AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

106th CONGRESS, 2nd SESSION/SENATE DOCUMENT 106–28

National Debate Topic for High Schools, 2000–2001

Resolved:
That the United States Federal Government Should Significantly Increase Protection of Privacy in One or More of the Following Areas: Employment, Medical Records, Consumer Information, Search and Seizure

NATIONAL DEBATE TOPIC FOR HIGH SCHOOLS, 2000-2001
Pursuant to 44 United States Code, Section 1333

Compiled by the Congressional Research Service
Library of Congress

U.S. Government Printing Office
Washington, DC 2001

Printed on recycled paper

44 U.S. CODE SECTION 1333

(a) The Librarian of Congress shall prepare compilations of pertinent excerpts, bibliographical references, and other appropriate materials relating to:

(1) the subject selected annually by the National University Extension Association as the national high school debate topic and

(2) the subject selected annually by the American Speech Association as the national college debate topic.

In preparing the compilations the Librarian shall include materials which in his judgment are representative of, and give equal emphasis to, the opposing points of view on the respective topics.

(b) The compilations on the high school debate topics shall be printed as Senate documents and the compilations on the college debate topics shall be printed as House of Representative documents, the cost of which shall be charged to the congressional allotment for printing and binding. Additional copies may be printed in the quantities and distributed in the manner the Joint Committee on Printing directs.

(Pub. L. 90-620, Oct. 22, 1968, 82 Stat. 1270.)

CONTENTS

Foreword	3
Introduction	5
Summary	5
General	6
Consumer Information	11
Employment	17
Medical Records	24
Search and Seizure	31
Technology	37

Foreword

The 2000-2001 high school debate topic is "Resolved: That the United States Federal Government Should Significantly Increase Protection of Privacy in One or More of the Following Areas: Employment, Medical Records, Consumer Information, Search and Seizure."

In compliance with 44 U.S. Code, section 1333, the Congressional Research Service of the Library of Congress prepared this bibliography to assist high school debaters in researching the topic. This bibliography is intended to assist debaters in the identification of further references and resources on the topic. In selecting items for this manual, the Congressional Research Service (CRS) has sampled a wide spectrum of opinions reflected in the current literature on this issue. No preference for any policy is indicated by the selection or positioning of articles cited, nor is CRS disapproval of any policy or article to be inferred from its omission.

Some of the U.S. government documents listed in this bibliography may be found in U. S. government depository libraries, which can be identified by local public or college libraries. The Library of Congress cannot distribute copies of these or other materials to debaters. This manual is also available on the GPO Access Home Page on the World Wide Web at http://www.access.gpo.gov.

The bibliography was prepared by Angela Napili, Information Resources Librarian and Melissa Burgess, Intern, Office of Information Resources Management, CRS under the direction of Sherry B. Shapiro, Information Resource Specialist. Production was made possible by Ann Eschete, Information Resources Assistant.

Good luck to each debater in researching, preparing and presenting arguments on this year's topic.

Daniel P. Mulhollan, Director
Congressional Research Service

RESOLVED: THAT THE UNITED STATES FEDERAL GOVERNMENT SHOULD SIGNIFICANTLY INCREASE PROTECTION OF PRIVACY IN ONE OR MORE OF THE FOLLOWING AREAS: EMPLOYMENT, MEDICAL RECORDS, CONSUMER INFORMATION, SEARCH AND SEIZURE

AN ANNOTATED BIBLIOGRAPHY ON THE 2000-2001 HIGH SCHOOL DEBATE TOPIC

Angela Napili,
Information Resources Librarian

Melissa Burgess, Intern
Office of Information Resources Management
Congressional Research Service

with the assistance of
Ann Eschete, Information Resources Assistant

February 2001

Introduction

The 2000-2001 high school debate topic is: "Resolved: That the United States Federal Government Should Significantly Increase Protection of Privacy in One or More of the Following Areas: Employment, Medical Records, Consumer Information, Search and Seizure."

This selective bibliography is intended to help debaters identify resources and references on the debate topic. The bibliography lists citations to books, congressional publications, and magazine and journal articles. The manual is divided into six subtopics: general, consumer information, employment, medical records, search and seizure, and technology. Debaters may look for these and related resources at their local high school, research, government depository, and public libraries.

Debaters may also wish to visit the speech and debate websites of the following:

> the National Federation of State High School Associations;
> *http://www.nfhs.org/NFISDA.htm*,
>
> the University of Kansas Government Documents Library;
> *http://kuhttp.cc.ukans.edu/cwis/units/kulib/docs/debate2000.html*, and
>
> the University of Michigan Documents Center,
> *http://www.lib.umich.edu/libhome/Documents.center/debate00.html.*

The above websites contain many links to documents and to websites of organizations active in the privacy debate.

Summary

The purpose of the debate manual is to provide students with a brief overview of information concerning the 2000-2001 national high school debate topic, **"Resolved: That the United States Federal Government Should Significantly Increase Protection of Privacy in One or More of the Following Areas: Employment, Medical Records, Consumer Information, Search and Seizure."** This bibliography includes citations to books, congressional publications, and magazine and journal articles. The compilation is not intended to supply complete coverage of the topic. Further research on the right of privacy in general, as well as each suggested subtopic, can be done at high school, research, depository, and public libraries.

Databases available through the Congressional Research Service's Office of Information Resources Management were used to prepare this bibliography.

The manual is divided into six subtopics: general, consumer information, employment, medical records, search and seizure, and technology.

The **general** section contains sources providing a broad overview of privacy issues and of the federal government's role protecting privacy.

The section on **consumer information** lists sources discussing the collection of personal information and the marketing of such information by commercial Internet companies, credit bureaus, and other businesses. Articles concerning the privacy controversy surrounding the 2000 Census are also included.

The **employment** section lists citations focusing on discrimination in the workplace due to genetic testing or physical examinations, the monitoring of employee activity through technological means, and mandatory drug testing.

The section on **medical records** concentrates on the increasing use of computer databases to maintain patient information and the vulnerability of such information to intrusion by other persons. This section also includes articles concerning the privacy of individuals with the HIV virus or AIDS disease.

The **search and seizure** section focuses on personal invasion by law enforcement officers using metal detectors, imaging devices, surveillance cameras, and other technology. The section also addresses privacy issues related to law enforcement officers' searches of homes or dormitories. In addition, several articles deal with the violation of privacy during traffic stops.

The section on **technology** provides a general overview of how technology is used either to protect or to invade one's privacy. Technologies discussed include the Internet, e-mail, encryption, cryptography, and cellular connections.

General

Alderman, Ellen. Kennedy, Caroline.
The right to privacy. New York, Knopf, 1995. 405 p.
Through discussions of particular court cases and interviews with individuals in privacy disputes, this book explores issues related to search and seizure, workplace privacy, and press freedom.

Banisar David. Davies, Simon.
Privacy and human rights 1999: an international survey of privacy laws & developments. Washington, Electronic Privacy Information Center, Privacy International, 1999. 180 p.
"This report reviews the state of privacy in over fifty countries around the world. It outlines the constitutional and legal conditions of privacy protection, and summarizes important issues and events relating to privacy and surveillance." Includes a country report for the United States.

Brin, David.
The transparent society: will technology force us to choose between privacy and freedom? Reading, Mass., Perseus Books, c1998. 378 p.
"No matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases." Instead of

advocating for more secrecy, Brin advocates "transparency -- the notion that we may all benefit by carefully increasing two-way information flows."

The End of privacy: the surveillance society. Economist, v. 351, May 1, 1999: 21-23.

"Despite a raft of laws, treaties and constitutional provisions, privacy has been eroded for decades. This trend is now likely to accelerate sharply . . . [I]n 20 years' time, will there be any privacy left to protect?"

Etzioni, Amitai.

The limits of privacy. New York, Basic Books, c1999. 280 p.

Etzioni argues that sometimes the individual right to privacy may be outweighed by the common good. The author weighs the public health, public safety, and privacy considerations related to medical records, national identification cards, community notification of released sex offenders, HIV testing of infants, and deciphering encrypted messages.

Givens, Beth. Fetherling, Dale.

The privacy rights handbook: how to take control of your personal information. New York, Avon Books, 1997. 335 p.

In layman's terms, authors from the Privacy Rights Clearinghouse describe whether and how consumers can protect privacy on the job, avoid wiretaps and eavesdropping, and monitor their credit reports, medical records, and government records.

Hendricks, Evan. Hayden, Trudy. Novick, Jack D.

Your right to privacy: a basic guide to legal rights in an information society. 2nd ed. Carbondale, Southern Illinois University Press, c1990. 184 p.

The Internet and the law. Nova law review, v. 23, winter 1999: whole issue (552-888 p.).

Partial contents.--Privacy in the digital age: work in progress, by Jerry Berman and Deirdre Mulligan.--Searching for security in the law of electronic commerce, by Amelia H. Boss.--The struggle for a new paradigm: protecting free speech and privacy in the virtual world of cyberspace, by Ira Glasser.

Contains reprints of magazine articles, book chapters, and reports on privacy issues. Includes writings on workplace privacy, medical records privacy, and issues related to large databases of consumers' personal information.

McLean, Deckle.

Privacy and its invasion. Westport, Conn., Praeger, 1995. 140 p.

"The purpose of this book is to identify some of the virtues of privacy, to recognize some of its flaws, and to convince the reader that privacy has been very important for a very long time . . ." Discusses the relationship between privacy and press freedom, and describes invasions of the privacy of African-Americans, sexual assault victims, and the poor.

McWhirter, Darien A. Bible Jon D.
Privacy as a constitutional right: sex, drugs, and the right to life. New York, Quorum Books, 1992. 206 p.
Explores the historical and philosophical foundations of constitutional privacy, or "the extent to which the United States Constitution protects people from unreasonable intrusions into their private lives."

