIS is Visiting Assistant Professor of Law at Marquette University. He is the author of *The Thirteenth Amendment and American Freedom* (2004) and *Destructive Messages: How Hate Speech Paves the Way for Harmful Social Movements* (2002).

KENNETH D. TUNNELL is Professor of Criminal Justice at Eastern Kentucky University. He is the author of *Pissing on Demand* (2004) and *Living Off Crime* (2005) and editor of *Political Crime in Contemporary America* (1994).



ROBERT G. VAUGHN is Professor of Law and A. Allen King Scholar at American University. He teaches a seminar on Public Information Law and Policy and is the author of a number of works relating to freedom of information, whistleblower protection, and public employment law.

CAROL A. B. WARREN is Professor Emeritus of Sociology at the University of Kansas. Her interests are in social control, law and psychiatry, gender, and interpretive methods. She is the author of *Pushbutton Psychiatry: A History of Electroconvulsive Therapy in America* (2002, with Timothy Kneeland).

JULIET WILLIAMS holds a joint appointment in the Law & Society Program and the Women's Studies Program at the University of California–Santa Barbara. She edited *Public Affairs: Politics in the Age of Sex Scandals* (2004) and is the author of *Liberalism and the Limits of Power* (2005).

CHRISTOPHER WOLF is a partner in Proskauer Rose LLP, where he chairs the firm's Privacy and Data Security Practice Group. He was counsel for the plaintiff in *McVeigh v. Cohen*, the privacy case involving "Don't ask, don't tell." He is a recipient of the 2005 Burton Award for Excellence in Legal Writing.

MARY W. S. WONG is Professor of Law at Franklin Pierce Law Center. Her interests are in intellectual property and information technology laws, particularly the legal and policy challenges presented by digital technology and the Internet, in relation to both domestic U.S. law and international legal developments.

BRIAN L. ZIRKLE is a graduate student at the University of Kansas. His areas of interest are social control and work. He is currently examining public harassment as a form of social control and is beginning a project examining the cultural dynamics of temporary work.

Index

Boldface type refers to main entry.

- Abacus, 307
Abandonment doctrine, 244–245
Abood v. Detroit Board of Education
 (freedom of association), 237
Abortion, **1–7**, 412, 623; access to by poor
 and rural women, 3; ACLU support
 for, 16, 60; activists against, 3–5; as
 birth control, 2; clinics and clinic
 workers, 4; confidentiality and, 1;
 DeShaney v. Winnebago County
 Dept. Social Services, 606; Finkbine,
 Sheri, 1; gender equality and,
 250–251; government assistance for,
 60, 251, 463; harassment of doctors
 who perform, 184; history of, 1–2,
 469; Hyde Amendment, 463;
 medical, 6; morning-after pill as, 6,
 60; number of, 6; parental consent, 3,
 463; partial-birth, 6; paternity issues,
 375; patient privacy and, 4–6;
 Planned Parenthood of Southeastern
 Pennsylvania v. Casey (reproductive
 rights), 3, 17, 130, 219, 326, 603,
 613; as a privacy issue, 1, 2, 120,
 278, 436, 462–463, 613, 624; pro-
 choice movement, 1, 2; pro-life
 movement, 1, 2–3; *Roe v. Wade* 2, 6,
 60, 64, 66, 128, 130, 131, 165, 183,
 250–251, 325, 396, 462–463,
 469–473, 605, 613, 624; spousal
 consent, 3, 264; therapeutic, 1;
 trimester analysis, Supreme Court
 ruling, 472; undue burden standard,
 131; as unenumerated right, 126;
 waiting periods, 3; *Webster v.*
 Reproductive Health Services, 6,
 396, 437, **605–607**
Abortion and the Politics of Motherhood,
 2
abortioncams.com, 4
Accountability, 400–401
Accountant-client privilege, 443
Accurate Credit Transactions Act of 2003,
 322
Accurint, 342
Active airborne surveillance, 13
Actual malice, 24, 26
Adams, John, 162
Adams, John Quincy, 163
Adams, Samuel, 163
Adams, Sherman, 226
Adams v. Williams (automobile searches),
 34
Adoption, **7–12**; adoptees, rights of, 9–12;
 birth certificates, 7, 8; closed
 records, 7, 9, 11; contact preference
 forms, 10; contact vs. disclosure veto
 systems, 7, 10; *Does v. State* (1999),
 11, 12; historical perspectives on, 7,
 8; *Doe v. Sundquist* (1999), 11;
 matching practices in, 9; mutual
 consent registries, 9–10; Sexual
 History Newspaper Requirement
 (Florida), 374



- Advanced Encryption Standard (AES), 28, 103, 153
- Advanced Research Project Agency Network (ARPANET), 257, 297
- Adware, 203, 554
- Aerial surveillance, 80–82, 154, 155, 318–319
- Axiom, 564
- Affection, public displays of, 335
- Age Discrimination Act of 1967, 619
- Agent-initiated surveillance, 539–540
- Aid to Families with Dependent Children, 109
- Airborne surveillance and intelligence, **12–14**, 547
- Airspace, as sovereign territory, 14
- Air travel, **14–15**, 18; Computer-Assisted Passenger Prescreening System (CAPPS II), **106–107**
- Alabama v. White* (automobile searches), 30
- Alien and Registration Act of 1940, 132, 282, 336
- Aliens, denaturalization and deportation of, 338
- Alito, Justice Samuel, 6, 131
- Ali v. Playgirl, Inc.* (appropriation of name or likeness), 432
- Allen, Anita, 410, 412, 615
- Almandos, Luis Reyna, 231
- Alpha Medical Clinic v. Anderson* (late-term abortions), 615
- Al Qaeda, 125, 351
- Alsop, Joseph, 226–227
- American Association of Registration Executives, 8
- American Bar Association, 147
- American Birth Control League (ABCL), 59
- American Civil Liberties Union (ACLU), **15–17**, 421, 627; chemical castration, challenges to, 497; civil liberties, absolutist approach to, 16; creation of, 15–16; as defense counsel, 16; individual privacy, protection of, 16–17, 83; legalization of abortion, support for, 16, 60; membership of, 16; Safe Harbor Principles, stand on, 476; Technology and Liberty Project, 17
- American Coalition of Life Activists (ACLA), 4
- American Communities Survey, 571–572
- American Jobs Creation Act of 2004, 295
- American Law Institute: Model Penal Code, 65, 326; *Restatement of Torts*, 398
- American Library Association (ALA): Code of Ethics, 328–329; definition of privacy, 327, 328
- American Management Association, 590
- American Medical Association (AMA), 56, 60
- American Public Health Association (APHA), 56
- Americans with Disabilities Act of 1990, 619
- American Teleservices Association, 178
- America Online, 309
- Anderson, Ross, 29
- Androgyny, 516
- Animal Farm*, 424
- Anonymity, **17–19**, 408; in assisted reproductive technologies (ART), 21–22; for birth parents in adoptions, 7; in a cashless society, 166; computers and diminished ability to maintain, 17–19; digital signatures, 166; of human study subjects, 286; and Internet use, 153, 309; online, breaches of, 17; overriding, reasons for, 23–24; personal identifiers and, 17; as the “refuge of scoundrels,” 18; as self-directed informational privacy, 18; telemarketing as intrusion on, 177; and United States Postal Service, 572, 573; value of, 18; violations of, 551; in voting, 18
- Anthropometric identification system, 53–54
- Anti-abortion activists, 3–5
- Anti-abortion laws, repeal of, 60
- Anti-contraception laws, 59
- Anti-war protestors, 284–285
- Anti-wiretap statutes, **19–21**, 47
- Appropriation of name or likeness privacy tort, 73, 311, 394, 398, 430, 432–433
- Aristotle, 405, 447–448
- Arizona v. Hicks* (plain view doctrine), 388

- Armed forces: anti-gay harassment, 180; “don’t ask, don’t tell” policy, **178–181**; drug testing in, 185, 590; homosexuality and, 179–180; racial integration of, 179; Servicemembers Legal Defense Network (SLDN), 180; substance abuse prevention programs, 589
- Arms control, 91
- Arrington v. New York Times* (appropriation of name or likeness), 433
- Arthur Andersen LLP v. United States* (e-mail, retention of), 201
- Artificial insemination, 21
- Ashcroft, John, 6
- Assassinations of foreign leaders, U.S. involvement in, 92, 93, 488
- Assisted reproductive technologies (ART), **21–24**; anonymity and, 21–22; defined, 21; giving up anonymity, reasons for, 23–24
- Associated Press v. Walker* (libel), **24–26**
- Asymmetric-key cryptography. *See* Public-key cryptography
- Attorney-client privilege, 439–440
- Audio surveillance, 21
- Audit trail, currency transactions, 43
- Authentication, **26–27**; Clipper and Capstone systems, **101–104**, 302; cryptography as, 153; defined, 26; Internet access, 305, 306; Pretty Good Privacy (PGP) program, 309, **388–389**; single-factor, 26–27; Social Security number as, 514
- Authoritarian governments, information access in, 174
- Automatic teller machine (ATM), **27–30**; access to accounts from, 28–29; criminal activity involving, 29; invention of, 28; password protection, 373; using, 334
- Automobile, **30–31**; cell phones, use of, 334; electronic toll collection, **206–207**; exclusionary rule and, 31; explosives, detecting, 622; fingerprint scanners for, 232; passengers, searches of, 35; physical tracking device, insertion of, 457; plain view exception, 34, 386–387, 519; police checkpoints, 30, 31, 33, 123, 393, 510–513; reasonable expectation of privacy and, 32, 80, 518; road rage, 334; searches of, 30–31, **32–36**, 79–80, 86–88, 123, 144–145, 511, 518–519; sense-enhancing technologies for search of, 490
- Avery Dennison adhesive technology economic espionage case, 292
- AWACS aircraft, 13
- Background checks, **37–38**, 189, 420; consent for, 38; defined, 37; for employment, 37–38; private investigators and, 434; tenants, 321, 323; unregulated, 38; of volunteers by charitable organizations, 37, 38
- Backscatter portal, 621
- Baldwin, Roger, 16
- Banisar, David, 420
- Bank Holding Company Act of 1956, 40
- Banking and financial records, **38–43**, 400; account takeover, 289; Bank Secrecy Act (BSA), 39–40, **43–45**; credit card transactions, 38; Currency Transaction Report, 40, 43; disclosure of, 39, 170–171; European Data Protection Directive, 41, **207–210**, 303, 395; Fair Credit Reporting Act (FCRA), 38, 39, 42, 119; Financial Services Modernization Act of 1999, 39, 40–42, 119; gathering information about, reasons for, 44; government access to, 39; identity fraud, potential for, 39; opt-in vs. opt-out, 41, 137, **363–364**, 476; Right to Financial Privacy Act (RFPA), 39; sharing of information about, 39, 40–41, 42, 119; Suspicious Activity Report, 43
- Bankruptcy, 172, 323
- Bankruptcy Abuse: Prevention and Consumer Protection Act of 2005, 384
- Bank Secrecy Act (BSA), 39–40, **43–45**
- Barber v. Time, Inc.* (public disclosure of private facts), 431
- Bar code readers and scanners, **45–46**, 349
- Barlow, John, 419
- Bartnicki v. Vopper* (wiretapping), **46–49**, 73



- Bauer v. Kincaid* (public records), 49,
49–51
- Bay of Pigs invasion, 92, 93
- Bazooka microphones, 312
- BBBOnline privacy seal program, 302, 476
- Bell, Alexander Graham, 597
- Bellis v. United States* (self-incrimination,
partnership), 71
- Berman, Jerry, 420
- Bertillonage, 54
- Bertillon, Alphonse, 53
- Best interest of the child test, 217, 220
- Better Homes for America*, 276
- Bigamy, 218
- Big Brother, **51–53**, 180
- Bingham, Rep. John A., 127
- Biomedical experimentation, 286–288
- Biometric identifiers, **53–55**; for air
travelers, 15; applications of, 54; for
ATM machines, 28, 54; as
authentication, 26; in bar codes, 45–
46; categorization of, 54; defined,
53; fingerprints, 15, 28, 45, 54, 107,
230–232, 341; for identification, 54;
iris scans, 15, 28; on national identity
card, 349; and passwords compared,
373; physical attributes as, 54;
privacy issues raised by, 54–55; in
smart cards, 510; theft of, 55; for
verification, 54; voice, 566–577,
598; voiceprints, 107
- Birth certificate(s), **55–58**; for adopted
children, 7, 8; confidentiality of, 57;
demographic information contained
on, 56; efforts to standardize, 55–56;
identity fraud and, 57; restricted
access to, 57–58; U.S. Standard
Certificate of Live Birth, 56–57;
walk-in requests for, 57
- Birth control, **58–61**, 412, 623; cost as
barrier to, 60; *Eisenstadt v. Baird*, 2,
17, 60, 66, **191–192**, 219, 250, 265,
613; family planning, public
acceptance of, 59, 263–264, 623;
federal support for, 60; *Griswold v.*
Connecticut, 2, 17, 65–66, 126, 131,
165, 182, 191, 218, **261–266**, 325,
396, 436, 462, 613, 623; Margaret
Sanger, 58, 59; pills, 59, 60;
prescriptions, refusal of pharmacists
to fill, 60; as right to be let alone, 59;
role of in women's equality, 61;
sterilization, 60, 182, 411, 464, 497;
and women's equality, 250–251. *See*
also Contraception
- Birth rate, 59
- Birth registration, 56
- Black box devices, 202
- Black, Justice Hugo, 162, 182, 264
- Blacklisting, 284, 337–338
- Blackmun, Justice Harry A., 6, 183, 463,
518
- Black Panther Party, 133, 574
- Blaze, Matt, 103
- Blood alcohol level, 61, 145, 477, 510
- Blood testing, **61–64**, 477–478; of criminal
suspects and arrestees, 145; for
detecting substance use and abuse,
61, 185, 508–509; for DNA typing,
61, 63; of employees, 37; greater
good argument for, 61–62; for HIV,
62–63; legality of, 61–62;
premarital, for syphilis, 62; prenatal,
62; results, disclosure of, 63
- Bloustein, Edward J., 408–409
- Board of Directors of Rotary International*
v. Rotary Club of Duarte (freedom of
association), 238
- Board of Education of Independent School*
District Number 92 v. Earls (drug
testing, extracurricular activities),
187
- Body-cavity searches, 391, 533
- Bono, Rep. Sonny, 369
- Border Patrol checkpoint operations, 33,
123, 560
- Bork, Robert, 594
- Bottoms v. Bottoms* (child custody), 517
- Bowers v. Hardwick* (consensual
homosexual acts), **64–67**, 128, **265**,
324, 436–437, 516, 624
- Boyd v. United States* (seizure of personal
papers), **67–72**, 74, 154, 261, 607,
623–624
- Boy Scouts of America v. Dale* (freedom of
association), 238–239
- Bradwell v. Illinois* (women's equality),
248
- Brandeis, Justice Louis B., **72–76**, 407,
409; Brandeis Brief, 75; and cult of
domesticity, 248–249; defense of
federalism, 75; defense of the First