Murphy, Richard S.
Property rights in personal information: an economic defense of privacy. Georgetown law journal, v. 84, July 1996: 2381-2417.
"While there are undoubtedly economic benefits to disclosure of information, including personal information, there are also substantial economic benefits to personal privacy."

Myers, Jennifer M.
Creating data protection legislation in the United States: an examination of current legislation in the European Union, Spain, and the United States. Case Western Reserve journal of international law, v. 29, winter 1997: 109-147.
"In light of the recent adoption of the E.U. Directive, it is imperative that the United States create comprehensive data protection legislation. Without comprehensive national legislation the United States may be precluded from receiving data. European nations have already expressed concern that the United States does not have data protection legislation. Besides hampering trade among nations, lack of comprehensive data protection permits intrusions into databases that can affect an individual's privacy and cause abuses to that individual."

Posner, Richard A.
The economics of privacy. American economic review, v. 71, May 1981: 405-409.
Reviews some economic research on privacy as "concealment of information." Points out similarities between fraud in the sale of goods and fraud in "selling" oneself in the labor market, argues that privacy can "reduce the efficiency of the marketplace," and discusses the possible economic effects of privacy legislation.

Privacy and the law: a symposium. George Washington law review, v. 67, June-Aug. 1999: 1097-1322.
Partial contents.--Privacy and the First Amendment right to gather news, by Rodney A. Smolla.--Balancing the rights of privacy and the press: a reply to Professor Smolla, by Erwin Chemerinsky.--Privacy and the public official: talking about sex as a dilemma for democracy, by Anita L. Allen.--The limits of privacy: culture, law, and public office, by William A. Galston.--The dark side of family privacy, by Barbara Bennett Woodhouse.--The distribution of Fourth Amendment privacy, by William J. Stuntz.--"How much justice can you afford?"--a response to Stuntz, by Carol S. Steiker.--Making the best of Fourth Amendment law: a comment on the distribution of Fourth Amendment privacy, by Louis Michael Seidman.

The Privacy law sourcebook 1999: United States law, international law, and recent developments. Edited by Marc Rotenberg. Washington, Electronic Privacy Information Center, 1999. 572 p.

A full-text compendium of privacy-related U.S. federal statutes, foreign legal documents, and international privacy agreements from the European Union, the OECD, and more. This book could be useful for comparing U.S. policies with those in other nations.

Privacy problem: special report. National journal, v. 32, Sept. 2, 2000: 2708-2724.

Discusses such topics as online privacy, medical records and the cost of privacy.

Regan, Priscilla M.
Legislating privacy: technology, social values, and public policy. Chapel Hill, University of North Carolina Press, c1995. 310 p.

The Right to privacy. Edited by Ellen Frankel Paul and others. New York, Cambridge University Press, 2000. 317 p.

Partial contents.--Privacy, control, and talk of rights, by R. G. Frey.--Privacy as a matter of taste and right, by Alexander Rosenberg.--Privacy and constitutional theory, by Scott D. Gerber.–Privacy and technology, by David Friedman.--The priority of private medical information, by Judith Wagner DeCew.--The right to privacy and the right to die, by Tom L. Beauchamp.--Can public figures have private lives? by Fredrick Shauer.

Rights to privacy. Edited by Robert Emmet Long. New York, H.W. Wilson, 1997. 179 p.

Rosen, Jeffrey.
Unwanted gaze: the destruction of privacy in America. New York, Random House, c2000. 274 p.

Examines sexual harassment law and its relation to privacy invasion in the workplace. Rosen argues that "law can sometimes do more harm than good when it tries to remedy invasions of privacy." Rosen also warns that as privacy erodes, individuals will often be judged out of context, based on isolated bits of personal information.

Why privacy matters. Wilson quarterly, v. 24, autumn 2000: 32-38.

"Privacy protects us from being judged out of context in a world of short attention spans. Genuine knowledge of another person is the culmination of a slow process of mutual revelation."

Rosenstiel, Tom. Dolittle, John.
Does a public person deserve a private life? World & I, v. 12, Dec. 1997: 68-75.

Tom Rosenstiel argues that "privacy is a right," while John Doolittle contends that "the public has rights too."

Smith, Janna Malamud.
Private matters: in defense of the personal life. Reading, Mass., Addison-Wesley Pub., c1997. 278 p.

Smith, Robert Ellis.
Our vanishing privacy: and what you can do to protect yours. Port Townsend, Wash., Breakout Productions, 1999. 132 p.

Strum, Philippa.
Privacy, the debate in the United States since 1945. Fort Worth, Tex., Harcourt Brace College Publishers, c1998. 225 p.
Contents.-- Privacy in the age of genetic information.-- Insecurity of social security numbers.-- Records of one's life.-- Bodily privacy and integrity.--Criminal justice system and privacy.--Big Brother really is watching you.--Privacy in the workplace – Is privacy dead?

Sykes, Charles J.
The end of privacy. New York, St. Martin's Press, 1999. 282 p.
Sykes tries to document "the attack on privacy" by discussing medical records, workplace privacy, "the exposure culture" and "the tell-all society," and how government and the courts have handled privacy issues.

U.S. Congress. House. Committee on Government Reform and Oversight.
A citizen's guide on using the Freedom of Information Act and the Privacy Act of 1974 to request government records; first report. Washington, G.P.O., 1997. 76 p. (Report, House, 105th Congress, 1st session, no. 105-37).
"In the closing days of the 104th Congress, the Senate and the House of Representatives completed action on the Electronic Freedom of Information Act Amendments of 1996. The President signed this legislation into law on October 2, 1996, when it became Public Law 104-231. With the exception of two sections, these amendments become effective 190 days after enactment of the legislation. The other two sections become effective 1 year after enactment. Because the 1996 amendments change some FOIA access rights, this seventh edition of the Guide was prepared to reflect these modifications. It also contains bibliography additions and editorial changes."

U.S. Congress. House. Committee on Ways and Means. Subcommittee on Social Security.
Social Security Administration's website. Hearing, 105th Congress, 1st session. May 6, 1997. Washington, G.P.O., 1998. 106 p.
"Serial 105-27"

U.S. Congress. Senate. Committee on Governmental Affairs.
H.R. 1271–the Family Privacy Protection Act of 1995. Hearing, 104th Congress, 1st session on H.R. 1271. Nov. 5, 1995. Washington, G.P.O., 1997. 196 p. (Hearing, Senate, 104th Congress, 1st session, S. Hrg. 104-783)

Warren, Samuel D. Brandeis, Louis D.
The right to privacy. Harvard law review, v. 4, Dec. 15, 1890: 193-220.
A landmark article arguing for the right "to be left alone." One of the earliest discussions of privacy rights in American law.

Whitney, Sally.
The great privacy debate. Best's review, v. 101, June 2000: 134-141.
Gives an overview of federal legislation regarding medical records and financial records privacy.

Zuckerman, M. J.
Chances are, somebody's watching you. USA today, Nov. 30, 2000: A1.
This article discusses legal and policy issues related to camera surveillance of public spaces.

Consumer Information

Bennett, Robert A.
The burden of privacy. U.S. banker, v. 110, July 2000: 54-58.
"Weighty privacy regulations afflict not only financial companies, but many other businesses. But no relief's in sight, as the public strongly favors privacy protection."

Cavoukian, Ann. Tapscott, Don.
Who knows: safeguarding your privacy in a networked world. New York, McGraw-Hill, c1997. 233 p.

Clausing, Jeri.
Europe and U.S. reach data privacy pact; the deal involves personal information gathered on foreign consumers. New York times, Mar. 15, 2000: C6.

Cuccinelli, Ken.
Consumer privacy? It's a cyber cinch. Public utilities fortnightly, v. 137, Nov. 15, 1999: 22-34.
With a deregulating market, utilities must share their consumer data with energy marketers in their territories. The more information energy marketers have about consumers, the better the products, prices and payment plans they can offer. This information, however, may include sensitive details about a consumer's finances and habits. Regulators have tried to strike a balance among conflicting interests - the consumer's right to privacy, the burden imposed on utilities to release customer information available, and the needs

of marketers for real information to create viable offerings in a timely fashion. It is argued that the encrypted CD-ROM is the most cost-effective way to transfer consumer data to energy marketers. The utility provides marketers with a CD-ROM with specific consumer data encrypted. When the consumer gives the marketer his password, it accesses the consumer's information. The encrypted CD-ROM is a quick and cost-efficient way for utilities to supply information while protecting their customers' privacy.

Culnan, Mary J.
Georgetown Internet privacy policy survey: report to the Federal Trade Commission. Washington, McDonough School of Business, Georgetown University, 1999. 96 p.
A survey of 361 websites to determine "the extent to which commercial Web sites have posted privacy disclosures based on fair information practices."

Privacy and the top 100 web sites: report to the Federal Trade Commission. Washington, Online Privacy Alliance, 1999. 11 p.

Donlon, J. P. Lynch, Michael W.
Privacy at stake. Chief executive, Nov. 2000: 54-68.
"Access to personal data and how it's handled has always been a sensitive issue, but the development of the Internet has heightened concern. Yet, information is the lifeblood of the modern economy. The question is how businesses can recognize the individual's right to privacy while retaining the ability to collect and use information intelligently."

Eye at the keyhole: privacy in the digital age. Washington post, Mar. 8, 1998: A01.
Contents.--Data firms getting too personal, by Robert O'Harrow. --Governments find information pays, by Rajiv Chandrasekaran. --Databases start to fuel consumer ire, by John Schwartz.

Garfinkel, Simson.
Privacy and the new technology: what they do know can hurt you. Nation, v. 270, Feb. 28, 2000: 11.

Gruenwald, Juliana.
Who's minding whose business on the Internet? CQ weekly, v. 56, July 25, 1998: 1986-1990.
"Congress is struggling with how to deal with the emerging technology of the Internet and protecting the privacy of consumers who are using it."

Jennings, Charles. Fena, Lori.
The Hundredth window: protecting your privacy and security in the age of the Internet. New York, Free Press, 2000. 278 p.

The authors discuss many ways that consumers' personal information is collected and used without their knowledge. "Unless you are very careful—and fairly skillful—the coming 'digital metabolism' of a billion interconnected computers will soon be on your trail, tracking you like a hungry bloodhound."

McColl, Hugh L.
Communities of trust: the issue of privacy. Vital speeches of the day, v. 66, July 1, 2000: 557-560.
"A speech to the Society of American Business Editors and Writers by the chairman and chief executive officer of Bank of America. McColl states: 'Many lawmakers in the country seem convinced that their proposed remedies for customer privacy concerns will soothe our fears, banish our doubts and cast out our demons. Frankly, I'm not convinced. I think the privacy issue is more complex than politicians, consumer activists - and even some reporters - believe. I think the potential for negative unintended consequences is huge. And I think that, as usual, if we act rashly we'll come to regret it.'"

Neal, Douglas. Morgan, Nicholas.
Our data, our selves. Wilson quarterly, v. 24, autumn 2000: 51-57.
"Rather than trying to set abstract standards for privacy in the marketplace, we can begin to think about personal information as personal property."

O'Harrow, Robert.
Laws on use of personal data form a quilt with many holes. Washington post, Mar. 9, 1998: A12.
"Many civil libertarians and privacy advocates say the growing technical capability to gather and collate personal data is overwhelming what once were preserves of privacy."

Picking up on 'cookie' crumbs; web sites want to track your every move. Should you let them? Washington post, Mar. 9, 1998: F25.
"Cookies were originally intended 'to help computers on the other end recognize when a single person had arrived at a web site.' Now cookies can linger on your browser and keep close tabs on you. Includes web site which tells "more about what cookies are used for, and how to set your computer to reject them."

Who's got your number? Data access feeds a new breed of crime. Washington post, Mar. 10, 1998: A08.
"Unsettling truth about life in the digital age: sensitive personal information once assumed to be private and secure is more available and vulnerable to abuse than ever before."

Prewitt, Kenneth. Pear, Robert.
Privacy concerns threaten a 'backlash,' Census director fears. New York times, Apr. 2, 2000: 19.

Privacy policies on-line: improving for consumers. Consumers' research, v. 82, Oct. 1999: 26-30.
Presents excerpts from the Federal Trade Commission's review of privacy issues posed by the on-line collection of personal information.

Punch, Linda.
Big brother goes online. Credit card management, v. 13, June 2000: 22-32.
"Consumers' and lawmakers' worries about privacy 'could spell trouble for the [credit] card industry in its quest to capture e-commerce market share.'"

Rosen, Cheryl. Bacheldor, Beth.
The politics of privacy protection. InformationWeek, no. 795, July 17, 2000: 40-48.
Describes recent political developments related to online privacy legislation and self-regulation. Authors also report that in a Forrester Research survey of 50 companies, 66% of respondents answered "No" to the question "Should the government set online privacy policies?"

Shapiro, Andrew L.
Privacy for sale: peddling data on the Internet. Nation, v. 264, June 23, 1997: 11-12, 15-16.
Warns that "the creeping ubiquity of digital computer technology has ushered in a major industry of high-tech data pushers who are dedicated to gathering and selling personal information about practically everyone, mostly for marketing purposes. (Privacy experts estimate that the average American is profiled in at least twenty-five, and perhaps as many as 100, databases.)

Singleton, Solveig.
Privacy as censorship: a skeptical view of proposals to regulate privacy in the private sector. Washington, Cato Institute, 1998. 32 p. (Policy analysis no. 295).
"This paper explores the tangled moral and economic issues surrounding the collection and transfer of information about consumers by businesses using the Internet and other networks. It concludes that we have little to fear from private collection and transfer of consumer information; our attention should shift to threats from government databases."

Smith, Frances B.
Internet taxation schemes threaten consumers' privacy. Consumers' research, v. 82, Oct. 1999: 34-35.
"There is a real danger that in their zeal to collect sales taxes, some states and local jurisdictions may force vendors to require that their Internet

customers disclose personal information for tax liability and collection purposes."

Special issue on privacy and ethical issues in database/interactive marketing and public policy. Journal of public policy and marketing, v. 19, spring 2000: whole issue (154 p.).

Partial contents.--Privacy and ethical issues in database/interactive marketing and public policy: a research framework and overview of the special issue, by George R. Milne.--Consumer online privacy: legal and ethical issues, by Eve M. Caudill and Patrick Murphy.--Protecting privacy online: is self-regulation working? by Mary J. Culnan.--Marketing without consent: consumer choice and costs, privacy, and public policy, by Ross D. Petty.--Internet privacy and security: an examination of online retailer disclosures, by Anthony D. Miyazaki and Ana Fernandez.--Dimensions of privacy concern among online consumers, by Kim Bartel Sheehan and Mariea Grubbs Hoy.

Stepanek, Marcia.

None of your business: customer data were once gold to e-commerce. Now, companies are paying a price for privacy jitters. Business week, no. 3687, June 26, 2000: 78-80.

Considers upcoming privacy legislation and its effects on the stock market and company profits.

Tedeschi, Bob.

Giving consumers access to the data collected about them online. New York times, July 3, 2000: C6.

"When the online privacy debate reached its peak earlier this year, the watchwords were 'notice' and 'choice.' Consumer groups demanded that online advertising companies like DoubleClick give consumers more notice when tracking their behavior, and give them the choice to avoid such tracking. But there are two other core privacy principles: giving consumers 'access' to data collected on them and providing them with the 'security' that the data is kept private. The first two terms continue to be volleyed back-and-forth by legislators scoring points in this year's campaign, but the latter two have received scant air time."

Tynan, Daniel.

Privacy 2000: in web we trust? PC world, v. 18, June 2000: 103-116.

An overview of privacy practices and abuses on the World Wide Web, and recent lawsuits related to consumer privacy.

U.S. Board of Governors of the Federal Reserve System.

Interagency financial institution web site privacy survey report. Washington, The Board, 1999. 60 p.

A survey "to determine the extent to which financial institution Web sites posted privacy policies and information practice statements." The report makes no policy recommendations.

Report to the Congress concerning the availability of consumer identifying information and financial fraud. Washington, The Board, 1997. 36 p.
"In considering whether any legislation is desirable, the Congress must carefully evaluate whether the availability of sensitive information poses a sufficient risk to consumers and institutions to justify new laws . . . Care should be taken not to impair the flow of information that is crucial for legitimate purposes."

U.S. Congress. House. Committee on Banking and Financial Services. Subcommittee on Financial Institutions and Consumer Credit.
Consumer financial privacy. Hearing, 105th Congress, 1st session. Sept. 18, 1997. Washington, G.P.O., 1997. 512 p.
"Serial no. 105-33"

U.S. Congress. House. Committee on Commerce. Subcommittee on Telecommunications, Trade, and Consumer Protection.
Electronic commerce: the current status of privacy protections for online consumers. Hearing, 106th Congress, 1st session. July 13, 1999. Washington, G.P.O., 1999. 127 p.
"Serial no. 106-39 "

Recent developments in privacy protections for consumers. Hearing, 106th Congress, 2nd session. Oct. 11, 2000. Washington, G.P.O., 2000. 107 p.
"Serial no. 106-160"

U.S. Congress. House. Committee on Ways and Means. Subcommittee on Social Security.
Protecting privacy and preventing misuse of the social security number. Hearing, 106th Congress, 2nd session. July 17, 2000. Washington, G.P.O., 1999. 37 p.
"Serial no. 106-43"

U.S. Federal Trade Commission.
Privacy online: fair information practices in the electronic marketplace: a report to Congress. Washington, The Trade, 2000. 208 p.
"A report based on a survey of commercial websites' information practices. The report concludes that, 'while there will continue to be a major role for industry self-regulation in the future, the Commission recommends that Congress enact legislation that, in conjunction with continuing self-regulatory programs, will ensure adequate protection of consumer privacy online.'"

U.S. General Accounting Office.
Identity fraud: information on prevalence, cost, and Internet impact is limited. Washington, G.A.O., 1998. 63 p.

"GAO/GGD-98-100 BR", "B-279537"
"This document provides information on (1) law enforcement's responsibilities for investigating identity fraud and the difficulties in tracking such crime; (2) statistics or other data showing the prevalence of identity fraud; (3) the costs of identity fraud; and (4) identity fraud and the Internet, including the status of self-regulation by computerized database services that collect and disseminate personal identifying information."

Wang, Huaiqing. Lee, Matthew K.O. Wang, Chen.
Consumer privacy concerns about Internet marketing. Communications of the ACM, v. 41, Mar. 1998: 63-70.
Discusses the roles of government, business, and consumers in protecting individual privacy, advocating that "privacy enhancing technologies, industry self-regulations, legislation, and legal enforcement regimes be coordinated." Authors also categorize and describe different types of consumer privacy concerns.

Whitaker, Reg.
The end of privacy: how total surveillance is becoming reality. New York, New Press, 1999. 195 p.
Explores the impact of surveillance technology on political power. Also discusses how consumers willingly give up their personal information and privacy for the sake of convenience.

Zurier, Steve. Smith, Robert Ellis. Wientzen, H. Robert.
Privacy sound off: regulation vs. self-regulation. InternetWeek, no. 773, Sept. 21, 1998: 35.
"Privacy advocates say the government must pass tough new laws to protect children, safeguard medical records and combat identity theft. The business community, which supports targeted privacy laws, fears legislation could stifle e-commerce."