- Amendment, 74; dissenting opinion in *Olmstead v. United States*, 72, 73–74, 120, 169, 357, 360–361; on home, 275, 278; influence of on privacy law, 72; New Deal, support of, 75; right to be let alone doctrine, 21, 72, 120, 169, 311, 357, 430, 462, **466–467**, 614; “The Right to Privacy,” 72, 248, 311, 397, 406, 430, 466
- Brandeis Award, Privacy International, 75
- Brandeis Brief, 75
- Brandenburg v. Ohio* (inflammatory speech), 16, 74
- Branzburg v. Hayes* (reporter’s privilege), 442
- Breast cancer, genetic testing for, 378, 379
- Breastfeeding, in public, 335
- Brennan, Justice William J. Jr., 162, 192, 250, 263, 313, 340, 519
- Breyer, Justice Stephen, 487
- Broadcast signals, interception of, 13
- Brock, David, 99
- Brontë v. Finkel* (freedom of association), 237
- Brown v. Board of Education* (school segregation), 16, 284
- Brownell, Herbert, 226
- Buck v. Bell* (forced sterilization), 527–528
- Buckley Amendment Family Educational Rights and Privacy Act (FERPA), 460
- Buckley, Sen. James L., 221
- Bugging, 21, 193, 202, 204
- Burger, Chief Justice Warren, 183, 369, 519
- Bush, President George H. W., 99, 186
- Bush, President George W.: on abortion, 6; Foreign Intelligence Surveillance Act (FISA), violations of, 351, 401; national identity card, 348; wiretaps on U.S. citizens calling overseas, 612
- Buxton, Charles Lee, 59, 262
- Cable Communications Policy Act of 1984, **77–79**; personally identifiable information, collection and disclosure of, 77–78, 169, 385; privacy notices, requirements for, 78; viewing habits, knowledge of, 77
- Cached data, 114, 299
- Cady v. Dombrowski* (automobile searches), **79–80**
- California v. Ciraolo* (aerial surveillance), **80–82**, 154, 155, 318–319, 545–546
- California v. Greenwood* (garbage at curb), 155–156, 244, 458, 560, 580
- California v. Hodari D.* (random searches), 233
- Caller ID, 90, 197
- Camfield v. City of Oklahoma City* (obscenity), **83–84**
- Cannon v. United States* (bigamy), 218
- CAN-SPAM Act of 2003, 521, 554
- Cantrell, Margaret Mae, 313
- Capstone chips. *See* Clipper and Capstone chips
- Cardwell v. Levy* (automobile searches), 32
- Carey v. Population Services International* (contraception, minors), 66, 374
- Carnivore software, **84–86**, 200, 302, 308, 382, 609
- Carroll v. United States* (automobile searches), 30, 34, 35, **86–88**
- Cashless society, 165
- Castro, Fidel, U.S. efforts to assassinate, 93, 488
- Celebrities, privacy rights of, 313–314, 367–369, 425–426
- Cellular telephone(s), **88–91**, 204, 395; in airborne surveillance and intelligence, 13; analog vs. digital, 89; CIA monitoring of, 93; credit score in obtaining, 130; disposable, 90; eavesdropping, potential for, 88; and fixed telephones compared, 89, 90; location of, determining, 90, 257, 318; privacy issues unique to women, 613; private investigators and, 434; proliferation of, 258; ring tones, downloading, 308; technical challenges re: privacy, 88–89; use of, 334, 424; video voyeurism and, 545, 600; wiretapping and, 19, 46–49, 104
- Censorship, 25
- Center for Democracy and Technology (CDT), 420–421, 627
- Centers for Disease Control and Prevention (CDC), 56, 446, 512
- Central Intelligence Agency (CIA), **91–94**, 488; clandestine operations by,



- 92–93; Cold War activities, 92–93;
and Freedom of Information Act,
240; mission, 91; origins of, 91–92;
and Privacy Act of 1974,
exemptions, 417; and privacy,
violations of, 93–94; after September
11 attacks, 92; structural
organization, 91; Watergate scandal
and, 92
- Chain of custody, digital evidence, 114,
115
- Chambers v. Mahoney* (automobile
searches), 30
- Chandler v. Miller* (urine testing), 17,
590
- Chaplin, Charlie, 337
- Chemical castration, 496–497
- Child abuse, 37, 615
- Child custody, 217, 517
- Child molestation, 323
- Child pornography, 83–84, 365–366
- Children's Online Privacy Protection Act
of 1998 (COPPA), **94–95**, 303, 364,
399, 403, **428**
- Child Welfare Act of America, 8
- Chimel v. California* (search incident to
arrest), **95–97**, 558
- Christie, Agatha, 314
- Christopher's Law, 494
- Church Committee. *See* Senate Select
Committee to Study Governmental
Operations with Respect to
Intelligence Activities (Church
Committee)
- Citizens Against Drug Impaired Drivers,
512
- Citizens for Reliable and Safe Highways,
512
- Civil inattention, 334
- Civil liberties, sacrifice of, 401–402
- Civil Rights Act of 1964, 499, 500, 619
- Civil rights movement, 226, 284, 345
- Civil service laws, **97–99**; employee
selection procedures, 97–98;
personal accountability in, 98;
privacy protection for public
employees, 97, 98
- Civil Service Reform Act of 1883, 97
- Civil War, 164
- Claritas, 563, 564
- Clickstream data, 304
- Clinton, Hillary Rodham, 99
- Clinton-Lewinsky scandal, **99–101**, 400
- Clinton, President William J.: efforts to
overturn ban on gay military
personnel, 179–180; Escrowed
Encryption Standard (EES), 101;
Monica Lewinsky and, **99–101**, 400;
national identity card, 348; selective
availability, end to, 257; sex offender
registries, 494
- Clipper and Capstone chips, **101–104**, 302
- Closed-circuit television (CCTV), 544
- Code of Fair Information Practices, 214
- Code of Fair Labor Practices, 214
- Coherent cluster concept, 412
- Coherentism, 406, 407–411
- Cold War, 337; CIA activities during, 92–
93
- Cole v. Young* (response to McCarthyism),
338
- Colfax, Schuyler, 164
- Collection agencies, 142, 290
- Collective bargaining, right to, 237
- Colmer, William, 284
- Colorado v. Bannister* (automobile
searches, plain view exception),
34
- Combined DNA Index System (CODIS),
498
- Committee in Support of the People of El
Salvador (CISPES), 227
- Communications Act of 1934, 361, 551
- Communications Assistance for Law
Enforcement Act (CALEA), 102,
104–105
- Communications Decency Act (CDA),
105–106
- Communications mobility, 89–90. *See also*
Cellular telephone(s)
- Communist Party, U.S., 132, 336; film
industry infiltration, 284, 337–338;
government infiltration, 283; labor
union infiltration, 282, 283,
604–605
- Communist Party v. Subversive Activities
Control Board* (freedom of
association), 132, 236
- Community-based activism, 16
- Community notification systems (CNS),
493
- Community Protection Act of 1990, 493

- Comprehensive Crime Control Act (1990), 63
- CompuServe Inc. v. Cyber Promotions, Inc.* (spam), 521
- Computer-Assisted Passenger Prescreening System (CAPPS II), **106–107**, 108
- Computer espionage, 108
- Computer extortion, 108
- Computer forensics, 111, 114, 115
- Computer Fraud and Abuse Act of 1986, **107–109**
- Computer Matching and Privacy Protection Act of 1998, **109–111**
- Computer(s), **111–116**, 399; altered images and sounds, 115; anti-spyware programs, 309; anti-virus software, 308; anonymity and, 17–19; back-door entry to, 114; broadband connection, 114; crash of, 114–115; data exchange between, 167; digital divide, 422; disk wiping software, 113; effect of on economic recordkeeping, 563; encryption of information, 102; firewalls, 308, 309; Fourth Amendment protection and, 125, 360; hacking, 41, 107, 289, 381, 435; identity fraud and, 39; industrial espionage, potential for, 293; interconnectivity, challenges of, 107, 111; keystroke loggers, 86, 203, 308, **320**; legal liability for failing to protect sensitive data, 111; overwriting files, 113, 114; password protection, 27, **373–374**; pornography on, 105, 114; and potential for sharing financial records, 38–39; removing files from, 112–113; scanning device for fingerprinting, 230; security, 86, 107; spyware, 114, 303, 306, 308–309, 381, 567; unauthorized access to, 108; wireless (Wi-Fi) connectivity, 111, 114
- Computer trespass, 108
- Comstock, Anthony, 59
- Comstock Law, 59, 60
- Confession. *See* Religious privilege
- Confessional culture, **116–117**
- Confidentiality, **117–120**; abortions and, 1; adoption and, 7; in assisted reproductive technologies, 22; of birth certificates, 57, 58; and blood testing campaign against syphilis, 62; breach of, 119, 433; defined, 117; of e-mail messages, 200–201; in employer-employee relationships, 119; exceptions to, 117–118; FBI records, 226; of financial records, 119; formal agreements regarding, 119; Globally Unique Identifier (GUID), 301; and informed consent, conflict between, 286, 287; juvenile arrestees, 148; of library records, 327, 399; of married relationships, 265; of medical records, 63, 111, 118–119, 268–269; origins of the word, 117, 118–119; partner notification, 372; patient rights, **376–370**; physician-patient privilege, 270, 375, 439, 442–443; as privacy, 410–411; privilege and, 118; rootkits, 301, 308; statutes addressing, 118–119; trade secrets, 48, 119; uninstall features, 301, 308; XCP (Extended Copy Protection) software, 301. *See also* Informational privacy; Privilege
- Conflicts of interest, 170, 423
- Congress of Industrial Organizations (CIO), 283
- Conscientious objection, 16
- Constitutionally protected area test, 361
- Constitutional protections, **120–132**, 380; adaptations to new technologies, need for, 357; automobile and, 30–31; individual autonomy, 125–131; informational privacy, 120–125, 243, 394; for prisoners, 390; privacy law, 396–397; for reproductive rights, 462; and strip searches, 532; tradition, reliance on, 128–129; and traffic crimes, 461; for the unborn, 471; unenumerated rights, 126, 127–131, 396
- Consumer Credit Protection Act of 1968, 211
- Consumer databases, security breaches of, 137
- Consumer debt, 136, 142, 211
- Consumer Return Databases, 564
- Contact tracing. *See* Partner notification



- Contact veto system, 7, 10
- Content-neutral laws of general applicability, 47
- Contraception: emergency, 6, 60; influence of on abortion, 2; married couples, *Griswold v. Connecticut*, 2, 17, 59, 66, 130, 131, 191, **261–266**, 325, 396, 436, 462, 613, 623; minors, *Carey v. Population Services International*, 66; morning-after pill, 6; as unenumerated right, 126; unmarried couples, *Eisenstadt v. Baird*, 2, 17, 60, 66, 130, **191–192**, 219, 250, 265, 613
- “Contra” conspiracy, 93
- Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 215
- Cooley, Judge Thomas, 311, 397, 466
- Coolidge, President Calvin, 276
- Coolidge v. New Hampshire* (plain view doctrine), 387
- Cooper v. Pate* (constitutional protects for prisoners), 390
- Copyright infringement, 301
- Coser, Rose, 422
- Couch v. United States* (private information from third parties), 318
- Counterfeiting, 167
- Counterintelligence, 91
- Counter Intelligence Program (COINTELPRO), **132–134**, 225, 280
- Countersurveillance, 462, 540
- Counterterrorism activities, 91
- Cousins v. Wigoda* (freedom of association), 237–238
- Covenant of enjoyment, 321, 324
- Cox Broadcasting Corp. v. Cohn* (public disclosure of private facts), **134–135**, 314, 432
- Credit bureaus: credit report, requesting, 141; data compiled by, 140–141; Fair Credit Reporting Act (FCRA) and, 42, 141, **211–214**; sharing of consumer information by, 42, 138; three major, 140
- Credit card(s), **135–138**; account takeover, 289; application fraud, 289; debt, employee, 37; fingerprints on, 232; history of, 135–136; identity fraud and, 135, 137–138, 402; Internet transactions, 307, 308, 381; number, disclosure of, 197; personally identifiable information stored on, 384; proliferation of, 165; role of credit score in issuance of, 139, 211; as a source of information for data brokers, 157; system, organizational structure of, 137; transaction-generated data, 136, **562–565**; transactions, sharing of information about, 38
- Credit history, 17, 138, 211, 322–323
- Credit rating, **138–143**; accuracy of, 140; collection agencies, referral to, 142; compilation of, 141–142; identity fraud and, 289; mistakes in, 348; on-time payments, 141; positive and negative influences on, 141–142; tenants, 321; uses of, 139
- Credit reports: information contained on, 141; on the Internet, 213; sharing of, 137, 141, 213–214
- Credit score, 138; criticisms of, 139–140; determination of, 140, 158, 159; fairness of, 140; raising, 142
- Crimes Against Nature statutes, 437
- Criminal identity theft, 289
- Criminal suspects and arrestees, **143–148**; blood testing, 145; court records, disclosure of, 172; disclosure of information about, 143, 146–148; DNA samples from, 146, 498; drug testing of, 185–186; forced sterilization of, 182, 497, 527; juvenile confidentiality, 148; privacy rights of, 143, 285–286; rap sheet, 148; searches, 144–145
- Criminal trespass, 566
- Cruel and Unusual Punishment clause, Eighth Amendment, 390, 392
- Cruzan v. Director of the Missouri Department of Health* (right to die), 16, **148–151**, 265, 397, 468
- Cryptography, **151–153**; Clinton administration support for, 103; Clipper and Capstone chips, **101–104**, 302; Data Encryption Standard (DES), 28, 103, 152; functions of, 153; key, as

- authentication, 26; need for, 151;
 - public-key, 152–153, 166, 388–389;
 - substitution, 151; symmetric-key, 152; for systems of anonymity, 19;
 - transposition, 151; types of, 151
- Cult of domesticity, 248–249, 275
- Curcio v. United States* (seizure of personal papers), 71
- Currency and Foreign Transactions Reporting Act. *See* Bank Secrecy Act (BSA)
- Currency Transaction Report, 40, 43
- Curtilage, **153–156**, 357; fences, 155, 156; four facts determining, 154; garbage at the curb, 155–156, 458, 560; “No Trespassing” signs, 155, 355, 356; open fields doctrine, 154–155, 318, 355, 356; *United States v. Dunn*, **577–578**
- Curtis Publishing Company v. Butts* (libel), 24, 25
- Customer Proprietary Network Information (CPNI), 551
- Customer relations management, 159
- Customs Act of 1867, 69
- Cyber Bug, 547
- Daily Times Democrat v. Graham* (public disclosure of private facts), 431
- Dalia v. United States* (multiple search warrants), 582
- Danai v. Canal Square Associates* (co-mingled garbage), 247
- Data brokers, 75, 136, **157–159**, 166, 301, **383**, 564
- Data controller, 208
- Data Encryption Standard (DES), 28, 103, 152
- Data intercept tools, 85. *See also* Carnivore
- “Datamania,” 565
- Data mining, 137, **159–161**, 204, 415, 536; data sources, 159–160; and personally identifiable information, 383; privacy concerns, 161, 420; social benefits of, 160–161; and statistical analysis compared, 160; terrorists, identification of, 161, 342
- Data packets, 202
- Dataveillance, 18
- Davies v. Freedom of Information Commission* (freedom of information), 184
- Davis v. Mississippi* (fingerprinting), **161–162**
- Daytime television talk shows, 116
- DCS1000, 84–85, 200, 382, 600
- Deadbeat dads, 375
- Debit cards, 166
- Deceased celebrities, privacy rights of, 314
- Decennial census, 56, 569
- Decisional privacy, 265, 393, 412
- Decision tree analysis, 160
- Declaration of Independence, **162–165**; enforcement mechanism, lack of, 163; origins of, 162–163; and slavery, failure to address, 163, 164
- deCODE Genetics, 176
- Defamation, truth as defense for, 134–135, 408
- Defense Language Institute, 180
- Defense of Marriage Act, 131
- Delaware v. Prouse* (automobile searches), 33
- DeMay v. Roberts* (privacy, childbirth), 397, 614
- Democratic governments, information access in, 174
- Dennis v. United States* (Communist party membership), 132
- Depo-Provera, 464, 496, 497
- DeShaney v. Winnebago County Dept. Social Services* (abortion), 606
- DeSilver, Albert, 16
- The Desperate Hours*, 313, 561–562
- Dialed number recorder (DNR), 195
- Diana, Princess of Wales, 367, 368
- Diaries, 124, 483
- Diaz v. Oakland Tribune* (public disclosure of private facts), 431
- DidTheyReadIt server, 308
- Dietemann v. Time, Inc.* (intrusion upon seclusion), 312, 430
- Diffie, Whitfield, 166
- Digital bit streams, 202
- Digital cash, **165–166**, 562
- Digital credentials, 27
- Digital divide, 422
- Digital evidence, handling of, 114, 115
- Digital rights management (DRM), 301