Employment

American Management Association.
2000 AMA survey: workplace monitoring & surveillance. New York: American Management Association, 2000. This is available on the Web at: *http://www.amanet.org/research/pdfs/monitr_surv.pdf* (as of Jan. 29, 2001)
"Nearly three-quarters of major U.S. firms (73.5%) record and review employee communications and activities on the job, including their phone calls, e-mail, Internet connections, and computer files." Reasons given for surveillance include: performance review, legal compliance, legal liability, and productivity measures.

2000 AMA survey on workplace testing: medical testing. New York: American Management Association, 2000. This is available on the web at: *http://www.amanet.org/research/pdfs/medicl2.0.pdf* (as of Jan. 29, 2001)

"Seventy-one percent of major U.S. firms require medical examinations of new hires, current employees, or both."

Anton, Gary. Ward, Joseph J.

Every breath you take: employee privacy rights in the workplace--an Orwellian prophecy come true? Labor law journal, v. 49, Mar. 1998: 897-911.

Article focuses on several hot issues concerning employee privacy in the workplace in Florida, including the topic of co-worker dating, the privacy of employee e-mail and computer files, employer attempts to control off-duty activity of employees, and employee background checks.

Bennett, Steven C. Locke, Scott D.

Privacy in the workplace: a practical primer. Labor law journal, v. 49, Jan. 1998: 781-787.

"This article briefly addresses the concept of privacy in the workplace, explores workplace limitations on the right of privacy, and notes forms of employer action that may constitute invasions of employee privacy. The article concludes with advice to employers on means to ensure that invasion of privacy claims are minimized."

Caldwell, Bernice.

Genetic testing advances: privacy retreat? Employee benefit plan review, v. 54, Oct. 1999: 6-10.

While genetic information will allow doctors to win the fight against life-threatening illness and disease, it also poses a serious threat to privacy, civil liberties, and discrimination in employment and insurance. Entering the 21st century, genetic information may well become a major constitutional issue in regard to how it can be used and who should have access to it. Currently, about 3/4 of major U.S. firms require medical testing of new hires, current employees, or both. However, because of the danger that the secrets hidden in people's genes will someday be used against them, genetic testing should be kept out of the workplace until some basic principles have been established.

Carlson, Tucker.

Linda Tripp's Pentagon papers. Weekly standard, v. 3, Mar. 30, 1998: 20-22.

"The federal government is famously reluctant to give reporters confidential information about its employees. How did Jane Mayer, who wrote the Linda Tripp story for the New Yorker, get access to information in Tripp's personnel file?"

Cranford, Michael.
Drug testing and the right to privacy: arguing the ethics of workplace drug testing. Journal of business ethics, v. 17, Dec. 1998: 1805.
As drug testing has become increasingly used to maximize corporate profits by minimizing the economic impact of employee substance abuse, numerous arguments have been advanced which draw the ethical justification for such testing into question, including the position that testing amounts to a violation of employee privacy by attempting to regulate an employee's behavior at home, outside the employer's legitimate sphere of control. It is first proposed that an employee's right to privacy is violated when personal information is collected or used by the employer in a way which is irrelevant to the terms of employment. It is argued that drug testing is relevant and therefore ethically justified within the terms of the employment agreement, and therefore does not amount to a violation of an employee's right to privacy.

Dean, Lisa. McCullagh, Declan.
Q: Should employers have to reveal electronic-surveillance activities? Insight on the news, v. 16, Sept. 11, 2000: 40-43.
"Yes: They should be able to guard against misuse of the Internet on company time." "No: It is not good business to force companies to disclose their actions to employees."

Dickinson, Philip D.
Employee privacy rights & wrongs. Nashville, M. Lee Smith Publishers, 1996. 72 p.

Genetic information in the workforce. Labor law journal, v. 49, Feb. 1998: 867-876.
"Recent advances in genetic research have made it possible to identify the genetic basis for human diseases, opening the door to individualized prevention strategies and early detection and treatment. These advances hold much promise for improving health. However, genetic information can also be used unfairly to discriminate against or stigmatize individuals on the job . . . . This report demonstrates why American workers deserve federal legislation to protect them from genetic discrimination in the workplace."

Goldberg, Ilene. Sprotzer, Ira.
Workplace privacy: HIV testing, disclosure, and discrimination. Health care manager, v. 17, Dec. 1998: 21-27.
HIV testing and the disclosure of HIV-related information pose questions of privacy and public policy that are of concern in both public-and private-sector workplaces. Public-sector employees have constitutional protection from discrimination on the basis of their HIV-positive status. The Americans with Disabilities Act is an important source of protection for private-sector employees. There are also other federal laws that provide protection from discrimination. However, the scope of these laws is unclear. Similarly, while some state legislators have attempted to set standards to

protect the privacy of HIV-positive employees, laws vary from state to state. Case precedent is also inconsistent. Some current issues regarding HIV testing, employee privacy and protection from discrimination are discussed.

Guernsey, Lisa.
You've got inappropriate mail; monitoring of office e-mail is increasing. New York times, Apr. 5, 2000: C1.

Higgins, Michael.
High tech, low privacy. American Bar Association journal, v. 85, May 1999: 52-57.
"With employers electronically peering into workers' productivity and behavior, the line between being free to run a business and being free from personal prying is filled with legal static."

Hornak, Mark R.
New law expands paperwork burden and liability threat for employers. Washington, Washington Legal Foundation, 1998. 4 p. (Legal backgrounder, v. 13, no. 6)
Says that under the Consumer Credit Reporting Reform Act of 1996, "employers must now provide all applicants and employees with separate written disclosure statements, and secure their written authorization, prior to obtaining a background report about them from a reporting agency. Significant additional disclosures are now to be made both before and after an employer takes any 'adverse action' based on such reports."

Hubbartt, William S.
The new battle over workplace privacy: how far can management go? What rights do employees have? Safe practices to minimize conflict, confusion, and litigation. New York, AMACOM, 1998. 271 p.
Published by a division of the American Management Association, this book explains why employers may want to increase surveillance of employees, and tries to guide managers in developing legal and effective practices related to employee privacy. The book discusses employee monitoring, drug and medical testing, pre-employment checks, dress codes, searches, off-duty behavior, and related issues.

Individual rights in the corporation: a reader on employee rights. Edited by Alan F. Westin and Stephan Salisbury. New York, Pantheon Books, c1980. 473 p.

Kainen, Burton. Myers, Shel D.
Turning off the power on employees: using surreptitious tape-recordings and e-mail intrusions by employees in pursuit of employer rights. Labor law journal, v. 48, Apr. 1997: 199-213.
"This paper seeks to extend the debate on privacy in the workplace to a discussion of an employer's rights and remedies when an employee has engaged in surreptitious tape-recordings or computer e-mail intrusions. We

will examine how employers can affirmatively use such conduct to discipline employees, to defend against charges of wrongdoing, to limit damages under the after acquired evidence rule, and to seek relief against employees under a variety of legal theories, including statutory wiretapping or privacy violations, common law invasion of privacy claims, breach of the implied covenant of good faith claims, and for breach of the duty of loyalty."

Kaplan, Joseph V. Mahoney, John P.
Reckless disregard: intentional and willful violations of the Privacy Act's investigatory requirements. Federal lawyer, v. 44, May 1997: 38-44.
"In a case that serves as a strong wake-up call to federal agencies, the U.S. District Court for the District of Columbia recently ruled in Dong v. Smithsonian Institution, that a federal agency was liable for damages to reputation and attorneys fees for recklessly disregarding often-ignored provisions of the Privacy Act by improperly conducting an investigation into allegations of employee misconduct. Agencies have obligations under the Privacy Act when conducting employee investigations. The Dong case serves as an example of the consequences of violating those obligations."

Koch, Kathy.
Drug testing: does it deter drug abuse? CQ researcher, v. 8, Nov. 20, 1998: whole issue (1001-1024 p.).
"Drug testing has become a major weapon in the war on drugs. Nearly three-quarters of America's biggest companies require job applicants to undergo urinalysis -- up from only 21 percent a decade ago. Proponents say drug testing protects public safety and deters drug use, but opponents say neither can be proved. Until recently, most companies only tested job applicants and public-safety employees. But now employers randomly test all employees. Some state and local governments require random testing of public employees, high school students participating in after-school activities, prisoners and welfare and student-loan recipients. Many employee groups and civil libertarians see such expanded drug testing as a dangerous erosion of Americans' constitutional right to privacy."

Martucci, William C. Place, Jeffrey M.
Privacy rights and employee communication in the workplace. Employment relations today, v. 25, summer 1998: 109-120.
Most employers can probably find a variety of reasons for wanting to monitor the content and frequency of employee communication in, or originating from, the workplace. An employer investigating charges of sexual harassment has a strong incentive to determine whether alleged unlawful communication has taken place and to prevent any reoccurrence. A wide variety of motivations for communication monitoring exist, ranging from theft prevention to external security. However, employers that engage in monitoring activity may run afoul of state and federal laws created to protect individual privacy. In many cases, state statutes or common law include protections that go beyond those currently found at the federal level. A brief overview of federal law and state regulation of employer monitoring of

employee activity is presented in three areas: telephone communication, electronic messaging, and oral conversation.

O'Meara, Kelly Patricia.
Corporate image vs. right to privacy. Insight on the news, v. 16, June 19, 2000: 17-19.
Discusses companies' concerns with their employees' off-duty activities.

Privacy in the workplace: when employer-employee rights collide. New York, Alexander Hamilton Institute, c1987. 277 p.

Rothenberg, Karen.
Genetic information and the workplace: legislative approaches and policy challenges. Science, v. 275, Mar. 21, 1997: 1755-1757.
Deals with the legislative aspects of genetic predispositions toward occupational disease and employment.