- Digital signatures, 153, **166–168**
- Digital Signature Standard, 102
- Direct Marketing Association, Privacy Promise, 364
- Dirkes v. Borough of Runnimeade* (video rentals, pornography), **168–169**
- Disclosure(s), **169–174**; anonymous, 173; of association membership records, 346; of birth parent identity in adoptions, 7; of cellular phone conversations, 47; compelled, of tangible records, 234, 235, 359; in a confessional culture, **116–117**; confidentiality and, 117; court mandated, 118; of DNA information, 176–177; of education records, 221–222; of financial records, 39, 170–171, 229; freedom of association and, 236; by government, 170; of health information, 22, 111, 119, 268–269, 364; of information about criminal suspects and arrestees, 143, 146–148; knowing exposure doctrine, 196; leaks, 173, 410, 413; of library records, 328, 399; litigation and, 170, 171–172; non-content information, 197; open meetings laws, **362–363**; permissible, United States Postal Service, 573; of personal information, statutes protecting, 169, 350; Privacy Act of 1974, access provisions of, 170, 174; of private facts, 73, 311, 314–315, 394, 398, 429–430, 431–432, 467; protective orders, 171; public records, 134, 170–171; rape victim identity, 134–135, 314; and sexual violence, 506, 613–614; sources of, 170; of trade secrets, 48; video rental and purchase records, 595; voluntary self-disclosure, 394; whistleblowers, 170, 173
- Disclosure veto system, 7, 10
- Discrimination: based on genetic information and testing, 254–255, 378; gays, U.S. military, 179; gender, 18, 55, 499; racial, 332
- Disk wiping, 113
- DNA Analysis Backlog Elimination Act of 2000, 489
- DNA and DNA banking, **174–177**, 536; in the Clinton-Lewinsky scandal, 100; Common Rule, 177; defined, 174; destruction of specimens, 175; disclosures about, 175–177; “dragnets,” 162; FBI cataloging system for (CODIS), 498; and fingerprints compared, 231; genetic information and testing, 176; for identification purposes, 175; sex offenders, 498; testing, of arrestees, 146; unauthorized testing, 176
- Does v. State* (adoption records), 11, 12
- Doe v. Commonwealth’s Attorney* (consensual homosexual acts), 66
- Doe v. Poritz* (sex offender registries), 495
- Doe v. Sundquist* (adoption records), 11
- Domain Name Registrar, 304
- Domain name server (DNS), 114
- Domain Name System (DNS), 309
- Domestic terrorism, 227–228, 584, 587–588
- Domestic violence, 218–219, 275, 349, 397, 401, 411
- Do-Not-Call Registry (DNCR), **177–178**, 364, **399**, **553**
- “Don’t ask, don’t tell” policy **178–181**
- Doubleclick, 307
- Doublethink, 51
- Douglas, Kirk, 284
- Douglas, William O., 126, **181–183**; appointment to Supreme Court, 181; confidentiality of married relationships, 265; *Griswold v. Connecticut*, 182, 250, 263, 479, 623; on home, 278; penumbral rights, 126, 182, 263, 265; *The Right of the People*, 182; *Roe v. Wade*, 183; *Skinner v. Oklahoma*, 262; *United States v. Caldwell*, 575; *Village of Bella Terre v. Borass*, 596; *Warden v. Hayden*, 602
- Dow Chemical Co. v. United States* (aerial surveillance), 319, 457, 579
- Drinking age, 512
- Driver’s licenses: bar codes on, 45; fingerprints on, 232
- Driver’s Privacy Protection Act (DPPA) of 1994, 4, **183–184**
- Driving under the influence (DUI), 61
- “Droopy drawers,” 335

- Drudge, Matt, 100
- Drug and Alcohol Testing Industry Association, 589
- Drug Enforcement Agency (DEA), 581
- Drug-Free Workplace Act of 1988, 186
- Drugs, decriminalization of, 16
- Drug testing, **185–189**, 536, 588;
challenges to, 186–187;
confidentiality and, 273; federal employees, 186; methods of, 185; in the military, 185; post-accident, 188, 508–509, 590; pre-employment, 187, 188, 590; of pregnant women, 411; of prisoners, 185–186; random, 98, 186, 188, 590; for reasonable cause, 188; rehabilitation, 188; unrelated to law enforcement, 123; in the workplace, 98, 186, 188, 619
- DSA algorithm, 167
- Due Process clause, Fourteenth Amendment, 126–127, 129, 165, 179, 261–262, 263, 265, 324, 325, 330, 346, 396, 461, 463, 471, 479
- Dumpster diving, 243, 245, 246
- Dworkin, Ronald, 326
- East Asian Tigers, 292
- Eastman, Crystal, 16
- e-commerce: biometrics applications for, 54; and the cashless society, 165; privacy notices and, 427; verification, challenges to, 137; websites, 304, 306
- Economic Espionage Act of 1996 (EEA), 246, 292
- Economics of Privacy* website, 626
- Education records, disclosure of, 221–222
- Education, U.S. Department of, 384, 512
- Edwards v. Aguillard* (science education), 16
- Egg donors, anonymity of, 22
- Eighteenth Amendment, Prohibition, 86
- Eighth Amendment, Cruel and Unusual Punishment clause, 390, 392
- Eisenhower, President Dwight D., 225, 338
- Eisenstadt v. Baird* (contraception, unmarried couples), 2, 17, 60, 66, **191–192**, 219, 250, 265, 278, 374, 613
- Elder abuse, 37
- Electromagnetic laser scanner, 45
- Electronic communication service (ECS), 196
- Electronic Communication Privacy Act (ECPA) of 1986, 20, 78, 180, **192–198**, 205, 400; communications covered by, 193; domestic spying, 402; e-mail and, 200; exclusionary rule, 195–196; FBI violation of, 419; and government access to Internet communication, 302–303, 304; necessity/exhaustion requirement, 194–195; pen registers, use of, 197–198, **381–383**, 586; probable cause and, 194, 382; protections provided by, 610–611; and Stored Communications Act (SCA) compared, 196; subtitles of, 192; videotape surveillance, 545; warrants, need for, 196–197; wiretapping and, 193, 617–618
- Electronic eavesdropping: cellular telephones, potential for, 88, 312; criticisms of, 350; methods of, 312; as a search, 123
- Electronic Freedom of Information Act Amendments (EFOIA), 453
- Electronic Frontier Foundation (EFF), 419, 627
- Electronic mail (e-mail), **198–201**, 298;
address, as personally identifiable information, 17, 77, 199, 383; child's address, protection of, 94; defined, 198; file attachments, 199; forwarding, 199; gossip conveyed by, 259; and installation of keystroke logs, 320; interception of, 312; laws protecting the privacy of, 200–201; loss of privacy and, 393; monitoring of, 193, 198, 393, 584, 610, 618; opt-out mandate, 364; password protection, 373; protocol for sending, 198–199; replying to, 199–200; spam, 158, 166, 307, 383, **520–522**; storage and archiving of, 111, 125, 201; wiretapping and, 19, 20, 49, 180
- Electronic Privacy Information Center (EPIC), 75, 419, 420, 476, 546–547
- Electronic surveillance, 192, **201–206**, 360, 481; defined, 202; Foreign Intelligence Surveillance Act of



- 1978 (FISA), 205, **234–235**, 350, 401, 585, 586–587; necessity/exhaustion requirement, 194–195; privacy implications of, 420; statutes regulating, 610; USA PATRIOT Act and, 206; wiretapping, 12, 19–21, 47, 72, 73–74, 89–90, 102, 104–105, 132, 144, 193–196, 202
- Electronic toll collection, **206–207**
- Elkins v. United States* (silver platter doctrine), 507
- Elrod v. Burns* (freedom of association), 237
- Elshtain, Jean Bethke, 404
- Employee Polygraph Protection Act of 1988, 617, 619
- Employee Retirement Income Security Act of 1974 (ERISA), 255
- Employees: background checks of, 37–38; blood testing, 37; CIA monitoring of, 93; civil service, 97–99; criminal conviction and denial of employment, 38; drug testing, 616, 619; e-mail, monitoring of, 308, 393, 610, 618; institutionalized discrimination against, U.S. military, 179; invasion of privacy, claims of, 618–619; off-duty conduct, 619; relationships with employers, confidentiality in, 119; sexual harassment of, 499–500; theft by, 37; urine analysis, 37; workplace privacy, **615–620**; work-related searches, 353–355
- Employment identity theft, 289
- Encryption systems, 152. *See also* Cryptography
- Engel v. Vitale* (school prayer), 16
- Enlightenment, 53
- Entick v. Carrington and Three Other King's Messengers* (seizure of personal papers), 69
- Enzyme immunoassay, 589
- Enzyme-Linked Immunosorbent Assay (ELISA), 62, 185
- Enzyme-Multiplied Immunoassay Technique (EMIT), 185
- Equal Employment Opportunity Commission, 38
- Equal Protection clause, Fourteenth Amendment, 165, 192, 330, 331, 461
- Escrowed Encryption Standard (EES), 101–103
- Eskridge, William, 516
- Ethereal software, 86
- EtherPeek software, 86
- Ethertest software, 86
- Ethics in Government Act of 1978, 170, 171
- Eugenics, 464, 527, 529
- European Convention on Human Rights, 66
- European Court of Human Rights (ECHR), 66
- European Data Protection Directive, 41, **207–210**, 303, 395, 543, 555
- European Union, 399: Charter of Fundamental Rights, 303; Safe Harbor Principles, 364, **475–476**
- Exclusionary rule, searches, 31, 123–124, 507, 607
- Executive Order 9397, Social Security numbers, 513
- Executive Order 11905, assassination of foreign leaders, 488
- Executive Order 12333, assassination of foreign leaders, 488
- Executive Order 12564, drug-free federal workplace, 186, 590
- Executive privilege, 443
- Exigent circumstances, search warrants, 123, 145, 379–380, 481
- Ex parte Jackson* (search, sealed letters), 358
- External constituency surveillance, 538
- Factual Analysis Criminal Threat Solution (FACTS), 342
- Fair and Accurate Credit Transaction Act, 137, 291
- Fair Credit Reporting Act (FCRA), 38, 39, 42, 119, 137, 141, 142, 169, **211–214**; credit information, sharing of, 213–214; errors, correcting, 212–213; identity fraud, 214, 291; landlord access to tenants' credit history, 322–323; maximum possible accuracy and, 211–212
- Fair housing laws, 322, 323
- Fair information practices (FIPs), **214–217**, 398–399, 414; concept of mutuality, 215; defined, 214; opt-in vs. opt-out, 41, 137, **363–364**, 427; Organization

- of Economic Cooperation and Development (OCED) principles for, 215–216; in Privacy Act of 1974, 215, 273, 328; privacy notices, 427
- Fair Isaac Corporation (FICO), 141, 142
- False claims laws, 173
- False flag operation, 92
- False light privacy tort, 73, 311, 312–314, 394, 398, 430, 432
- False Statements Act, 475
- Falwell, Rev. Jerry, 314
- Family, **217–221**, 401; adoptive, protection of, 8–9; best interest of the child test, 217; child custody, 217; cohabitation agreements, 217; cult of domesticity, 248–249; freedom of intimate association, 239–240; government intrusion into, 21, 149; marital privacy, 17, 182, 218–219; prenuptial agreements, 217; relationships in *Nineteen Eighty-Four*, 52; separation agreements, 217; sexual harassment, reporting, 503; surveillance of, 538; and women's equality movement, 248
- Family Educational Rights and Privacy Act (FERPA), 49–50, **221–223**, 273, 328, **384**, 398, 403, 460
- Family planning: counseling, 375; public acceptance of, 59, 263–264, 623. *See also* Birth control
- Family values, decline of, 2
- Farm Equipment Workers International, 604
- Fayed, Dodi, 368
- Federal Assistance Suicide Funding Restriction Act of 1997, 603
- Federal Aviation Administration (FAA), 14, 186
- Federal Bureau of Investigation (FBI), **223–228**, 488; blind memoranda, 226, 281; Carnivore software, **84–86**, 200, 302, 308, 382, 609; and cellular telephones, determining the location of, 90; Combined DNA Index System (CODIS), 498; computer fraud, investigation of, 109; Counter Intelligence Program (COINTELPRO), **132–134**, 225, 280; covert practices, privacy threats posed by, 226–227; creation of, 223; DCS1000 software, 84–85, 200, 382, 600; discrediting of Martin Luther King Jr., 227; domestic terrorism, investigation of, 227–228; e-mail, scanning of, 200; fingerprint repository, 232, 347; information control, 281; informers, within the Communist Party, 132; intelligence investigations by, 224; J. Edgar Hoover, 133, 224, **279–282**, 337; Mass Media program, 280; MATRIX program, guidelines for enforcing, 343; National Crime Information Center, 224, **346–347**; obscenity file, 280; records maintained by, 225; searches without probable cause, 224, 419; secrecy, 482; Sex Deviate program, 225–226, 280; surveillance authority, 86, 224, 281; in Watergate scandal, 92, 281; wiretapping by, 104, 132, 224
- Federal Communications Commission (FCC), 105, 177, 204, 306
- Federal Highway Administration, 186
- The Federalist Papers*, 18
- Federal Railroad Administration, 186, 508
- Federal Reserve Board, 229
- Federal Rules of Evidence, 501
- Federal Theater Project (FTP), 283
- Federal Trade Commission (FTC), 177, 212, 246, 290, 364, 399, 427, 521; *Privacy Initiatives* website, 626
- Feeding tube, removal of, 149, 150
- Feingold, Sen. Russ, 369
- Fellini, Federico, 367
- Feminist movement, 2, 101, 250, 276, 400
- Ferguson v. City of Charleston* (urine testing), 591
- Fertility, treatment for, 21
- Fetal privacy, 22, 464
- FICO score, 141
- FidoNet, 381
- Fifth Amendment, protection against self-incrimination, 396; blood testing and, 61; documents, disclosure of, 124; drug-testing and, 187; fingerprinting, 231; forced confessions, 124; informational privacy as theory behind, 121; origins of, 69, 122; remedies for