Rothstein, Mark A. Gelb, Betsy D. Craig, Steven G.
Protecting genetic privacy by permitting employer access only to job-related employee medical information: analysis of a unique Minnesota law. American journal of law and medicine, v. 24, no. 4, 1998: 399-416.
"Legislation restricting employer access to irrelevant medical information will be more effective than laws making the use of genetic information unlawful. Until meaningful medical privacy legislation is enacted, individuals will continue to be reluctant to undergo genetic testing in the clinical setting because they fear the possible uses of the information."

Seumas, Miller. Weckert, John.
Privacy, the workplace, and the Internet. Journal of business ethics, v. 28, Dec. 2000: 255-265.
"The paper examines the general monitoring of work, and the monitoring of email, listservers and the World Wide Web. It is argued that many of the common justifications given for this surveillance and monitoring do not stand up to close scrutiny."

Sinton, Peter.
Big brother's watching the store: Internet surveillance services help business owners keep tabs on customers and employees - and raise concerns about privacy rights. San Francisco chronicle, July 12, 2000: C1.
Discusses ways that surveillance systems can help reduce shoplifting and employee theft, increase profits, and "help ensure safety and promote good behavior" among employees. Includes statistics on financial losses due to retail theft. The article also discusses privacy concerns related to workplace surveillance.

Skidmore, David A., Jr.
Caveat employer: disclosure of private facts. Federal lawyer, v. 44, Mar.-Apr. 1997: 50-54.

"The private facts tort protects individuals from public disclosure of truthful, private information. Employees are bringing suit against their employers based on the private facts tort in a variety of contexts. With the increased ease of gathering information, employers must be careful about what information they gather and more importantly, what information is disclosed."

Smith, William C.
Hypothetically handicapped. American Bar Association journal, v. 85, June 1999: 32-33.
Explains why the EEOC sued an industry for refusing to hire people based on a pre-employment physical which led to "conjecture about workers' future health."

Sullivan, Andrew.
Promotion of the fittest. New York times magazine, July 23, 2000: 16-18.
"The new science of genetic screening is so precise that it might just give workplace discrimination a good name."

Swanson, K. C.
New test, new concerns. National journal, v. 29, Jan. 4, 1997: 27-29.
"Though 13 states now offer varying levels of protection against genetic discrimination in the workplace or the insurance market, some specialists argue that the federal government should weigh in and provide strong, uniform safeguards."

U.S. Congress. House. Committee on Government Reform and Oversight. Subcommittee on National Security, International Affairs, and Criminal Justice.
Corporate America and the war on drugs: the importance of drug testing. Hearing, 104th Congress, 2d session. June 27, 1996. Washington, G.P.O., 1997. 156 p.
"Focus is on the role of corporate America and the importance of drug testing in the workplace as a means of combating the rising drug epidemic."

Verkerke, J. Hoult.
Legal regulation of employment reference practices. University of Chicago law review, v. 65, winter 1998: 115-178.
"Section I describes the nature of the problem and existing legal rules affecting the flow of information in the labor market. Section II develops a theoretical account of the interaction between employee turnover and employers' access to information about employee productivity. Section III applies this framework to the regulation of employment reference practices."

Medical Records

Ainslie, Donald C.
Questioning bioethics: AIDS, sexual ethics, and the duty to warn. Hastings Center report, v. 29, Sept.-Oct. 1999: 26-35.
"Bioethicists have tended to argue that if someone with HIV does not inform his sexual partners of this fact, health professionals who are aware of this situation ought (in most circumstances) to warn those partners. But according to the safer sex ethic accepted by many in the gay community, those who are HIV positive are not required to disclose their status to their sexual partners so long as they practice safer sex. Discussion of the duty to warn in bioethics has occurred largely in isolation from the discussion of sexual responsibility among those whom such warnings would affect."

Allen, Arthur.
Medical privacy? Forget it! Medical economics, v. 75, May 11, 1998: 151-152, 157-158, 160, 165-166.
"The right to doctor-patient confidentiality is under attack by computer technology, managed care, and genetic science. Can it survive the onslaught?"

American Management Association.
2000 AMA survey on workplace testing: medical testing. New York: American Management Association, 2000. This is available on the Web at: *http://www.amanet.org/research/pdfs/medicl2.0.pdf* (as of Jan. 29, 2001)
"Seventy-one percent of major U.S. firms require medical examinations of new hires, current employees, or both."

Angell, Marcia.
The Supreme Court and physician-assisted suicide--the ultimate right. New England journal of medicine, v. 33, Jan. 2, 1997: 50-53.
"If the Supreme Court lets the decisions stand, physicians in 12 states, which include about half the population of the United States, would be allowed to provide the means for terminally ill patients to take their own lives, and the remaining states would rapidly follow suit. Not since Roe v. Wade has a Supreme Court decision been so fateful."

Appelbaum, Paul S.
Threats to the confidentiality of medical records–no place to hide. JAMA [Journal of the American Medical Association], v. 283, Feb. 9, 2000: 795.
Regulations proposed by the Department of Health and Human Services covering access to medical records do not go far enough in protecting patients' privacy. As of February, 2000, no federal legislation exists to protect medical records and many state laws are inadequate. The proposed regulations would allow many agencies, companies, and individuals to access medical records without the patient's consent. This would even include lawyers and law enforcement officers. One bright spot in the regulations is

that medical records could not be sold or rented for marketing purposes without the patient's consent, says this editorial.

Burr, Chandler.
The AIDS exception: privacy vs. public health. Atlantic monthly, v. 279, June 1997: 57-61, 64-67.
Contends that largely in order to accommodate civil rights concerns the "practice of traditional public health has been to a great degree suspended for acquired immune deficiency syndrome and for human immunodeficiency virus, the virus that causes it. Although various traditional public-health steps are being taken against AIDS and HIV, in differing combinations from state to state, the result is a chaotic patchwork--one that is inadequate, a growing number of critics say, to the task of containing and eradicating AIDS."

Carter, Patricia I.
Health information privacy: can Congress protect confidential medical information in the "Information Age"? William Mitchell law review, v. 25 winter 1999: 223-286.
"This article will review the various sources of legal rights to confidentiality of individual health care information and will conclude that the current complex patchwork of federal and state protections is insufficient in this age of information technology. Comprehensive federal legislation will be required to meet the challenge of maintaining the confidentiality of individually identifiable medical information, while still making appropriate information available for necessary and valuable public uses."

Cohen, Jordan J.
Archival research versus privacy rights: finding the right balance. Academic medicine, v. 73, Oct. 1998: 1081.
"How private should medical information be? That question has leapt to the front ranks of the controversy over 'patient rights' legislation, as law-makers attempt to respond to alleged abuses in the managed care industry and to the widespread public alarm about the potential misuse of medical information."

Colfax, Grant Nash. Bindman, Andrew B.
Health benefits and risks of reporting HIV-infected individuals by name. American journal of public health, v. 88, June 1998: 876-879.
"Review the benefits and risks of name reporting of persons infected with HIV. Public health departments have linked name reporting with medical referrals, risk reduction counseling, and partner notification programs . . . . Whether name reporting actually improves individual or public health, therefore justifying the increased risk of loss of confidentiality and possibly reduced testing rates, remains unknown."

Etzioni, Amitai.
Medical records: enhancing privacy, preserving the common good. Hastings center report, v. 29, Mar.-Apr. 1999: 14-27.

"The justification for providing access to medical records 'is that doing so benefits the public by securing public safety, controlling costs, and supporting medical research.' Argues that we 'can achieve the common good while better protecting privacy by making institutional changes in the way information is maintained and protected.'"

Fuller, B.P., and others.
Privacy in genetics research. Science, v. 285, Aug. 27, 1999: 1359-1361.
Contains policy recommendations of the National Action Plan on Breast Cancer. Authors discuss recommendations to restrict the use of genetic information in health insurance and in the workplace.

Genetic secrets: protecting privacy and confidentiality in the genetic era. Edited by Mark A. Rothstein. New Haven, Yale University Press, c1997. 511 p.
Partial contents: Informed consent and genetic research, by Ellen Wright Clayton.--DNA data banks, by Jean E. McEwen.--The law of medical and genetic privacy in the workplace, by Mark A. Rothstein.--Justice and genetics: privacy protection and the moral basis of public policy, by Madison Powers.--Laws to regulate the use of genetic information, by Philip R. Reilly.--Genetic secrets: a policy framework, by Mark A. Rothstein.

George Washington University.
Protecting the confidentiality of health information. Washington, National Health Policy Forum, 1998. 7 p. (Issue brief no. 724)
The forum concentrates on three key issue areas: "controlling access to health information, conducting research, and preempting state laws."

Goldman, Janlori. Hudson, Zoe.
Exposed: a health privacy primer for consumers. Washington, Georgetown University, Health Privacy Project, 1999. 16 p.
Briefly describes the current state of laws for protecting privacy, warns consumers of who can access their personal health information, cites polling data on Americans' privacy concerns, and includes a bibliography for further research.

Virtually exposed: privacy and e-health. Health affairs, v. 19, Nov.-Dec. 2000: 140-148.
"Privacy concerns are keeping consumers from reaping the full benefit of online health information."

Goldman, Janlori. Hudson, Zoe. Smith, Richard M.
Privacy: report on the privacy policies and practices of health web sites. Oakland, California Health Care Foundation, 2000. 98 p.
Among the findings: "Health Web sites recognize consumers' concern about the privacy of their personal health information and have made efforts to establish privacy policies; however, the policies fall short of truly

safeguarding consumers . . . There is inconsistency between the privacy policies and the actual practices of health Web sites."

Gostin, Lawrence.
Health care information and the protection of personal privacy: ethical and legal considerations. Annals of internal medicine, v. 127, no. 8, part 2, Oct. 15, 1997: 683-690.
"As the values and effectiveness of health care in the United States are being considered, citizens must acknowledge that one of the burdens of achieving cost-effective, accessible health care might be some loss of personal privacy. In exchange, the government is obliged to create reasonably strong assurances of fair practices in the collection and use of information."