- violations of, 124; seizure of personal papers, 67–72, 74, 124, 154, 261
- File-sharing services, 203, 304, 305, 306
- File Transfer Protocol (FTP), 485
- Film industry, investigation of, 284
- Financial Crimes Enforcement Network (FinCEN), 43, 44
- Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act), 39, 40–42, 119, **229–230**, 400; Financial Privacy Rule, 229; hacking, security against, 41; opt-in/opt-out rights, 41, 364; and personally identifiable information, 385; privacy notices, 428; privacy protections, exemptions from, 42; Safeguards Rule, 229; sharing of customer information, limits on, 40–41, 137
- Fingerprints and fingerprinting, 54, 107, **230–232**, 341, 347, 415; of air travelers, 15; of arrestees, 145, 498; in bar codes, 45; *Davis v. Mississippi*, **161–162**; and polygraph tests compared, 581; primary uses, 231; scanning, for ATM use, 28
- Finger v. Omni Publications International Ltd.* (appropriation of name or likeness), 433
- First Amendment: Brandeis defense of, 74; protections, limits on, 25; religion clause, 125; right to free speech under, 4, 135, 147
- Fisher, Florence, 9
- Fiske, Robert Jr., 99
- Flanagan, Hallie, 283
- FLIR (forward-looking infrared radar). *See* Thermal sensor imaging
- Florida Department of Law Enforcement (FDLE), 342
- Florida Star v. B. J. F.* (public disclosure of private facts), 314, 432
- Florida Sunshine in Litigation Act, 171–172
- Florida v. Bostick* (surveillance, bus station), **232–234**, 531
- Florida v. Boyner* (random searches), 233
- Florida v. Riley* (aerial surveillance), 155, 457
- Fluorescence polarization immunoassay, 589
- Flynn, Larry, 314
- Fonda, Henry, 230
- Ford, President Gerald, 314, 488
- Foreign Intelligence Surveillance Act of 1978 (FISA), 205, **234–235**, 350, 401, 481, 585, 586–587
- Foreign Intelligence Surveillance Court (FISC), 234, 587
- Foreign shell banks, 44
- Forensic video analysis, 546–547
- Foucault, Michel, 116, 421, 516
- Fourteenth Amendment, 219; Due Process clause, 126–127, 129, 165, 179, 261–262, 263, 324, 325, 330, 346, 396, 461, 463, 471, 479; Equal Protection clause, 165, 192, 330, 331, 461; Privileges and Immunity clause, 127–128
- Fourth Amendment, protection against unreasonable search and seizure, 396, 479; aerial observation and, 81; distinction between home/structure and vehicle/ship, 87; exclusionary rule, 123; home in, 121; limited application of, 122; mere evidence rule, 71, **339–342**; origins of, 121–122; pen register devices, 382; as protection for informational privacy, 120; random searches, 233; remedies for violations of, 123; subpoenas and, 70
- France, Anatole, 424
- Frankfurter, Justice Felix, 507
- Franklin, Benjamin, 162
- Frank W. Winne & Son, Inc. v. Palmer* (industrial espionage), 246
- Fraud: at bank ATMs, 29; computer, 107–109; detection, 159; employee, 37
- Fraud alerts, 214
- Freedom of Access to Clinic Entrances Act, 4
- Freedom of association, **235–240**, 396; *Abood v. Detroit Board of Education*, 237; anonymity in, 18, 125; *Board of Directors of Rotary International v. Rotary Club of Duarte*, 238; *Boy Scouts of America v. Dale*, 238–239; *Bronti v. Finkel*, 237; *Communist*

- Party of the United States v. Subversive Activities Control Board*, 132, 236; *Cousins v. Wigoda*, 237–238; disclosure requirements, 236; *Elrod v. Burns*, 237; *Healey v. James*, 236; House Un-American Activities Committee (HUAC) threats to, 283–285, 336; intimate, protections for, 239–240; *Keller v. State Bar of California*, 237; *Kusper v. Pontikes*, 237; McCarthyism, **336–339**; membership requirements, 236, 237; *NAACP v. Alabama*, 125, 236, **345–346**; political parties, membership in, 237–238; *Roberts v. United States Jaycees*, 238; *Shelton v. Tucker*, 236
- Freedom of Information Act (FOIA), 118, **240–242**, 400; as citizen surveillance of government, 539; enactment of, 240; exemptions to, 147–148, 240, 242, 415, 452; FBI records released under, 227; fees, 241; implications of for personal privacy, 241–242; “information of a personal nature,” 362–363; origins of, 281; passage of, 451–452; requests, 133, 241, 423; requirements under, 240–241; tax records, sharing of, 295
- Freedom of intimate association, 239–240
- Freedom of movement, expectation of, 122
- Frequent shopper cards, 159, 565
- Friedan, Betty, 250, 277
- Fried, Charles, 407, 409
- Fried, Marlene Gerber, 2
- Frozen embryos, 23
- Fruit of the poisonous tree doctrine, 233, 293–294
- Fundraising, 159
- Galton, Francis, 230
- Garbage, 195, **243–247**; abandonment doctrine, 244–245; *California v. Greenwood* (garbage at curb), 155–156, 244, 458, 560, 580; co-mingled, 247; dumpster diving, 243, 245, 246; industrial espionage, 245–246; personally identifiable information obtained from, 290; public trash vs. private trash, 245; reasonable expectation of privacy and, 244, 247; shredded documents, seizure of, 245; *State v. Roland*, 247
- Garbology, 243
- Galella, Ron, 367
- Gas Chromatography/Mass Spectrometry (GC/MS), 185, 589
- Gates, Gerald W., 570
- Gavison, Ruth, 407, 410
- Gender, **247–252**, 395; Census Bureau statistics, 569; cross-gender searches, 391; cult of domesticity, 248–249; discrimination, 18, 55; feminist movement, 2, 101, 251; “personal is political,” 247, 251, 277, 400, 436; privacy issues unique to, 411, 613; reproductive rights, **462–465**; separate spheres doctrine, 249–250; sexual harassment, 247–248, 401, 411, **499–504**, 614; sexual misconduct, 249; sexual norms, 334; Supreme Court rulings about, 250–251; women’s rights movement, 248, 250
- Genealogical research, 57
- General warrants, 69, 479
- Genetic exceptionalism, 231, 254, 256
- Genetic information and testing, 176, **252–256**; confidentiality of, 616; disclosure of in assisted reproductive technologies, 22; discrimination based on, 254–255, 378; of DNA samples, 176, 252; government and, 254; paternity, determination of, 252; patient privacy, 378–379; for predisposition to genetic diseases, 252, 253–254; written consent for, 255
- Genetic Information Nondiscrimination Act of 2006, 63, 254
- Genetic inheritance, 9
- Geneva Convention, 93
- Genocide, 395
- Geographic information systems (GIS), 258
- Gerety, Thomas, 409
- Gerstein, Richard, 409
- Gideon v. Wainwright* (right to counsel), 16



- Gilbert, Ben, 226
Gilbert v. California (handwriting exemplars), 70
 Gilligan, Carol, 615
 Gilman, Charlotte Perkins, 275–276, 278
 Gilmore, John, 419
 Givens, Beth, 420
 Glass-Steagall Act of 1933, 40, 229
 Globally Unique Identifier (GUID), 301
 Global positioning system (GPS), 90, 93, 203, **256–259**, 306, 462
 GMail, 201, 305
 Goffman, Erving, 5, 333
 Goldberg, Justice Arthur, 263
 Goldwater, Sen. Barry, 179
 Gonorrhea, 62
Goodridge et al. v. Department of Public Health (same-sex marriage), 218
 Gossip, 48, **259–261**, 466, **600**; FBI information gleaned from, 280–281; manners and, 260; social roles associated with, 259–260
 Gostin, Lawrence O., 446
Gouled v. United States (mere evidence rule), 339–340
 Government in the Sunshine Acts, 362
 Gramm-Leach Bliley Act (GLBA). *See* Financial Services Modernization Act of 1999
 Grand Jury proceedings, secrecy of, 147
 Great Depression, 40, 229, 283
 Greater good argument, blood testing, 61–62
Griswold v. Connecticut (contraception, married couples), 2, 131, 165, 218, **261–266**, 374, 396, 462, 613; ACLU involvement in, 17; as individual autonomy issue, 126, 532; as marital privacy, 278, 325, 436, 527; patient rights and, 377; as precedent, 65–66, 191, 361; William O. Douglas on, 182, 250, 263, 479, 623
 Griswold, Estelle, 59, 262
 Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations, 343
 Hacking: of banking and financial records, 41; for credit card numbers, 289; criminalization of, 107; use of by private investigators, 435; vulnerability to, 381
Hale v. Henkel (search and seizure, subpoenas), 70
Hamberger v. Eastman (intrusion upon seclusion), 430
 Handwriting exemplars, 70, 341
 Hannegan, Robert, 181
 Harassment: of abortion doctors, 184; anti-gay in the military, 180; based on sexual orientation, 180, 502; sexual, 247–248, 324, 353, 411, **499–504**, 505, 614; surveillance as, 408; tenants by landlords, 321, 324; use of DMV records for, 184
Harkey v. Abate (voyeurism), 614
 Harlan, Justice John, 74, 263, 277, 346, 361
 Harm principle, 405
 Harms/benefits ratio, 286
Harris v. McRae (government assistance for abortion), 251
Harris v. Thigpen (HIV testing of prisoners), 392
Harris v. United States (plain view doctrine), 96, **267–268**, 386–387, 457, 601
 Hart, H. L. A., 326
 Hart, John, 182
 Hash, 167
 Hatch, Sen. Orrin, 369
 Haury, Emil, 243
 Health and Human Services, U.S. Department of, 56, 445
 Health, Education, and Welfare (HEW), U.S. Department of: and adoption law, 9; fair information practices, recommendation for, 414; Project Match, 109
 Health fraud, 271
 Health Information Portability and Accountability Act of 1996 (HIPAA), **268–269**, 377, 384, 400; built-in exceptions to privacy rules of, 63; and confidentiality of patient data, 22, 111, 119, 375; and discrimination based on genetic information, 256; patient consent, 377; privacy notices, 428; Privacy Rule, 256, 269, 274, 364, 445;

- protected health information (PIH), 445
- Health maintenance organizations (HMOs), 118
- Health privacy, **270–274**; abortions, 4–6; genetic information, 271; Health Information Portability and Accountability Act (HIPAA), 11, 22, 119, **268–269**, 273–274, 364; patient records, need for access to, 271; patient rights, **376–379**; personally identifiable information and, 384–385; physician-patient privilege, 270, 375, 439, 442–443; public health surveillance, 271; student records, 273; Supreme Court decisions re:, 271–272; and third-party payment, 271; trafficking in patient information, 271
- Health Privacy Project, 626
- Healy v. James* (freedom of association), 236
- Hearsay, 259
- Hellman, Martin, 166
- Henke v. Commerce* (system of records), 415
- Hennings, Thomas, 337
- Henry, Edward, 230
- Hester v. United States* (open fields doctrine), 154–155, 356
- Hübel v. Sixth Judicial District* (disclosure of personal identity), 75
- Hijackings, 14
- Hill family, James J., 313
- HIPAA. *See* Health Information Portability and Accountability Act of 1996 (HIPAA)
- Hippocratic Oath, 118, 377
- Hirabayashi v. United States* (wartime internment), 16
- Hirsch v. S. C. Johnson & Son, Inc.* (appropriation of name or likeness), 432
- Hiss, Alger, 283
- The History of Sexuality*, 116
- HIV. *See* Human immunodeficiency virus (HIV)
- Hodge, James G., Jr., 446
- Hodgson v. Minnesota* (abortion, spousal consent), 264
- Hoffa v. United States* (private information from third parties), 318
- Hoffman, Abbie, 284
- Hollywood Ten, 284
- Holmes, Justice Oliver Wendall, 623
- Holmes v. Curtis Publishing Co.* (false light), 432
- Holt v. United States* (incriminating testimonial communication), 70
- Home, **274–279**; aerial surveillance of, 81; constitutional amendments protecting, 263; cult of domesticity, 248–249, 275; curtilage, **153–156**; domestic violence, 218–219, 275, 349, 397, 401, 411; fingerprint scanners for, 232; idealized images of, 275–276, 277; inviolability of, 74, 121, 168, 182, 243, 275, 370, 393, 480; Louis Brandeis on, 275, 278; mail-order houses, 276–277; mere evidence rule, **339–342**, 602; personal papers, search of, 67–72, 74, 124, 154, 261; pornography in, 66, 365, 396, 412; prisoner’s cell as, 286; “sanctity of the domestic circle,” 278; search and seizure, plain view doctrine, 386, 457, 578; sex offenders and, 499; women’s liberation movement and, 277–278; zone of privacy, 219, 278, 462, 623
- Homeland Security, U.S. Department of, 15, 106, 215, 342, 349
- Homeless persons, 422
- Homophobia, 280
- Homosexual activity: Boy Scouts and, 238–239; between consenting adults, 64–67, 128, 130, 265, 397, 516–517; “don’t ask, don’t tell” policy, **178–181**; security risk and, 226; as unenumerated right, 126
- Hoover, J. Edgar, 133, 224, **279–282**, 337
- Horsley, Neal, 4
- Horton v. California* (plain view doctrine), 387
- Hostile environment sexual harassment, 500, 502
- Hotmail, 201
- House Un-American Activities Committee (HUAC), 225, **282–285**, 336, 604
- Howard, Sen. Jacob, 127
- Hudson, Rock, 226



- Hudson v. Michigan* (searches, exclusionary rule), 123, 145
- Hudson v. Palmer* (searches, prison cells), **285–286**, 391
- Hufstедler, Judge Shirley, 312
- Human immunodeficiency virus (HIV)
testing: in assisted reproductive technologies, 23; blood bank testing for, 62–63; mandatory testing, 63; partner notification, **371–373**; in premarital testing, 63; prenatal, 63; prisoners, 391–392; results, disclosure of, 63, 272
- Human subjects protections, **286–288**;
anonymity in, 288; harms/benefits ratio, 286–287; informed consent, 286, 287; legal cases surrounding, 288; Tuskegee Institute syphilis study, 287
- Humphrey, Laud, 287
- Huntington's Disease, 378
- Hustler* magazine, 314
- Hustler v. Falwell* (celebrity parodies), 315
- Hyde Amendment, 463
- Hypertext Transfer Protocol (HTTP), 485
- ICANN (International Corporation for Assigned Names and Numbers), 304, 609
- Identity fraud, **289–292**, 295, 394; account takeover, 289; application fraud, 289; birth certificates and, 57; civil liberties and, 402; computers, role of, 39; consumer databases, security breaches of, 137; credit cards and, 135, 137–138; data brokers and, 158; digital cash and, 166; dumpster diving and, 243, 246; Internet and, 289, 298, 300, 308–309; and personally identifiable information, 384; recent increase in, 290; statutes to address, 214, 229
- IKONOS satellite, 14
- Illinois v. Gates* (searches, workplace), 481
- Immigration violations, 147–148
- Impeachment, President Clinton, 99, 100
- In a Different Voice*, 615
- Inalienable human rights, 162
- Indenture contracts, 7
- Individual autonomy: abortion decisions and, 120; constitutional protections for, 125–131; and doctrine of unenumerated rights, 126, 127–131; Due Process clause, Fourteenth Amendment, 126–127, 129, 165, 179, 261–262, 263, 265, 324, 325, 330, 346, 396, 461, 463, 471, 479; penumbral rights, 126, 182, 263, 265, 396; and principle of government noninterference, 125–126; Privileges and Immunity clause, Fourteenth Amendment, 127–128
- Individuals with Disabilities Education Act (IDEA), 222
- Industrial espionage, 245–246, **292–293**, 434, 482, 538
- Inevitable discovery, **293–294**
- Infant mortality, 56, 62
- Informational privacy, 394; collection of information, restrictions on, 121; constitutional protections for, 120–125; enforcement of, 395; Fourth Amendment as protection for, 120; *Griswold v. Connecticut* and, 264; and national security, 124–125, 395, 401; self-directed, 18, 394
- Information control, 281, 410, 422, 424
- In re Buzzanca* (child custody), 23
- In re Grand Jury Proceedings* (telegraph privacy), 318
- In re Harris* (seizure, personal papers), 71
- In re Quinlan* (right to die), 397, 467
- Instant Messaging (IM), 198, 298, 304, 306
- Insulation from observability, 422
- Intellectual property rights, 292, 381
- Intelligence Activities and the Right of Americans*, 488
- Intel v. Hamidi* (spam), 521
- Intermediate scrutiny standard, content-neutral laws, 47
- Internal Revenue Code, 295
- Internal Revenue Service (IRS), **294–296**, 488; accountant-client privilege, 443; collection agency outsourcing, 295; Currency Transaction Report, 40, 43; and personally identifiable information, protection of, 295; Privacy Impact Assessment, 295
- Internal Security Act of 1950, **292–297**, 337