Gostin, Lawrence O. Webber, David W.
The AIDS Litigation Project: HIV/AIDS in the courts in the 1990s, part 2. AIDS & public policy journal, v. 13, spring 1998: 3-19.
"The AIDS Litigation Project presents cases reported in the state and federal courts from 1991 to 1997 involving the AIDS epidemic. Part 1 of this study presented cases involving the duties of the government and individuals in preventing HIV transmission. Part 2 examines cases involving the rights of individuals, as they come into conflict with the power of government or the interests of other individuals."

Hall, Mark A. Uhlmann, Wendy R.
When genes are decoded, who should see the results? New York times, Feb. 29, 2000: D7.
"Two experts discuss the issue and discuss the need for safeguards to prevent use of genetic information in hiring, promoting or dismissal of workers."

Hodge, James G. Gostin, Lawrence O. Jacobson, Peter D.
Legal issues concerning electronic health information: privacy, quality, and liability. JAMA [Journal of the American Medical Association], v. 282, Oct. 20, 1999: 1466-1471.
Argues that increased privacy protections can improve the quality and reliability of medical information.

Improving the privacy and security of electronic health information. Academic medicine, v. 72, June 1997: 522-523.
"The prospect of storing health information in electronic form raises concerns about patients' privacy and data security. The National Library of Medicine, the Warren Grant Magnuson Clinical Center of the National Institutes of Health, and the Massachusetts Health Data Consortium asked the Computer Science and Telecommunications Board of the National Research Council (NRC) to examine ways of maintaining the privacy and security of electronic health information. As a result, in October 1995, the NRC formed the Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure. For 17 months this

committee visited with health care organizations and representatives from a variety of constituencies to discuss challenges and solutions. The committee's recommendations are presented in this article."

Jacobson, Louis.
Conservatives push for health care privacy. National journal, v. 30, Jan. 10, 1998: 80.
Conservatives in the Consumer Coalition oppose a provision in a Medicare bill which "would require doctors to file reports about such care [of seniors who want to pay for medical services not covered by Medicare] with the Health and Human Services Department."

Kloss, Linda L.
Seeking confidentiality of medical records. USA today (magazine), v. 128, Jan. 2000: 26.

Longman, Phillip J. Brownlee, Shannon.
The genetic surprise. Wilson quarterly, v. 24, autumn 2000: 40-50.
"[T]he collision of two well-established trends in medicine and law may soon make the private sector's role in spreading the risk of health care costs unworkable, and government provision of universal health care coverage increasingly difficult to avoid. The first of these trends is the rapid advancement of genetic testing... The second trend that will have an impact on private health insurance is the plethora of 'right to privacy' laws passed in response to widespread fears that genetic tests will be used as a basis for discrimination."

Medical records privacy. Congressional digest, v. 79, Aug.-Sept. 2000: 193-224.
Contributors to this issue include the American Collectors Association, the American Hospital Association, the Blue Cross and Blue Shield Association, the U.S. Department of Health and Human Services, Sen. Edward Kennedy, and the Health Privacy Project. They argue both sides of the question: "Should the government set comprehensive standards to protect the privacy of personal medical information?"

Nakashima, Allyn K.
Effect of HIV reporting by name on use of HIV testing in publicly funded counseling and testing programs. JAMA [Journal of the American Medical Association], v. 280, Oct. 28, 1998: 1421-1426.
Data from six "state health departments (Louisiana, Michigan, Nebraska, Nevada, New Jersey, and Tennessee) 12 months before and 12 months after HIV reporting was introduced" found that "confidential HIV reporting by name did not appear to affect use of HIV testing in publicly funded counseling and testing programs."

Pear, Robert.
Clinton will issue new privacy rules to shield patients. New York times, Dec. 20, 2000: A1.

Describes President Clinton's "sweeping new rules to protect the privacy of medical records by requiring doctors and hospitals to get consent from patients before disclosing health information."

Reilly, Philip R.
Efforts to regulate the collection and use of genetic information. Archives of pathology & laboratory medicine, v. 123, Nov. 1999: 1066-1070.
Argues that "everyone would benefit from enactment of a general medical privacy law that covers access to and use of all health information."

Rindfleisch, Thomas C.
Privacy, information technology, and health care. Communications of the ACM, v. 40, Aug. 1997: 93-100.
Looks at threats to patient information privacy and the countermeasures that might prove most effective.

Rothstein, Mark A. Gelb, Betsy D. Craig, Steven G.
Protecting genetic privacy by permitting employer access only to job-related employee medical information: analysis of a unique Minnesota law. American journal of law and medicine, v. 24, no. 4, 1998: 399-416.
"Legislation restricting employer access to irrelevant medical information will be more effective than laws making the use of genetic information unlawful. Until meaningful medical privacy legislation is enacted, individuals will continue to be reluctant to undergo genetic testing in the clinical setting because they fear the possible uses of the information."

Serafini, Marilyn Werber.
Double trouble. National journal, v. 29, Sept. 20, 1997: 1830-1831.
Warns that imprecisely worded legislation on the cloning of humans and privacy of medical records could "have the unintended consequence of banning important genetics research."

Starr, Paul.
Smart technology, stunted policy: developing health information networks. Health affairs, v. 16, May-June 1997: 91-105.
Discusses how privacy concerns have impeded the development of public data repositories for health care research, policy, and consumer education.

Sullivan, Andrew.
Promotion of the fittest. New York times magazine, July 23, 2000: 16-18.
"The new science of genetic screening is so precise that it might just give workplace discrimination a good name."

Tobler, Laura.
When medical secrets have nowhere to hide. State legislatures, v. 23, Apr. 1997: 24-27.

"It is perfectly legal to share patients' medical records. Some are wondering why."

U.S. Congress. House. Committee on Commerce. Subcommittee on Health and Environment.
The Medical Information Protection and Research Enhancement Act of 1999. Hearing, 106th Congress, 1st session. July 15, 1999. Washington, G.P.O., 1999. 165 p.
"Serial 106-53"
A hearing on a bill, "To ensure confidentiality with respect to medical records and health care-related information, and for other purposes."

U.S. Congress. House. Committee on Commerce. Subcommittee on Health and Environment.
Medical records confidentiality in the modern delivery of health care. Hearing, 106th Congress, 1st session. May 27, 2000. Washington, G.P.O., 1999. 121 p.
"Serial no. 106-34"

U.S. Congress. House. Committee on Commerce. Task Force on Health Records and Genetic Privacy.
Privacy, confidentiality and discrimination in genetics. Washington, G.P.O., 1998. 106 p.
At head of title: 105th Congress, 2nd session, Committee print 105-T.

U.S. Congress. House. Committee on Government Reform and Oversight. Subcommittee on Government Management, Information and Technology.
Protecting health information: legislative options for medical privacy. Hearing, 105th Congress, 2d session. May 19, 1998. Washington, G.P.O., 1999. 233 p.
"Serial no. 105-179"

U.S. Congress. House. Committee on Ways and Means. Subcommittee on Health.
Confidentiality of health information. Hearing, 106th Congress, 1st session. July 20, 1999. Washington, G.P.O., 2000. 128 p.
"Serial 106-29"

U.S. General Accounting Office.
Medical records privacy: access needed for health research, but oversight of privacy protections is limited; report to congressional requesters. Feb. 24, 1999. Washington, G.A.O., 1999. 28 p.
"GAO/HEHS-99-55, B-280657"
"Examine[s] how medical information is used for research and the need for personally identifiable information, (2) identif[ies] research that is and is not subject to current federal oversight requirements, (3) examine[s] how IRBs [institutional review boards] ensure the confidentiality of health information used in research, and (4) identif[ies] the safeguards health care

organizations have put in place to protect the confidentiality of health information used in research."

Why your health privacy is threatened. Consumers' research, v. 80, Apr. 1997: 24-28.

Electronic information systems are potentially vulnerable to misuse both from insiders and outsiders who access patient information for personal or economic gain. This article looks at this issue using a case history as an example.

Search and Seizure

Anderson, Sean.

Individual privacy interests and the "special needs" analysis for involuntary drug and HIV tests. California law review, v. 86, Jan. 1998: 119-177.

"The author proposes an analysis that looks primarily at the blameworthiness of the conduct or status that would trigger drug or HIV testing. Such an approach, the author argues, would better protect the individual interests that the Fourth Amendment ought properly to defend."

Barnes, Jennifer L.

Students under siege? Constitutional considerations for public schools concerned with school safety. University of Richmond law review, v. 34, May 2000: 621-645.

Barrio, Adrian J.

Rethinking Schneckloth v. Bustamonte: incorporating obedience theory into the Supreme Court's conception of voluntary consent. University of Illinois law review, v. 1997, winter 1997: 215-251.

Note "radically reassess the Supreme Court's conception of voluntary consent. Specifically, this note argues that Schneckloth misapprehended the potential for psychological coercion in the context of consent searches. Because consent searches contain inherently compelling pressures that threaten the exercise of valuable privacy rights, the Fourth Amendment (by analogy to the Fifth Amendment as interpreted in Miranda) requires the police to give a suspect prophylactic warnings prior to requesting his permission to search. These warnings must, at a minimum, communicate to the suspect that he may withhold consent."

Colb, Sherry F.

Innocence, privacy, and targeting in Fourth Amendment jurisprudence. Columbia law review, v. 96, Oct. 1996: 1456-1525.

"Dominant Fourth Amendment thought on the right to be free of unreasonable searches and seizures fails to integrate the substantive and procedural components of this right. The harms that the right is intended to prevent are both the substantive harm of privacy being violated and the procedural harm of government invasion of privacy without justification.