- Internal Security Committee, 284
- International Coalition of Library Consortia (ICOLC), 329
- International Data Encryption Algorithm (IDEA), 389
- International Federation of Library Associations and Institutions (IFLA), Statement on Libraries and Intellectual Freedom, 328
- International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, 44
- Internet, **297–310**; abortion providers, posting names of, 4; account, access by third parties, 115; ads on, 203, 246, 554; and anonymity, loss of, 18, 125; browsers, 300, 304; and cable access combined, 78; cached data, 114, 299; censorship, ACLU challenges to, 17; chats, 203; Children's Online Privacy Protection Act of 1998 (COPPA), **94–95**, 303, 364, 399, 403; clickstream data, 304; communications, law enforcement access to, 105; cookies, 94, 305, 307, 309, 536; copyright infringement, 301; court records, access to, 172; credit card transactions, 307, 308; data brokers, use of, 301; defined, 297; dial-up access, 308; digital rights management, 301; digital signatures, 166; domain name registration, 304–305, 309; e-commerce websites, 304, 306; effect of on Foreign Intelligence Surveillance Act, 587; employee communication, monitoring of, 308; and exchange of aerial image data, 14; file-sharing services, 203, 304, 305, 306; free software available on, 308; government access to communications on, 302–303; high-speed connections, 28; identity fraud and, 289, 298, 300, 308–309; industrial espionage and, 293; investigative consumer checks, 323; keystroke loggers, 86, 203, 308, **320**; law enforcement access to personal data, 303; manners in using, 334; opt-in vs. opt-out, 364; origins of, 257, 297; packet-sniffing software, 84, 308; passwords, 307, 308, 309; peer-to-peer (P2P) technologies, 305, 306, **380–381**; pharming, 309; phishing, 309; pornography on, 105, 305; Pretty Good Privacy (PGP) program, adoption of, 389; privacy, influence of on, 299–303; privacy seal programs, 302; protocols for easy access to, 102; search engines, 158, 299, 303, 305, 308; searches, as library records, 329; service providers (ISPs), 304; sexual offenders, websites listing, 497; spam, 158, 166, 307, 383, **520–522**; spyware, 114, 303, 306, 308–309, 381, 567; stored records, access to, 196; as surveillance technology, 298; technologies used to capture and access user information, 303–309; telephony, 303, 304, 305, 306; third-party doctrine and, 458; transparency, lack of, 299, 309; unsecured broadband connection, 114; and USA PATRIOT Act, 586; use, CIA monitoring of, 93; user profiles, 306; web bugs, 307, 308, 309; web hosting, 304; WHOIS database, 304, **608–609**
- Internet Engineering Task Force, 389, 485
- Internet Message Access Protocol (IMAP), 198
- Internet Protocol (IP) address, 198, 202, 305, 383
- Interracial marriage, 330, 396, 412
- Intimacy, 409–410, 615
- Intracytoplasmic sperm injection (ICSI), 21, 23
- Intrusion upon seclusion privacy tort, 73, 311, 312–313, 394, 398, 429, 430–431, 492, 566
- Invention assignment agreement, 119
- Inventory searches, 35
- Investigative consumer reports, 323
- Inviolate personality, right of, 397, 409
- In vitro fertilization, 21
- Jackson, Reverend Jesse, 400
- Jacob Wetterling Crime Against Children and Sexually Violent Offender Registration Act of 1994, 494, 497
- Jaffe v. Redmond* (health privacy), 272



- Janis v. United States* (silver platter doctrine), 508
- Jefferson, Thomas, 162
- Johnson, President Lyndon B., 59, 226, 240
- Jones, Paula, 99
- Joplin, Janis, 314
- Journalism, **311–315**; ambush-type, 393; confidentiality in, 117, 147; investigative reporting, 312; libel law and, 26; newsworthiness as a defense, 314, 431; paparazzi, 312, **367–369**, 426; privacy vs. public's right to know, 288; reporter's privilege, 442, 574–575; sexual misconduct, reporting on, 249; use of remote sensing in, 13; yellow, 430. *See also* Media
- Judicial Conference of the United States, 172
- Judicial legislation, 127, 128
- Judiciary Act of 1789, 69
- Junk Fax Prevention Act of 2003, 554
- Junk mail, 137, 166, 563
- Jurisprudence and Gender*, 615
- Justice, U. S. Department of, 342, 512
- Juvenile delinquency, 224
- Kapor, Mitchell, 419
- Kass v. Kass* (child custody), 23
- Katz v. United States* (reasonable expectation of privacy), 32, 70, 74, 244, **317–319**, 327, 355, 361, 396, 456, 480, 490–491, 579, 610
- Keller v. State Bar of California* (freedom of association), 237
- Kennedy, Justice Anthony, 186, 325, 580, 624
- Kennedy, President John F., 225, 280, 367
- Kerberos tickets, 27
- Kerchoffs, Auguste, 152
- Kerry, Sen. John, 225
- Ker v. California* (search, plain view doctrine), 386
- Key-escrow system, 101
- Keystroke loggers, 86, 203, 308, **320**
- KGB, 92
- King, Martin Luther Jr., 227, 280, 282, 314
- Kirby, Michael, 217
- Kissinger, Henry, 246
- K-Mart Corp. v. Trotti* (intrusion upon seclusion), 430
- Knowing exposure doctrine, 196
- Korean War, 336–337
- Ku Klux Klan, 133, 282
- Kusper v. Pontikes* (freedom of association), 237
- Labor unions, Communist infiltration by, 282, 283, 604–605
- La Dolce Vita*, 367
- Lake v. Wal-Mart* (privacy tort), 73
- Landlord and tenant, **321–324**; adverse action reports, 324; background checks, 321, 323; covenant of enjoyment, 321, 324; credit history, access to, 322–323; fair housing laws, 322, 323; harassment, 321, 324; right to be let alone, 321
- Landsat system, 14
- Law Enforcement Access Field (LEAF), 102
- Lawrence v. Texas* (consensual homosexual acts), 67, 128, 130, 165, 179, 181, 183, 219, 265, 278, **324–327**, 397, 437, 506, 516, 624
- Leaks, 173, 410, 413
- Lee, Richard Henry, 162
- Levi, Edward, 227
- Lewinsky, Monica, 99. *See also* Clinton-Lewinsky scandal
- Lewis v. LeGrow* (video voyeurism), 614–615
- Liability, government officials, 124
- Libel law, 24–26, 69
- Library records, 161, **327–330**, 399; confidentiality of, 327; disclosure of, 328; USA PATRIOT Act requirements re., 327, 328, 329
- Life support, removal of, 150
- Lifton, Betty Jean, 9
- Lincoln, Abraham, 164
- Lisagor, Peter, 226
- Livingston, Robert R., 162
- Lobbying, 16
- Locational data, 203
- Locational privacy, 90
- Location-based services (LBS), 258
- Lochner v. New York* (workplace autonomy), 129, 261–262
- Locke, John, 162, 405
- Loving v. Virginia* (choice of marital partner), 130, 218, **330–332**, 396

- Loyalty Review Board (LRB), 338
 Luker, Kristin, 2
Lustig v. United States (silver platter doctrine), 507
 Lyons, Ricky, 581
- MacKinnon, Catherine, 248, 411
 Madonna, 437
Madsen v. Women's Health Center (abortion clinics), 4
 Magic Lantern software, 86, 320
 Mail-order homes, 276
 Magnetometers, 15
 Malware, 203, 308
 Mann, Steve, 423
 Mann Act. *See* White Slave Traffic Act
 Manners, 116, 260, **333–335**, 542
Manola v. Stevens (privacy, celebrity), 397
Mapp v. Ohio (automobile searches, exclusionary rule), 31, 481
 Marriage: bigamy/polygamy, 218; Defense of Marriage Act, 131; interracial, 330, 396; partner, choice of, 130, 218, 330–332; privacy within, 17, 182, 218–219; privilege within, 441; rape in, 411; same-sex, 131, 218, 325; sexual violence within, 504; spousal violence, 218–219
 Marshall, George, 337
 Marshall, Justice Thurgood, 519
Maryland v. Buie (search, plain view doctrine) 386, 559
Maryland v. Pringle (automobile searches, passengers), 35
 Marx, Karl, 421
 Matching programs, computers, 109–110
 MATRIX program. *See* Multi-State Anti-Terrorism Information Exchange Program (MATRIX)
 Matters of public concern, 49
 McCarran Act of 1950, 132
 McCarthy, Sen. Joseph, 225, 226, 282, 336, 612
 McCarthy-Army hearings, 338
 McCarthyism, **336–339**. *See also* House Un-American Activities Committee (HUAC)
McCormick v. England (breach of confidentiality), 433
 McDougal, James and Susan, 99
- McMahon, Brion, 337
 McVeigh, Timothy, 30
McVeigh v. Cohen (gays in the military), 180, 200
 Mead, Margaret, 404
 Media: alternative and nontraditional, 101; celebrities, privacy rights of, 313–314, 367–369, 425–426; daytime television talk shows, 116; deceased celebrities, privacy rights of, 314; FBI investigations into activities of, 226; First Amendment rights of, 313; Freedom of Information Act requests, 133; intentional infliction of mental injury, 314; libel law, 26; McCarthy hearings, 337, 338; political cartoons, 315; role of in maintaining and sustaining confessional culture, 116; talk radio, 101
 Medical ethics, 118
 Medical records, confidentiality of, 63, 111, 118–119
 Megan's Law, 494, 497, 498
 Mental incompetence, 486–487
 Mere evidence rule, 71, **339–342**, 602
 Mere relevance standard, 235
Messenger v. Gruner + Jahr Printing and Publishing (appropriation of name or likeness), 433
 Metal detectors, 15
Meyer v. Nebraska (parental autonomy), 129, 131, 219–220, 262, 374
Michael H. v. Gerald D. (rights of unwed fathers), 220
Michigan Dept. of State Police v. Sitz (automobile searches, sobriety checkpoint), 33, 511
Michigan v. Long (automobile searches), 34, 558–559
 Midler, Bette, 314
 Miller, Arthur R., 565
Miller v. Brooks (surveillance cameras), 546
Miller v. California (obscenity), 369, 371, 436
Miller v. Ford Motor Co. (appropriation of name or likeness), 432
 Mill, John Stuart, 395–396, 405
Minnesota v. Dickerson (search, stop and frisk), 531



- Miranda v. Arizona* (police interrogation), 16, 124
 Misapplication, 161
 Miscegenation statutes, 130, 218, 330
 Misclassification, 161
 Missile gap, 227
 Missionaries of the Unborn website, 5
 Mississippi Freedom Democratic Party, 226
 Missouri Open Records Act (MORA), 49, 50
 Mitchell, John, 133
Mitchell v. Baltimore Sun Co. (trespass), 566
 MKULTRA mind-control program, 92
 Mobile phone. *See* Cellular telephone
 Model Penal Code, American Law Institute, 65, 326
 Model State Public Health Privacy Act of 1999 (MSHPHA), 446
 Model State Vital Statistics Act and Regulations, 57
 Money laundering, 43, 44
 Money Laundering Control Act, 43
 Montgomery bus boycott, 345
 Moore, Sarah Jane, 314
Moore v. City of East Cleveland (family, definition of), 374
 Moral laws, recognition of, 127
 Morning-after pill, 6, 60
 Morse Code, 89
 Mothers Against Drunk Driving (MADD), 510, 512
 Motion Picture Association of America (MPAA), 381
 Multi-State Anti-Terrorism Information Exchange Program (MATRIX), 106, **342–343**
Murphy v. Waterfront Comm’n of New York Harbor (self-incrimination), 294
 Murrow, Edward R., 338
 Mutual transparency, 14

NAACP v. Alabama (freedom of association), 125, 236, **345–346**
Nader v. General Motors Corp. (intrusion upon seclusion), 430
 Napster, 381
 Narcotics trafficking, 44, 91, 232
 Narrowly circumscribed procedures, 162
 National Abortion Federation, 3
 National Abortion Rights Action League (NARAL), 2
 National Archives and Records Administration (NARA), 415
 National Bioethics Advisory Committee, 174
 National Cell Phone Courtesy Month, 334
 National Center for Health Statistics (NCHS), 56
 National Center for Missing and Exploited Children, 196, 342
 National Change of Address (NCOA) distribution, 572, 573
 National Conference of Commissioners on Uniform State Laws, 8, 272
 National Crime Information Center, 224, **347–348**
 National Cyber Security Alliance, 309
 National identity cards, 46, **348–349**, 420
 National Institute of Standards and Technology (NIST), 102, 167
 National Institutes of Drug Abuse (NIDA), 589
 National Labor Relations Act, 237
 National Network of Abortion Funds, 2
 National Organization of Women (NOW), 60, 421
 National Prohibition Act, 86–87, 357
 National Right to Life Committee, 3
 National Science Foundation Act, 105
 National security, individual privacy vs., 93–94, 124–125, 327, 395, 401
 National Security Act of 1947, 91
 National Security Agency, 102, 167, **349–351**, 419, 481, 598, 612
 National security letters (NSLs), 587
 National Sex Offender Registry (NSOR), 494
 National Telecommunication and Information Administration, 305
 National Traffic Safety Administration, 512
National Treasury Employees Union v. Von Raab (drug testing), 63, 186, 590
 National Venereal Disease Control Act of 1938, 62
 Natural rights, 182
 Necessaries doctrine, 218
 Negligent infliction, 314

- Netiquette, 199, 334
- Network Solutions, Inc., 305
- Neural network, 160
- Newsgathering torts, 312
- Newspeak, 52
- New State Ice v. Liebmann* (state regulation of business activity), 75
- Newsworthiness, 314, 431
- New York Anti-Vice League, 59
- New York Times v. Sullivan* (libel), 24, 74, 313
- New York Times v. United States* (publication of truthful information), 48
- New York v. Belton* (automobile searches), 34, 558
- New York v. Class* (automobile searches, police checkpoints), 31, 387, 511
- 911 emergency system, 563
- Nineteen Eighty-Four*, 51–53, 424
- Ninth Amendment, 127, 183, 263, 396, 617
- Nissenbaum, Helen, 18
- Nixon, President Richard, 225, 293, 424, 443, 488
- Nixon v. Administrator of General Services* (confidentiality), 264
- Nix v. Williams* (exclusion of physical evidence), 294
- No fly list, airline passengers, 15, 107, 159
- Noncompete agreement, 119
- Nondisclosure agreement, 119
- Nonpublic personal information, 42
- Norplant, 528, 529
- Noto v. United States* (subversive activities), 283
- “No Trespassing” signs, 155, 355, 356
- Novell, Inc. v. Weird Stuff, Inc.* (dumpster diving), 246
- Nuclear proliferation, 91, 92
- Obscenity, 16; adult theaters, 369–371; child pornography, 83–84, 365–366; in cyberspace, Communications Decency Act (CDA), **105–106**; FBI investigations into, 224, 280; legal definition of, 436; “patently offensive,” definition of, 106; right to possess in the home, *Stanley v. Georgia*, 66, **522–524**; three-part test for, 371, 436
- Observability, 422
- O’Connor, Justice Sandra Day, 233, 580
- O’Connor v. Ortega* (search and seizure, work-related), **353–355**
- Office of Strategic Services (OSS), 91
- Office of Transportation Vetting and Credentialing, 107
- Oldspeak, 52
- Oliver v. United States* (curtilage), 154–155, 318, **355–357**
- Olmstead v. United States* (wiretapping), **357–362**; Louis Brandeis on, 72, 73–74, 357, 360–361; Oliver Wendell Holmes on, 623; right to be let alone, 72, 120, 357
- Omnibus Crime Control and Safe Streets Act of 1968, 192, 193, 398, 610, 617; Title III, wiretaps, 19–20, 104
- Omnibus Transportation Employee Testing Act of 1991, 186
- Omnivore, 85
- Onassis, Jacqueline Kennedy, 367
- On Liberty*, 396, 405
- Online Privacy Alliance, 626
- Open fields doctrine, 154–155, 318, 355
- Open meetings laws, **362–363**, 423, **460**
- OpenPGP, 389
- Open records legislation, 7
- Open Skies doctrine, 14
- Operation Paperclip, 91
- Operation Rescue/Operation Save America, 3, 4, 184
- Opt-in vs. opt-out, 41, 137, **363–364**, 427, 476, 551
- Ordered liberty, concept of, 127
- Ordinary negligence, 26
- Organizational surveillance, 538
- Organization for Economic Cooperation and Development (OCED), principles of, 215–216
- Organized crime, 91
- Orth, Godlove S., 164
- Orwell, George, 51, 53, 424, 426
- Osborne v. Ohio* (child pornography), **365–366**
- Osborne v. United States* (attorney-client privilege), 70
- Otis, James, 68
- Packet-sniffing software, 86, 202; Carnivore, **84–86**, 200, 302, 308, 382, 609



- Packet switching technology, 297, 310
- Pam Lychner Act, 494
- Paparazzi, 312, **367–369**, 426
- Parental consent: for abortions, 3, 463; for collection/use of children's personally identifiable information, 94–95, 385
- Parent-child privacy: parental autonomy, 129, 130, 219–220, 265; rights of men to have relationships with their children, 220
- Parent, William, 407–408
- Paris Adult Theatre I v. Slaton* (obscenity, adult theaters), **369–371**
- Partial-birth abortion, 6
- Partner counseling and referral services (PCRS), 371
- Partner notification, **371–373**
- Passive airborne surveillance, 13
- Password(s): to access a computer, 27; as authentication method, 26, 54, 55; for Internet access, 307, 308, 309; numeric, for ATM use, 28; protection, **373–374**; stored on a computer, 381
- Pat down searches, 144, 391, 529, 556
- Patent infringement, 167
- Paternity, **374–376**
- Patient rights, **376–379**
- Patient Self-Determination Act, 150–151, 378
- Paton, Jean, 9
- PATRIOT Act. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)
- Paul v. Davis* (identification of arrestee), 146
- Pavesich v. New England Life Ins. Co.* (tort law privacy), 397–398
- Pay-at-the-pump technology, 137
- Payton v. New York* (search, exigent circumstances), **379–380**, 624
- Pedestrians, search of, 34
- Peeping Toms. *See* Voyeurism
- Peer-to-peer (P2P) technologies, 305, 306, **380–381**
- Pell, Sen. Claiborne, 221
- Penetration, defined, 504
- Pen mode, 85
- Pennsylvania v. Mimms* (automobile searches), 34
- Pen Register Act, 197, 198, 205
- Pen register devices, 104, 123, 202, 204, 234, 318, **381–383**, 458, 586
- Pentagon Papers, 443
- Pen/trap rule, 20
- Penumbral rights, 126, 182, 263, 265, 396, 623
- People v. Mackinnon* (silver platter doctrine), 508
- People v. Onofre* (consensual homosexual acts), 66
- Permission marketing, 363–364
- Persistent vegetative state, 149, 150, 397
- Personal accountability, 98
- Personal digital assistants (PDAs), 88, 455
- Personal identification number (PIN), 28
- “Personal is political,” 247, 251, 277, 400, 436
- Personality tests, 37
- Personally identifiable information, **383–385**; biometrics as a replacement for, 54; of children, collection and use of without parental consent, 94, 385; collection and use of, 77, 107, 111, 422; disclosure of, 77–78, 221–222; errors in, correcting, 78; examples of, 385; HIPAA requirements and, 377; on the Internet, 299; laws protecting confidentiality of, 22, 169, 183, 295; linked to credit cards, storage of, 135; obtained from trash, 290; for predictive analysis and profiling, 384; Privacy Act of 1974 and, 414; privacy notices and, 427; ready availability of, 39; sale of, 107–108; stored on a computer, access to, 381; telemarketing and, 552; third-party requests for, 78; U.S. Census data, 570
- Personal papers, seizure of, 67–72, 74, 124, 154, 261
- Personal Privacy in an Information Society*, 398
- Personal Privacy Protection Act, 369
- Personal privacy, protections against violations of, 116–117, 398–400
- Personal surveillance, 538
- Pharming, 309

- Phishing, 309
- Physician-assisted suicide, 128, 265, 378, 397, 603–604
- Physician-patient privilege, 270, 375, 439, 442–443
- Pierce v. Society of Sisters* (parental autonomy), 129, 262, 374, 375
- Pinkerton, Allan, 435
- Pinkerton Nat'l Detective Agency, Inc. v. Stevens* (intrusion upon seclusion), 431
- Plain view doctrine, 34, 267, 379, **386–388**, 457, 519, 578; three-part test for, 387
- Plan B. *See* Morning-after pill
- Planned Parenthood Federation of America, founding of, 59
- Planned Parenthood of Southeastern Pennsylvania v. Casey* (reproductive rights), 3, 17, 130, 219, 264, 265, 278, 326, 463, 613
- Planned Parenthood v. ACLA* (intimidation of abortion doctors), 4
- Platform for Privacy Preferences (P3P), 309
- Poe v. Ullman* (birth control), 262, 277, 278, 624
- Police checkpoints, 30, 31, 33, 511
- Political cartoons, 315
- Political dissent, suppression of, 122
- Political parties, membership in, 237–238
- Polygraph testing, 9, 37, 189, 580–581, 617, 619
- Pornography: adult, sale of, 324; adult theaters, 369–371; cached to the hard drive, 114; child, 83–84, 365–366; FBI involvement with, 224; on the Internet, 105, 305; private, home possession of, 66, 365, 396, 412; video rentals, 168–169
- Postmortem reproduction, 23
- Post Office Protocol version 3 (POP3), 198
- Powell, Justice Lewis Franklin, Jr., 356, 519
- Prayer in public schools, 16
- Preimplementation genetic diagnosis (PIG), 21
- Premarital blood testing, 62, 63
- Prenatal abuse, 375–376
- Prenatal testing: for HIV, 63; for inherited disease, 21, 379; mandatory for congenital infection, 62
- President's Commission for the Study of Ethical Problems in Medicine and Biomedical and Behavioral Research, 468
- Presley, Elvis, 314
- Pretexting, 41, 229
- Pretty Good Privacy (PGP), 309, **388–389**
- Prince v. Massachusetts* (child welfare), 262
- Prisoners, **389–393**, 422; cell, as home, 286; constitutional protections for, 390; drug testing of, 185–186; forced sterilization of, 182, 497, 527; guards, surveillance of, 422; HIV testing of, 391–392; reasonable expectation of privacy, 285–286, 533; secrecy among, 482; strip searches, 532; surveillance of, 185–186, 422; torture of, 93, 122. *See also* Criminal suspects and arrestees
- Privacy Act of 1974, **414–418**; access provisions of, 170, 174; amendments to, 109; and confidentiality of personally identifiable information, 22, 169; enactment of, 398, 400, 414–415; exceptions/exemptions to, 98, 107, 415–416, 417–418; fair information practices in, 215, 273, 414; FBI violation of, 419; and Freedom of Information Act, 452; government records, 118, 347; notification requirements, 416–417; reason for, 281; Social Security numbers, collection of, 415, 418, 514; tax records, protection of, 295; United States Postal Service, 573
- Privacy advocacy organizations, 75, 300, **419–421**, 476
- Privacy and inequality, **421–427**
- Privacy Alliance, 302
- Privacy, definition of, **393–403**; and accountability, 400–401; civil liberties, sacrifice of, 401–402; common law contribution to, 397–398; contradictions, reconciling, 402–403; privacy given

- away, 402; privacy law, overview of, 396–397; statutory privacy movement, 398–400
- Privacy-enhancing technologies, 309
- Privacy Foundation (PF), 421, 427
- Privacy Impact Assessment, IRS, 295
- Privacy International (PI), 75, 419–420, 476, 628
- Privacy notices, 78, 399, **427–429**; format, 429; readability, 428; statutes requiring, 428
- Privacy, philosophical foundations of, **404–414**; coherentists on the meaning and value of privacy, 407–411; feminist critique, 411–412; historical roots, 404–406; literature, 406–407; scope of privacy, 412–413
- Privacy Protection Commission, U.S., 398
- Privacy Rights Clearinghouse (PRC), 137, 420, 628
- Privacy seal programs, 302
- Privacy tort(s), 65, 73, 394, 397–398, **429–434**; appropriation of name or likeness, 73, 311, 394, 398, 430, 432–433; breach of confidentiality, 433; defined, 311, 312; false light, 73, 311, 312–314, 394, 398, 430, 432; intrusion upon seclusion, 73, 311, 312–313, 394, 398, 429, 430–431, 492, 566; negligence, 433; *Pavesich v. New England Life Ins. Co.*, 397–398; public disclosure of private facts, 73, 311, 314–315, 394, 398, 429–430, 431–432, 467
- Private investigator(s), 184, **434–435**, 482, 539
- Private key, 167
- Private parts, **435–438**, 483–484; defined, 435; exposure of, 334–335; restrooms and dressing rooms, **465–466**; sexual violence and, 504; video voyeurism, 525, 545, 615
- Private schools, 221
- Privilege, **438–444**; accountant-client, 443; attorney-client, 439–440; and confidentiality compared, 118; executive, 443; marital, 441; physician-patient, 270, 375, 439, 442–443; of press to report judicial proceedings, 135; purpose of, 444; by race and social class, 464; religious, 441–442; reporter's, 442; two-step test for, 444–445
- Privileges and Immunity clause, Fourteenth Amendment, 127–128
- Pro-choice movement, 1, 2
- Procurier v. Martinez* (inmate correspondence), 390
- Profiling, racial/ethnic, 93
- Progressive Labor Party, 284
- Prohibition, 86–87, 280, 357, 386
- Project Match, 109
- Pro-life movement, 1, 2–3
- Property rights, protection of, 129
- Proprietary privacy, 393
- Prosser, Professor William, 65, 73, 312, 398, 407, 430
- Prostitution, 224, 324, 397
- Protected health information (PIH), 445
- Protection from Personal Intrusion Act, 369
- Psychological investigations, 189
- Psychotherapy, 116, 272
- Public Access to Court Electronic Records (software), 172
- Public disclosure of private facts privacy tort, 73, 311, 314–315, 394, 398, 429–430, 431–432, 467
- Public figures, libel law and, 24–26
- Public health and safety, **444–447**; and civil liberties, 401; and disclosure of information, 377, 444–445; greater good argument, 61–62; inspection, rental properties, 322; partner notification, **371–373**; protected health information (PIH), 445; surveillance programs for, 271, 378, 445. *See also* Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Public Health Service, U.S., 62
- Public-key cryptography, 152–153, 166, 388–389
- Public/private dichotomy, 411, **447–451**; Aristotle and, 405, 447–448; components of, 448–449; false, 450; privacy implications of, 450–451; private parts, definition of, 435; reproductive rights and, 464–465; women's parity in, 250, 277

- Public records, 408, **451–453**; availability of, 49–50; on credit reports, 141; data mining of, 159, 342; disclosure of, 134, 170–171; open meetings laws, **362–363**; private investigators' use of, 434
- Public Utilities Commission v. Pollack* (right to be let alone), 182
- Quickbird satellite, 14
- Quid pro quo sexual harassment, 500
- Quilloin v. Walcott* (rights of unwed fathers), 220
- Quinlan, Karen Ann, 397, 467
- Rachels, James, 410
- Racial classification, 331
- Racial discrimination, 332
- Racial Integrity Act of 1924, 331
- RadarSAT satellite, 13
- Radio frequency identification (RFID), 46, 93, 204, 206, 349, 384, 420, **455–456**, 536
- Radioimmunoassay (RIA), 185, 589
- Rampellsoft, 308
- Random drug testing, 98, 186, 188, 590
- Rape: defined, 504; nonconsent, proof of, 505; shield laws, 501, 506; victim identity, disclosure of, 134–135, 314
- Reade, Edwin Godwin, 275
- Reagan, President Ronald, 186, 227, 258, 284, 348, 488, 590
- Real ID Act of 2005, 348
- Reasonable expectation of privacy, **456–459**; and abandonment compared, 244; automobile searches, 32, 80, 518; celebrities and, 368; and disclosure of information to third parties, 125; and drug testing policies, 186–187, 590, 594; employees, 616; exigent circumstances and, 380, 481; as a Fourth Amendment protection, 122, 144, 317, 509; and garbage left at curbside, 244, 247, 458; home and, 154, 577; *Katz v. United States* (reasonable expectation of privacy), 32, 70, 74, 244, **317–319**, 355, 361, 396, 456, 480, 490–491; *Oliver v. United States*, **355–357**; physical tracking device, insertion of, and plain view doctrine, 387, 457, 578; prisoners, 285–286, 533; as replacement for constitutionally protected area, 361, 457; restrooms and dressing rooms, 465, 525; *Terry v. Ohio*, 556; thermal sensor imaging, 122–123, 125, 145, 319, 457, **559–561**, 579; third-party doctrine, 458; and voice identification, 576–577; in the workplace, 353–355
- Reasonable suspicion, 125, 144, 145, 388, 530
- Recording Industry Association of America (RIAA), 381
- Red & Black Publishing Co. v. Board of Regents* (open meetings), **459–461**
- Red-light and speeding cameras, **461–462**, 546
- Redlining, 161
- Red Scare, 336
- Reductionism, 406–407
- Regression analysis, 160
- Rehnquist, Chief Justice William, 150, 315, 325, 511, 519, 580
- Reiman, Jeffrey, 404
- Relational privacy, 218
- Religion-based privacy issues, 55
- Religious privilege, 441–442
- Remedy of exclusion, 341
- Remote computing service (RCS), 196
- Remote sensing, 13
- Remsburg v. Docusearch, Inc.* (privacy protection, negligence), 433
- Reno, Janet, 99
- Reno v. American Civil Liberties Union* (indecent speech), 106
- Repeat customers, 167
- Reporter's privilege, 442, 574–575
- Reproductive cloning, 22
- Reproductive rights, **462–465**; defined, 462; protection of, 17, 396–397; race and social class, role of, 464
- Resources for further study: books, 625–626; films, 628–629; organizations, 627–628; websites, 626
- Restatement of Torts*, American Law Institute, 398
- Restraining orders, 367
- Restrooms and dressing rooms, 334, **465–466**, 594