Fourth Amendment analysis that pits the privacy rights of individuals against public crime control concerns fails to consider all the types of harm that the amendment is intended to prevent."

The qualitative dimension of Fourth Amendment "reasonableness." Columbia law review, v. 98, Nov. 1998: 1642-1725.

"The quantitative procedural approach to protections afforded by the Fourth Amendment should be supplemented by a qualitative substantive approach. The procedurally-based expectation of privacy test unnecessarily limits constitutional protections. Findings of unreasonableness of searches and seizures should include a balancing test opposing an individual's security and privacy interests against the specific class or classes of search and seizure. This consideration of substantive privacy interests is consistent with constitutional precedent."

The Constitution of the United States of America: analysis and interpretation; annotations of cases decided by the Supreme Court of the United States to June 29, 1992. Prepared by the Congressional Research Service. Washington, G.P.O., 1992. (Document, Senate, 103rd Congress, 1st session, no. 103-6)

The chapter on the Fourth Amendment describes the history and scope of constitutional search and seizure law, and discusses the amendment as it applies to electronic surveillance. The Fourth Amendment 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 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."

With 1996, 1998, and 2000 supplements. Available on the Web: *http://www.access.gpo.gov/congress/senate/constitution/*

Ferraraccio, Michael.

Metal detectors in the public schools: Fourth Amendment concerns. Journal of law and education, v. 28, Apr. 1999: 209-229.

Article asks "whether the use of metal detectors is an effective or desirable means of addressing violence in the schools. The article also addresses whether the justification put forth by the proponents are compelling enough to override students' privacy interests, ultimately concluding that there are serious constitutional concerns raised by their use, and the rationale for upholding school searches in other contexts does not apply to metal detector searches."

Gartner, Scott A.

Strip searches of students: what Johnny really learned at school and how local school boards can help solve the problem. Southern California law review, v. 70, Mar. 1997: 921-978.

"This Note advocates the categorical prohibition of strip searches in our

public schools . . . . If an incident rises to the level where a school official believes such a search would reveal evidence of a serious crime, that official should notify the student's parents as well as local law enforcement agents. It would then be up to the police to determine whether the school official's suspicion is enough to make out probable cause and to obtain a search warrant."

Harris, David A.

"Driving while Black" and all other traffic offenses: the Supreme Court and pretextual traffic stops. Journal of criminal law & criminology, v. 87, winter 1997: 544-582.

"Whren [v. United States] leaves us in an unsatisfactory situation. Any time we use our cars, we can be stopped by the police virtually at their whim because full compliance with traffic laws is impossible. And we can feel relatively certain that past will be prologue: African-Americans and Hispanics will suffer the bulk of this treatment. Whites will not have to endure it very often; if they did, it probably would not happen. And, once police stop drivers, the officers will be able to search almost everyone they want, some with consent and others with dogs."

Hendrie, Edward M.

Curtilage: the expectation of privacy in the yard. FBI law enforcement bulletin, v. 67, Apr. 1998: 25-32.

"The U.S. Supreme Court has interpreted the Fourth Amendment as providing the greatest degree of protection against government encroachment to the home. For Fourth Amendment purposes, that area immediately surrounding the home, the curtilage, has customarily been viewed as part of the home. This article explores the limits of the protection afforded the curtilage."

Jackson, Karoline E.

The legitimacy of cross-gender searches and surveillance in prisons: defining an appropriate and uniform review. Indiana law journal, v. 73, summer 1998: 959-995.

Note argues that "courts should explicitly recognize inmates' constitutional right to be free from cross-gender searches and surveillance. Sources of this constitutional right are found both in the privacy rights of the Fourth Amendment and the penumbras of the Bill of Rights. Forced inspections and observations of inmates by opposite-sex officers are degrading, humiliating, and violate the basic tenets of human decency. In analyzing inmates' claims of constitutional deprivations, courts should be extremely faithful in applying the Turner standard of review. Courts must clearly and specifically analyze all prongs of the Turner test. No longer can courts infringe on inmates' privacy rights based on nonpenological objectives and the speculative concerns of prison superintendents."

Johnson, Robert S.
Metal detector searches: an effective means to help keep weapons out of schools. Journal of law and education, v. 29, Apr. 2000: 197-203.

Johnston, Brad M.
The media's presence during the execution of a search warrant: a per se violation of the Fourth Amendment. Ohio State law journal, v. 58, no. 4, 1997: 1499-1534.
"Fourth Amendment analysis finds that media presence during the execution of search warrants implicates Fourth Amendment protection of individuals' privacy expectations, transforms media members from private actors into state actors, and offends the reasonableness threshold for constitutional invasions of individuals' homes."

Julie, Richard S.
High-tech surveillance tools and the Fourth Amendment: reasonable expectations of privacy in the technological age. American criminal law review, v. 37, winter 2000: 127-143.
Explores the scope of the Fourth Amendment's "right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures." Discusses methods for determining when a search has occurred. Also discusses how courts have ruled on the surveillance efforts of antinarcotic law enforcement officers.

Labaton, Stephen. Richtel, Matt.
Proposal offers surveillance rules for the Internet. New York times, July 18, 2000: A1.
Discusses a White House proposal to standardize rules concerning online surveillance by law enforcement agencies. Also reports on Carnivore, an F.B.I. computer system that "searches and intercepts private e-mail and can easily capture communications of people not suspected of crimes."

Lazarus, Jason.
Vision impossible? Imaging devices--the new police technology and the Fourth Amendment. Florida law review, v. 48, Apr. 1997: 299-335.
"This [Comment] discusses the two most likely places that police will use imaging devices: on the street at targeted suspects and at fixed checkpoints on all passersby. Part II of this [comment] reviews Fourth Amendment search analysis and discusses whether the use of an imaging device constitutes a search."

Lynch, Timothy.
In defense of the exclusionary rule. Washington, Cato Institute, 1998. 43 p. (Policy analysis no. 319)
"Much of the modern debate about the enforcement of the Fourth Amendment has focused on the wisdom of and constitutional necessity for the so-called exclusionary rule, under which evidence obtained in violation of the Fourth Amendment is ordinarily inadmissible in a criminal trial. Conservatives

often oppose the rule as not grounded in the Constitution, not a deterrent to police misconduct, and not helpful in the search for truth. Abolishing the exclusionary rule has been a high priority for conservatives for more than 30 years . . . . The drive to abolish the exclusionary rule is fundamentally misguided, on constitutional grounds, for the rule can and should be justified on separation-of-powers principles, which conservatives generally support."

Maclin, Tracey.
Open door policy. American Bar Association journal, v. 83, July 1997: 46-47.
"While the U.S. Supreme Court has not approved capricious vehicle stops outright, recent rulings will make it much easier for police to effectuate arbitrary and discriminatory intrusions on motorists and passengers with little, if any, constitutional restraint. Over the past two terms, the justices decided a trio of traffic stop cases: Whren v. United States, 116 S. Ct. 1769 (1996); Ohio v. Robinette, 117 S. Ct. 417 (1996); and Maryland v. Wilson, No. 95-1268 (Feb. 19, 1997)."

Race and the Fourth Amendment. Vanderbilt law review, v. 51, Mar. 1998: 333-393.
"In this Article, I argue that the Court should make racial concerns a part of its Fourth Amendment analysis. In particular, where evidence indicates racial targeting by the police, the state should be required to provide a race neutral explanation for the seizure other than probable cause of a traffic violation."

Regini, Lisa A.
Extending the Mimms rule to include passengers. FBI law enforcement bulletin, v. 66, June 1997: 27-32.
"This article will first revisit the Supreme Court's decision in Mimms v. Pennsylvania, which allows officers to order the driver from a lawfully stopped vehicle. It will then examine the Supreme Court's extension of this authority to passengers within the vehicle, decided in Wilson. Finally, the article will briefly address several additional constitutional restraints imposed if officers desire to intrude further into the passenger's personal liberty during the stop."

Riley, Laura B.
Concealed weapon detectors and the Fourth Amendment: the constitutionality of remote sense-enhanced searches. UCLA law review, v. 45, Oct. 1997: 281-336.
States that "currently under development in government-funded laboratories, concealed weapon detectors reveal images of all items concealed in or underneath a person's clothes from up to ninety feet away. Two of the detectors also reveal an image of the body's anatomical contours . . . . To avoid [a] reliance on irrelevant factors, Riley proposes a two-factor approach. First, courts should consider the 'place' under police surveillance and its conceptual

link to intimate and private interests. Second, courts should evaluate the 'intrusiveness' of the sense-enhanced surveillance, defined as the degree to which the device reveals more than the presence or absence of contraband or other evidence of crime. Riley concludes that under the suggested approach police use of the concealed weapon detectors would constitute a search under the Fourth Amendment."

Savage, David G.
Privacy rights pulled over. American Bar Association journal, v. 85, June 1999: 42, 44.
"Cops get more power to search personal effects in vehicles."

Serr, Brian J.
Great expectations of privacy: a new model for Fourth Amendment protection. Minnesota law review, v. 73, Feb. 1989: 583-642.
Reviews and criticizes Supreme Court decisions related to search and seizure. "Proposes a new model for fourth amendment decision making . . . that will expand the scope of citizens' rights to privacy under the fourth amendment without detracting from legitimate law enforcement efforts to detect and prevent crime."

Stanley, Kristal Otto.
The Fourth Amendment and dormitory searches--a new truce. University of Chicago law review, v. 65, fall 1998: 1403-1433.
"This Comment provides a framework to aid courts in evaluating the constitutionality of dormitory searches. It analyzes the competing educational and law enforcement interests at stake and suggests Fourth Amendment standards that balance the privacy interests of students and the interests of the colleges and universities in maintaining an environment consistent with their educational mission. Part I analyzes the current state of the dormitory search caselaw according to the issues of state action, consent, administrative searches, and the exclusionary rule. Part II presents the proposed framework in two steps: first, it establishes a threshold determination use to place the dormitory search into one of three categories; and second, it sets forth the appropriate Fourth Amendment standard for each of the three categories."