- Rhodes v. Chapman* (prisoner rights), 390
 Richardson, Elliot, 214
 Ridge, Tom, 106
The Right of the People, 182
 Right to be let alone doctrine, 311, 318, 357, 430, **466–467**; application of, 169, 182; arrestees, 146; as definition of privacy, 393, 614; judicial constitution of, 59; origins of, 72; patient rights, **376–379**; and rental property, 321; reproductive rights and, 462; telemarketing and, 177; wiretapping and, 609–610
 Right to die, 130–131, 265, 397, **467–469**; *Cruzan v. Director, Missouri Dep’t of Health*, 6, **148–151**, 265, 397, 603; feeding tubes, removal of, 149, 150; *In re Quinlan*, 397, 467; Patient Self-Determination Act, 150–151, 378; physician-assisted suicide, 128, 265, 378, 397, 603–604; Terri’s Law, 469
 Right to Financial Privacy Act of 1978, 39, 169, 398
 Right to know, 101, 288
 Right to life, 2. *See also* Pro-life movement
 “The Right to Privacy,” 72, 248, 275, 311, 397, 406, 430, 466
 Road rage, 334
Roberson v. Rochester Folding Box Co. (commercial appropriation of name/likeness), 72–73, 311, 398
 Roberts, Chief Justice John, 6, 131
Roberts v. United States Jaycees (freedom of association), 238
 Roentgen, W. C., 621
Roe v. Wade (legalization of abortion), 2, 60, 64, 66, 128, 130, 131, 165, 396, **469–473**, 607; and gender equality, 250–251; patient rights and, 377–378; as precedent for subsequent privacy cases, 265, 325; as privacy issue, 278, 436, 462–463, 613, 624; South Dakota challenge to, 6; William O. Douglas on, 183
 Rogers, William, 227
A Room of One’s Own, 614
 Roosevelt, Eleanor, 225, 280
 Roosevelt, President Franklin D., 181, 224, 262, 283, 513
 Rootkit, 301, 308
 Rosenberg, Julius and Ethel, 337
 Rotenberg, Marc, 420, 421
Roth v. United States (obscenity), 523
 Rounds, Gov. Mike, 6
 Roving wiretaps, 20, 303, 586, 612
 RSA (Rivest-Shamir-Adelman) algorithm, 167, 389
 RU-486, 6
R. v. Ayoob (sex offender registries), 495
R. v. Burke (sex offender registries), 495
 Safe Harbor Principles, 364, **475–476**
 Safe harbor provision, Children’s Online Privacy Protection Act, 94
 Salisbury, Harrison, 226
 Same-sex marriage, 131, 218, 325, 393
Sanchez-Scott v. Alza Pharmaceuticals (patient rights), 377, 615
 “Sanctity of the domestic circle,” 278
 Sanger, Margaret, 58, 59
 Santorum, Sen. Rick, 61
 Scalia, Justice Antonin, 186, 278, 325, 487
 Scanlon, Thomas, 407
 Scarlet Letter Law, 374
 Schaffer, Rebecca, 184
 Schiavo, Terri and Michael, 469
 Schindler, Bob and Mary, 469
 Schlesinger, James, 92
Schmerber v. California (blood samples, blood alcohol level), 61, 70, 145, **476–479**
 Schoeman, Ferdinand, 404, 406, 412
 Schwarzenegger, Governor Arnold, 369
 Scowcroft, Brent, 102
 Search engines, 158, 299, 303, 305, 308
 Search(es): of automobiles, 30–31, **32–36**, 79–80, 86–88, 123, 144–145, 490, 511, 518–519; body-cavity, 391, 533; criminal suspects and arrestees, 144–145; exclusionary rule, 31, 123–124, 481, 507, 607; “grab area,” 144; incident to arrest, 96–97, 144, 532; justification for, 123; notification of, 585; pat downs, 144, 391, 480, 529, 556; personal papers, 67–72, 74, 124, 154, 261; plain view doctrine, 34, 267, 379, **386–388**, 519, 578; probable cause argument for, 87, 122, 144, 224, 286; reasonable expectation of privacy,

- 32, 70, 74, 80, 122, 125, 144, 610; reasonable suspicion argument for, 125, 144, 145, 286, 388, 530; “relatively minor intrusion” argument for, 96; remedy of exclusion, 341; sealed letters, 358, 574; sneak and peek, 584, 585; stop and frisk, 480, **529–532**; strip, 391, 530, **532–534**, 621; thermal sensor imaging, 122–123, 125, 145, 319, 457, 489, **559–561**, 578–579; work-related, 353–355; x-ray devices for, 621–622
- Search warrant(s), **479–482**; absence of, 65, 168; and aerial surveillance, 81; criteria for obtaining, 20; defined, 32; exceptions to requirement for, 144, 532; and exigent circumstances, 123, 145, 379–380, 481; for financial records, 39, 43; garbage as evidence for, 156; for installing keystroke loggers, 320; lack of, 95; mere evidence rule, 71, **339–342**, 602; need for, 87, 123, 144, 194; and open fields doctrine, 154–155, 318, 355, 356; sense-enhancing technologies and, 490; and spying on American citizens, 93, 125; for stored communications, 196–197; and telephone conversations, 73; in the workplace, 354
- Second Treatise on Government*, 405
- Secrecy, **482–485**; age-related, 483; birth parent identity in adoptions, 7; and CIA operations, 92; confidentiality as, 117; diaries, encryption systems, 152, 483; and FBI operations, 482; of Grand Jury proceedings, 147; president’s need for, 443; to prevent industrial espionage, 246, 482; and privacy, relationship between, 410, 484–485; private investigators and, 482; private parts, 483–484; sacred knowledge as, 484; secret societies, 483
- Secret knowledge, 54, 55, 484
- Secret prisons, 93
- Secure Automobile Inspection Lanes (SAIL), 621–622
- Secure Flight, 106–107
- Secure Hashing Algorithm, 102
- Secure Socket Layer (SSL) protocol, 152, **485–486**
- Seeger, Pete, 225
- Selectee list, airline passengers, 15, 107
- Selective availability, 258
- Self, concept of, 412
- Self-determination, notion of, 2
- Self-disclosure, voluntary, 394, 401
- Self-incrimination, protection against. *See* Fifth Amendment
- Self-preservation, right to, 405
- Self-regarding behavior, 64, 66, 327, 396, 405
- Self-regulation, of privacy practices, 301–302, 476
- Self-restraint, 335
- Sell v. United States* (mental incompetence), **486–487**
- Senate Internal Security Subcommittee (SISS), 225, 337
- Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (Church Committee), 133, 281, **488–489**
- Sense-enhancing technologies, **489–493**. *See also* Thermal sensor imaging
- Separate spheres doctrine, 249–250
- September 11. *See* Terrorism, September 11 attacks
- Servicemembers Legal Defense Network (SLDN), 180
- Session key, 103
- Seven dirty words, 106
- Sex Deviate program, FBI, 225–226
- Sex Offender Information Registration Act (Canada), 494
- Sex offender(s), **496–499**; buffer zones for neighbors, 497–498; laws related to, 494, 496; notification laws, 497; registries of, 323, **493–496**, 497–498, 524; treatment for, 496–497
- Sexual harassment, 247–248, 324, 353, 401, **499–504**, 505
- Sexual History Newspaper Requirement (Florida), 374
- Sexually transmitted diseases, 3; federal public health campaign to contain, 62; gonorrhea, 62; partner notification, **371–373**; patient rights



- and, 378; syphilis, 62, 287. *See also*
Human immunodeficiency virus
(HIV)
- Sexually violent predator (SVP)
legislation, 496
- Sexual misconduct, 249
- Sexual norms, 334
- Sexual orientation, right to privacy,
178–179
- Sexual violence, 401, 503, **504–507**,
613–614
- Shahar v. Bowers* (consensual sexual
activity), 517
- Shakedown search, 285
- Shelby Amendment, Driver's Privacy
Protection Act, 183
- Shelton v. Tucker* (freedom of association),
236
- Shepherd-Barron, John, 28
- Shield laws: rape, 501, 506; reporter's
privilege, 442
- "Shoe leather epidemiology," 62
- Shoplifting, 465
- Shredded documents, reconstruction of,
246
- Shulman v. Grou W. Productions, Inc.*
(public disclosure of private facts),
431
- Signals intelligence (SIGNIT), 13, 349
- Silver platter doctrine, **507–508**
- Silverthorne Lumber Co. v. United States*
(fruits of the poisonous tree
doctrine), 293
- Simjian, Luther George, 28
- Simple Mail Transfer Protocol (SMTP),
198
- Single-factor authentication, 26–27
- Sipple v. Chronicle Publishing Co.* (public
disclosure of private facts), 314, 431
- Sixth Amendment, right to an attorney, 294
- Skinner v. Oklahoma* (sterilization of
convicts), 182, 262, 374, 497, 527
- Skinner v. Railway Labor Executives'*
Ass'n. (drug testing), 186, **508–510**,
589–590
- Skipjack encryption algorithm, 102
- Skype program, 306
- Slavery, 163, 164, 396
- Slochow v. Board* (response to
McCarthyism), 338
- Smart cards, 26, 28, 29, 54, 373, **510**
- Smart stamps, 573
- Smith Act. *See* Alien and Registration Act
of 1940
- Smith v. Daily Mail* (publication of truthful
information), 48
- Smith v. Maryland* (telecommunications
privacy), 318, 458, 459
- Smith, William French, 227
- Smyth v. Pillsbury Co.* (e-mail
confidentiality), 200–201
- Sneak and peek searches, 584, 585
- Sobel, David, 420
- Sobriety checkpoint, 33, 123, 393,
510–513
- Social inequality, 335
- Socialist Workers Party, 133
- Social proximity, 334
- Social Security Act of 1935, 62
- Social Security number, **513–515**;
anonymity and, 17; on birth
certificates, 57; and census data, 571;
child's, protection of, 94; collection
and use of, 107, 415, 418, 420; on
credit reports, 141; of criminal
suspects and arrestees, 172; as IRS
identification, 294–295; as key
customer identifier, 290; laws
protecting disclosure of, 183; as
personally identifiable information,
77, 383, 513; as a universal
identifier, 348; use of by an imposter,
289, 393, 513–514
- Sodomy, **515–518**; court rulings on, 64–67;
defined, 515; same-sex, as a crime,
65, 324, 437
- Sony Corp. v. Universal City Studios, Inc.*
(intellectual property), 381
- Sound-alike ads, 314
- South Dakota v. Dale* (drinking age), 512
- South Dakota v. Opperman* (automobile
search), **518–520**
- Spam, 158, 166, 307, 383, **520–522**
- Spatial proximity, 334
- Sperm donors, anonymity of, 22, 23
- Spousal abuse. *See* domestic violence
- Sprinkle, Annie, 437
- Spyware, 114, 303, 306, 308–309, 381, 567
- Stanley v. Georgia* (pornography in the
home), 66, 365, 396, **522–524**, 624
- Stanley v. Illinois* (rights of unwed fathers),
220, 374

- Starr, Kenneth, 99
 State of California Office of Privacy Protection, 626
 State security, 13
State v. Diaz (surveillance cameras), 546
State v. Glas (voyeurism), 525
State v. Rhodes (domestic violence), 275
State v. Roland (garbage left at curb), 247
 Statutory rape, 249
Steele v. United States (search and seizure, contraband), 386
 Steinem, Gloria, 225, 250, 277
Stenberg v. Carhart (reproductive rights), 17
 Stephanie's law, **524–526**
 Sterilization, 60, 182, 411, 464, 497, **527–529**
 Stern, Carl, 133
 Stevens, Justice John Paul, 511, 519, 580
 Stevenson, Adlai, 225
 Stevens, Rep. Thaddeus, 164
 Stewart, Justice Potter, 162, 264, 519
Stigma: Notes on the Management of Spoiled Identity, 5
 Stigmatization, 287
 Stop and frisk search, 480, **529–532**
 Stored communications, surveillance of, 20–21
 Stored Communications Act (SCA), 196; actions prohibited by, 205; and Electronic Communications Privacy Act compared, 196; exclusions, 198; information accessible by subpoena, 318; information protected by, 196
 Strict scrutiny standard, 2, 131
 Strikes, 283
 Strip search(es), 391, 530, **532–534**, 621
Stromberg v. California (symbolic speech), 16
 Structured behavioral control program, 92
 Student Nonviolent Coordinating Committee (SNCC), 284
 Students for a Democratic Society (SDS), 133, 236
 Subject-initiated surveillance, 539, 540
 Substitution cryptography, 151
 Suburban sprawl, 276
 Subversive Activities Control Board (SACB), 296
 Subversive activities, investigation of, 282–283, 488–489
 Subversive Activities Review Board, 132
 Summers, Anthony, 281
 Sumner, Sen. Charles, 164
 Supermarket loyalty cards, 565
 Supreme Court Multimedia, 626
 Surrogacy, 22, 376
 Surveillance, **534–544**; ACLU concerns about, 17; aerial, 80–82, 154, 155, 318–319; agent-initiated, 539; airborne, **12–14**, 547; audio and video, 21; Big Brother, **51–53**, 424; of bus stations, train depots, and airports, 232; cameras, 29, 195, **544–549**; capacity of computer chips, 46; to circumvent terrorist activities, 93, 125; computer networks, 293; countersurveillance, 462, 540; creep, 461, 541; data mining and, 159; defined, 535; electronic, 192, **201–206**, 360, 481; employer, 616; external constituency, 538; by the FBI, 86, 224, 281, 488; federal powers of, Supreme Court interpretation of, 132–133; of financial activities, 39; Foreign Intelligence Surveillance Act of 1978 (FISA), 205, **234–235**, 401, 585, 586–587, 611; as harassment, 408; Internet as, 299; intimate areas protected from, 74; library records, 329; mail, 572; National Security Agency responsibilities, 350; in open fields, 356; organizational, 538; parental, cellular telephones, 90; pen register devices, 104, 123, 202, 204, 234, 318, **381–383**, 586; personal, 538–539; of prison guards, 422; of prison inmates, 185–186, 422; privacy implications of, 542–544; private investigators and, 434, 538; processes, 540–542; provisions for in Internal Security Act of 1950, 297; public health, 271, 378, 445; radio frequency identification (RFID), 46, 93, 204, 206, 349, 384, 420, **455–456**, 536; of restrooms and dressing rooms, 465; secrecy in, 482; sexual contacts, 62; stored



- communications, 20–21; structures, 537–540; subject-initiated, 539, 540; technological innovations in, 535–536; of telephone conversations, 357; tenants by landlords, 321; traditional, 535; two-way mirrors, 568; using sense-enhancing technologies, **489–493**; warrants and, 144; workplace, 482
- “Surveillance society,” 51, 53
- Suspicious Activity Report, 43
- Symmetric-key cryptography, 152
- Syphilis: premarital testing for, 62; Tuskegee Institute study, 287
- System of records, 415
- Tact, 334
- Taft, Chief Justice William Howard, 359
- Talk radio, 101
- Tamper-proof hardware encryption chip. *See* Clipper and Capstone chips
- Tangible employment action, 500
- Tangible records, compelled disclosure of, 234, 235, 359, 585
- Tarasoff v. Regents of the University of California* (health privacy), 272
- Tax evasion, 43
- Tax Reform Act of 1976, 169
- Taylor v. United States* (search and seizure, contraband), 386
- Tearoom Trade*, 287
- Technology: intrusions made possible by, 82; in War on Terror, 124–125
- Telecommunication Act of 1996, **551–552**; Customer Proprietary Network Information (CPNI), 551; opt-in rights, 551; Title V, Communications Decency Act (CDA), **105–106**
- Telemarketing, 89, 137, 166, 295, 399, 420, **552–555**, 573; Do-Not-Call Registry (DNCR), **177–178**, 364, 399, 553–554; opt-out mandate, 364; and personally identifiable information, 383
- Telephone(s): caller ID, 90, 197; calls, tracing the origin or destination of, 20; cellular, 19, 46–49, **88–91**, 93, 104, 130, 204, 257, 258, 308, 318, 334, 395, 424, 434, 545, 600, 613; consumer transactions by, 137; wiretapping, 19–20, 89–90
- Telephone Consumer Protection Act (TCPA) of 1991, 178, 553
- Telephone numbers, privacy status of, 89, 107
- Tell All Adoption Law. *See* Sexual History Newspaper Requirement (Florida)
- Tenth Amendment, states’ rights, 331
- Terrorism: anti-abortion movement as, 4; and birth certificates, control of, 57; domestic, 227–228, 584, 587–588; financing of, attempts to curb, 44; foreign agents in the U.S., 234; high factor score for, 342; identification of terrorists by data mining, 161, 342; and increase in background checks, 37; Multi-State Anti-Terrorism Information Exchange Program (MATRIX), 106, **342–343**; quotient, 342; September 11 attacks, 15, 31, 43, 227, 395, 401; surveillance as means to circumvent, 93–94; terrorist screening database, 106–107; vehicle searches and, 31; wiretapping on suspicion of, 12
- Terry v. Ohio* (pedestrian searches), 34, 233, 530, **555–559**
- Texas v. Brown* (automobile search, plain view doctrine), 387, 457
- Thalidimide, 1
- Therapeutic abortions, 1
- Thermal sensor imaging, 122–123, 125, 145, 319, 457, 489, 491, **559–561**, 578–579
- Thin-Layered Chromatography (TLC), 185, 589
- Third Amendment, quartering of soldiers in private homes, 121, 263
- Third-party doctrine, 458, 585
- Thirteenth Amendment, abolition of slavery, 164, 396
- Thomas, Justice Clarence, 325, 487
- Thompson v. Close-up, Inc.* (false light), 432
- Thomson, Judith Jarvis, 407, 410, 412
- Thornburgh v. Abbott* (inmate correspondence), 390
- Thornton v. United States* (automobile searches, incident to arrest), 35
- Thoughtcrime, 52
- Thought Police, 51, 52
- Thurmond, Sen. Strom, 517

- Tileston v. Ulmann* (birth control), 262
Time, Inc. v. Hill (false light), 313, **561–562**
The Tin Drum (film), 83
Tinker v. Des Moines Independent School District (student rights), 16
 TIROS weather satellites, 14
 “Too much information,” 117
 Torture, of prisoners, 93, 122
 Total Information Awareness Program, 343
 Trade secrets, 48, 119, 245–246
 Traffic data, 202
 Traffic enforcement, 461–462
 Transactional data, 202, 203
 Transaction-generated data, 136, 166, **562–565**
 Transmission Control Protocol/Internet Protocol (TCP/IP) data, 85, 485
 Transportation Safety Administration (TSA), 15, 106, 621
 Transport Layer Security (TLS), 485
 Transposition cryptography, 151
 Trap-and-trace devices, 104, 195, 197, 202, 204, 234, 381
A Treatise on the Law of Torts, 397
 Trespass, 154, 311, 312, 317, 321, 359, 369, 393, 397, 408, **566–567**
 Trespass to chattels, 521, 566–567
 Trilateralism, 257
 Triple Data Encryption Standard (TDES), 28, 152
 Tripp, Linda, 100
 Trohan, Walter, 225
 Trojan Horse, 86, 203, 320
Troxel v. Granville, 265
 Truman, President Harry, 181, 283, 338, 349
 Trumbo, Dalton, 284
 Trusted traveler system, 15
 TRUSTe privacy seal program, 302, 399, 476
 Truth, as a defense, 134–135, 313
 Tuck, William, 284
 Turner, Carlton, 590
Turner v. Safely (inmate correspondence), 390
 Tuskegee Institute syphilis study, 287
 Twenty-First Amendment, repeal of Prohibition, 86
 Twining, Nathan, 227
 Two-Minute Hate, 51
 Two-way mirrors, **567–568**
 Tydings Committee, 338
 Ullman, Abraham, 262
 Underage drinking, 512
 Undue burden standard, 131
 Uneasy access, 615
 Unenumerated rights, 126, 127–131, 182, 396
 Uniform Adoption Act, 8
 Uniform Code of Military Justice, 324
 Uniform Resource Locators (URLs), 198
 Uniform Trade Secrets Act, 119
 Unindicted co-conspirators, naming of, 147
 Unintended pregnancy, 60
 Union shop, 237
 United Electrical, Radio, and Machine Workers of America, 283, 604
 United States Census, **569–572**; access to taxpayer data, 295; confidentiality and, 569; data available from, 563; data brokers and, 158; decennial census, 56, 569; personally identifiable information, collection of, 570; Public Use Microdata Samples (PUMS), 571; standard birth certificate, 56
 United States Children’s Bureau, 8
United States Department of Defense v. Federal Labor Relations Authority (privacy, home), 624
 United States Postal Service (USPS), 553, **572–574**; anthrax scare, 573; National Change of Address (NCOA) distribution, 572, 573; private mail boxes (PMBs), 572–573; sender identification program, 573
 United States Secret Service, 109
United States v. Caldwell (reporter’s privilege), **574–575**
United States v. Carolene Products (government interference), 262
United States v. Causby (trespass, airline flights), 566
United States v. Chadwick (automobile searches, containers), 35
United States v. Councilman (privacy, e-mail), 200



- United States v. Dionisio* (voice identification), **575–577**, 598
- United States v. Dunn* (curtilage), 154, **577–578**
- United States v. Flores-Montana* (automobile searches, border crossing), 30, 31
- United States v. Karo* (tracking devices), 457
- United States v. Keith* (electronic surveillance), 350
- United States v. Knotts* (tracking devices), 457, 546
- United States v. Kyllo* (searches, thermal sensor imaging), 122–123, 145, 319, 457, 491, 560, **578–580**
- United States v. Leon* (automobile searches, good faith exception to exclusionary rule), 31
- United States v. Martinez-Fuerte* (automobile searches, border crossing), 33, 531
- United States v. Mendenhall* (search, freedom to leave), 530
- United States v. Miller* (financial privacy), 39, 318, 458
- United States v. Morris* (computers fraud and abuse), 108
- United States v. Nixon* (Pentagon Papers), 443
- United States v. NY Telephone* (pen register devices), 318
- United States v. Ortiz* (automobile searches, police checkpoints), 33
- United States v. Rabinowitz* (search incident to arrest), 96
- United States v. Robinson* (automobile searches, incident to arrest), 35
- United States v. Ross* (automobile searches, containers), 35
- United States v. Scheffer* (urine analysis), **580–581**
- United States v. Scott* (industrial espionage), 245
- United States v. Steagald* (multiple search warrants), **581–583**
- United States v. United States District Court* (warrants, national security exception), 125
- United States v. Vuitch* (reproductive rights), 17
- United States v. Wade* (voice exemplars, incriminating evidence), 70, 294
- United States v. Westinghouse Electric Corp.* (employee health records), 272
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), **583–588**; ACLU challenges to, 17; automobile searches and, 31; bar codes in conjunction with, 46; cyberterrorism and computer fraud, 109; domestic terrorism, crime of, 584, 587–588; e-mail and, 198, 200; evidence of criminal intent, 228; FBI under, 228; foreign intelligence gathering within the U.S., 586–587; Internet Protocol (IP) addresses and, 198; Internet use, monitoring of, 586; library records, requirements for, 327, 328, 329; national security letters (NSLs), 587; as outgrowth of Internal Security Act of 1950, 296; passage of, background, 583–584; pen registers under, 198, 382, 586; personal records, 585–586; privacy implications of, 421; provisions affecting privacy interests, 584; scope of, 583; sneak and peek searches, 584, 585; student information, disclosure of, 223; summary of, 584; Title III, International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, 44; and Video Privacy Protection Act, 595; wiretapping under, 20, 104, 303, 584, 611–612
- Universal identification, 231
- Universal Product Code (UPC), 45
- Unmanned aerial vehicles (UAVs), 12
- Unreachability, 18. *See also* Anonymity
- Upjohn Co. v. United States* (attorney-client privilege), 440
- Upskirting, 523, 600
- Urban Mass Transportation Administration, 186
- Urine analysis, **588–591**; of arrestees, 145; *Chandler v. Miller*, 17; for detecting

- substance use and abuse, 61, 185, 588–589; of employees, 37; mandatory, 63; of political candidates, 17; student athletes, 593–594; *United States v. Scheffer*, 580–581
- U.S. Department of Justice v. Reports Committee for Freedom of the Press* (disclosure of information, arrestees), 148
- Usenet groups, 298, 381
- Vehicular tracking devices, 257
- Vernonia School District v. Wayne Action* (drug testing, student athletes), 187, **593–594**
- Viagra, 60
- Video Privacy Protection Act of 1988 (VPPA), 168, 169, **594–596**
- Video surveillance, 21
- Video voyeurism, 524–526, 545, 598, 615
- Video Voyeurism Prevention Act of 2003, 545
- Village of Bella Terre v. Borass* (family, nontraditional residences), **596–597**
- Violent Crime Control and Law Enforcement Act of 1994, 184
- Voice exemplars, 70, 341
- Voice identification, 576–577, **597–598**
- Voice-Over-Internet Protocol (VoIP), 90, 104, 303, 304, 305, 306, 381
- Voiceprints, 107
- Volokh, Eugene, 431–432
- Volstead Act. *See* National Prohibition Act
- Voluntary passive euthanasia, right to, 130
- Voluntary self-disclosure, 394
- Voorhis Act, 282
- Voyeurism, 116, 321, 465, 524–526, 568, **598–600**, 614–615
- Vucetich, Juan, 230, 231
- Warden v. Hayden* (search and seizure, mere evidence rule), 70, 340–341, **601–602**
- War driving, 203
- Ware, Willis, 214
- War on Drugs, 44
- War on Terror, 44; immigration violations, 147–148; relationship between informational privacy and national security in, 124–125. *See also* Terrorism
- Warrantless search(es): of automobiles, 30–31, 87–88; plain view doctrine, 34, **386–388**; reasonable expectation of privacy, 459
- Warren, Chief Justice Earl, 263, 330, 331, 436
- Warren, Samuel, 72, 120, 248, 275, 278, 311, 397, 406, 407, 409, 430, 466, 614
- Washington et al. v. Glucksberg et al* (physician-assisted suicide), 128, 265, 397, **603–604**
- Washington v. Chrisman* (search, plain view doctrine), 386
- Wasserman blood tests, 62
- Watch lists, airline passengers, 15
- Watergate scandal, 424; CIA operations during, 92; FBI operations during, 92, 281; and Privacy Act of 1974, 414–415
- Watkins v. United States* (subversive activities), **604–605**
- Wayman, James, 54
- Wayne, John, 284
- Web bugs, 307, 308, 309
- Weber, Max, 421
- Webster v. Reproductive Health Services* (reproductive rights), 6, 396, 437, **605–607**
- Wechsler, Ely and Herbert, 182
- Weeks v. United States* (search and seizure, exclusionary rule), 96, 481, 507, **607–608**
- Weird Stuff, Inc., 246
- Welch, Sen. Joseph, 338
- Wells, Sumner, 225
- Westin, Alan, 18, 174, 404
- West, Robin, 615
- Whalen v. Roe* (confidentiality), 118, 264, 271–272, 361, 412
- Whistleblowers, 170, 173
- White, Justice Byron, 134, 243, 244, 263, 519
- Whitehead, Don, 225
- White Primary Cases, 238
- White Slave Traffic Act, 224
- White, Vanna, 313
- Whitewater land deal, 99



- Whitney v. California* (right to protest and assemble), 74
- WHOIS database, 304, **608–609**
- Whren v. United States* (automobile searches), 33
- Wigmore, John, 231
- Wilkes, John, 69, 480
- Wiley, Kathleen, 100
- Willis, Edwin, 284
- Window peeping, 312. *See also* Voyeurism
- Wireless access points (WAPs), 203
- Wireless computer connectivity (Wi-Fi), 111
- Wireless phone. *See* Cellular telephone
- Wiretap Act of 1968, 361
- Wiretapping, **609–613**; anti-wiretap statutes, **19–21**, 47; cellular telephones and, 89–90, 104; defined, 19, 104; exclusionary rule, 195–196; executive authority to permit, 350–351; by the FBI, 104, 132, 224; *Katz v. United States*, 32, 70, 74, 244, **317–319**, 327, 355, 361, 396, 456, 480, 490–491, 610; for law enforcement, 19–20, 102, 104–105, 132, 144; by National Security Agency, 350, 612; *Olmstead v. United States*, 72, 73–74, **357–362**; and pen registers and trap-and-trace devices compared, 204–205; prior consent for, 193–194; privacy tort, 312; provisions for in Internal Security Act of 1950, 297; roving, 20, 303, 586, 612; statutes affecting, 47, 398–400; on suspicion of terrorist activities, 12; under the USA PATRIOT Act, 20, 104, 303, 611–612
- Wolf v. Colorado* (search and seizure, states' obligation), 480
- The Woman Rebel*, 59
- Women and Economics*, 275
- Women and privacy, **613–615**; reproductive rights, 17, 396–397, **462–465**, 613
- Women's equality: abortion and, 250–251; consciousness-raising groups, 250, 277; cult of domesticity, 248–249; home, changing nature of, 277, 278; liberation movement, 247, 251; “personal is political,” 247, 251, 277, 400, 436; poor and marginalized women, 251; role of birth control in, 61, 250; sexual harassment, 247–248, 401, 411, **499–504**, 505, 614; sexual misconduct, 249, 501; suffrage, 248
- Wong Sun v. United States* (fruits of the poisonous tree doctrine), 293
- Woolf, Virginia, 614
- Workplace: privacy, **615–620**; reasonable expectation of privacy regarding, 98, 610; violence in, 37. *See also* Employees
- Work product doctrine, 440
- World Wide Web, 298, 399
- World Wide Web Consortium (W3C), 309
- Writs of assistance, 68, 69, 122, 479
- XCP (Extended Copy Protection) software, 301
- X-ray devices, 54, 489, 492, **621–622**
- X.509 identity certificates, 27
- Yates v. United States* (advocacy to commit violent act), 132, 283
- Zacchini v. Scripps-Howard Broadcasting* (celebrity parodies), 313
- Zachary's Law, 494
- Zimmermann, Phil, 388, 389
- ZIP Code Improvement Plan, 563
- ZIP codes, 553
- Zone of privacy, 126, 134–135, 219, 238, 250, 263, 278, 317, 462, 470, 589, **623–624**
- Zubulake v. UBS Warburg* (e-mail, retention of), 201
- Zurcher v. Stanford Daily* (mere evidence rule), 341