Thermal imaging: much heat but little light. FBI law enforcement bulletin, v. 66, Dec. 1997: 18-24.
"Several court decisions illustrate the constitutional arguments for and against police use of thermal imagers without a search warrant. Within certain guidelines, law enforcement can use thermal imagers in compliance with the requirements of the Fourth Amendment of the U.S. Constitution."

Thompson, Anthony C.
Stopping the usual suspects: race and the Fourth Amendment. New York University law review, v. 74, Oct. 1999: 956-1013.

Urbonya, Kathryn R.
The fishing gets easier. American Bar Association journal, v. 83, Jan. 1997: 46, 48.
"Police gain more latitude in traffic stops, and other powers could be on the way."

Technology

Bettelheim, Adriel
Lawmakers, industry debate how to tackle 'cybercrime' without jeopardizing privacy. CQ weekly, v. 58, Mar. 4, 2000: 473.

Brin, David.
The transparent society: will technology force us to choose between privacy and freedom? Reading, Mass., Perseus Books, c1998. 378 p.
"No matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases." Instead of advocating for more secrecy, Brin advocates "transparency -- the notion that we may all benefit by carefully increasing two-way information flows."

Cate, Fred H.
Privacy in the information age. Washington, Brookings Institution Press, 1997. 248 p.

Cha, Ariana Eunjung.
Your PC is watching: programs that send personal data becoming routine. Washington post, July 14, 2000: A01.
A report on "spyware" or "electronic eavesdroppers" that collect data from consumers' computers and send the information to companies without the users' knowledge.

Computers, surveillance, and privacy. Edited by David Lyon and Elia Zureik. Minneapolis, University of Minnesota Press, c1996. 285 p.

Dean, Lisa S.
What price security? Security management, v. 43, June 1999: 42-44.
Modern technology has made it possible to build a file on every American and to record and track their daily lives. Computers now collect and store immense databases on individuals, with detailed records about their health status and treatment, employment history, financial transactions, educational performance, travel habits, and even their DNA. A discussion of some of the most controversial government databases - those that store medical, employment, ID, and DNA records - and how their existence threatens the privacy of every U.S. citizen is presented.

DeCew, Judith Wagner.
In pursuit of privacy: law, ethics, and the rise of technology. Ithaca, N.Y., Cornell University Press, 1997. 199 p.

The Electronic privacy papers: documents on the battle for privacy in the age of surveillance. Edited by Bruce Schneier and David Banisar. New York, Wiley, c1997. 747 p.

Garfinkel, Simson.
Database nation: the death of privacy in the 21st century. Cambridge, Mass., O'Reilly, c2000. 312 p.
Garfinkel sees many threats to privacy: the inadequacy of laws protecting medical records privacy, surveillance by law enforcement agencies and businesses, and the selling among marketers of personal consumer data. "Without government protection for the privacy rights of individuals, it is simply too easy and too profitable for business to act in a manner that's counter to our interests." The book contains an extensive annotated bibliography.

Gruenwald, Juliana.
Mixed signals in the debate over encryption technology. CQ weekly, v. 56, June 13, 1998: 1589-1592.
"Top law enforcement officials and computer executives caucused on Capitol Hill to discuss the future of encryption technology that scrambles data and prevents intruders from gaining unauthorized access."

Henderson, Harry.
Privacy in the information age. New York, Facts on File, 1999. 262 p.
A broad overview of privacy law and related issues, plus an extensive guide to researching the topic. Includes a research bibliography, a glossary of terms, and descriptions of organizations involved in the privacy debate.

Herkert, Joseph R. Cartwright, G. Phillip.
The conscience of computer science. Change, v. 30, Jan.-Feb. 1998: 61-63.
Highlights professional organizations that study the social and ethical implications of information technology.

The Internet and the law. Nova law review, v. 23, winter 1999: whole issue (552-888 p.).
Partial contents.--Privacy in the digital age: work in progress, by Jerry Berman and Deirdre Mulligan.--Searching for security in the law of electronic commerce, by Amelia H. Boss.--The struggle for a new paradigm: protecting free speech and privacy in the virtual world of cyberspace, by Ira Glasser.

Jacobson, Louis.
Washingtonclout.com. National journal, v. 30, Dec. 19-26, 1998: 3012-3017.

Internet companies have learned to court lawmakers and regulators. Rules on data privacy, online advertising and taxes have an impact on Internet commerce.

Kang, Jerry.
Information privacy in cyberspace transactions. Stanford law review, v. 50, Apr. 1998: 1193-1294.
This article discusses cyberspace privacy, "examines what is technologically different in cyberspace and how information privacy will be threatened by new technologies unfettered by old laws." Proposes a "Cyberspace Privacy Act, which would govern the processing of personal information collected in the course of executing cyberspace transactions in the United States."

Labaton, Stephen. Richtel, Matt.
Proposal offers surveillance rules for the Internet. New York times, July 18, 2000: A1.
Discusses a White House proposal to standardize rules concerning online surveillance by law enforcement agencies. Also reports on Carnivore, an F.B.I. computer system that "searches and intercepts private e-mail and can easily capture communications of people not suspected of crimes."

Masci, David.
Internet privacy: is more government regulation needed? CQ researcher, v. 8, Nov. 6, 1998: whole issue (953-976 p.).
Law enforcement agencies "favor government limitations on the use of sophisticated encryption technology, which makes on-line communications secure--even from the police. They fear that strong encryption software will aid criminals in hiding their activities. But privacy advocates argue that encryption technology assures companies and consumers that their on-line communications are not being tampered with."

Munro, Neil.
What bugs the FBI. National journal, v. 30, May 9, 1998: 1042-1046.
"High-tech firms and federal authorities are locked in a debate over new scrambling devices for phones and computers. While the FBI worries that the technology will help crooks, industry complains that the G-men are behind the times."

Pilant, Lois.
The debate over encryption. Police chief, v. 66, Jan. 1999: 31-35.
"Encryption is the ability to disguise messages, rendering them unintelligible to anyone but the authorized recipient . . . . Users include the world's technically sophisticated criminals, who use encryption products to protect the electronic files stored on their computers' hard drives, making them inaccessible to anyone, especially law enforcement."

Privacy in the age of computers. Human rights, v. 26, winter 1999: whole issue (28 p.).

Contents.--Introduction: privacy in the age of computers.-- Cyberspace privacy: a primer and proposal, by Jerry Kang.--Public records, public policy, and privacy, by Robert Gellman.--Privacy for sale: peddling data on the Internet, by Andrew L. Shapiro.--Children in cyberspace: a resource guide, by Beth Givens.--Rules of the road for navigating the information superhighway, by Barry Fraser.--E-mail in the workplace: limitations on privacy, by Mary E. Pivec and Susan Brinkerhoff.-- Electronic gadgets never forget, by Royal Van Horn.

Race, Tim.
While the public's concern over online privacy seems to be pervasive, nuances -- and contradictions -- abound. New York times, July 24, 2000: C4.

"Online, it seems, privacy is in the eye of the beholder. That's why the public debate over electronic privacy can get so confusing. Whose privacy? Protected from whom?"

Rivest, Ronald L.
The case against regulating encryption technology. Scientific American, v. 279, Oct. 1998: 116-117.

Notes that "U.S. government agencies want to restrict the use of data encryption because they fear that criminals and spies may use the technology to their own advantage . . . . But it is poor policy to clamp down indiscriminately on a technology merely because some criminals might be able to use it to their advantage."

Smith, H. Jeff.
Managing privacy: information technology and corporate America. Chapel Hill, University of North Carolina Press, c1994. 297 p.

Symposium on Internet privacy. Santa Clara computer and high-technology law journal, v. 16, May 2000: whole issue (510 p.).

Partial contents:--Privacy expectations in a high tech world, by Beth Givens.--At the intersection of visible and invisible worlds: United States privacy law and the Internet, by Dorothy Glancy.--Big Bird meets Big Brother: a look at the Children's Online Privacy Protection Act, by Laurel Jamtgaard.--Privacy on the Internet: the evolving legal landscape, by Debra A. Valentine.

Technology and privacy: the new landscape. Edited by Philip E. Agre and Marc Rotenberg. Cambridge, Mass., MIT Press, c1997. 325 p.

Partial contents: Convergence revisited: toward a global policy for the protection of personal data, by Colin J. Bennett.--Privacy-enhancing technologies: typology, critique, vision, by Herbert Burkert.--Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity, by Simon G. Davies.--Controlling surveillance: can privacy protection be made effective? by David H. Flaherty.--Does privacy law work? by Robert Gellman.

Thompson, Kimberly R.
Cell phone snooping: why electronic eavesdropping goes unpunished. American criminal law review, v. 35, fall 1997: 137-162.
Comment "concludes that the current prosecutorial response to cellular eavesdroppers is not overly problematic given that a civil remedy is available to victims, cellular subscribers can utilize technology which can not be intercepted, and the Wiretap Act sought to balance the privacy of cellular communication with the interests of radio hobbyists."

Tomkins, P. L.
Panopticon: technology, the individual and social control in the early 21st century. RUSI (Journal of the Royal United Services Institute for Defense Studies) journal, v. 143, Apr. 1998: 51-57.
Considers the relationship between increased technology and loss of privacy.

Tonsing, Mike.
The digital certificate comes of age. Federal lawyer, v. 45, Oct. 1998: 20-21.
"The electronic passports of the information superhighway, the ID cards of the Internet, the sealed pouches of cyberspace. By digitally signing and encrypting one's email transmissions, one can be assured that such messages are protected from eavesdropping [and] tampering."

U.S. Congress. House. Committee on Commerce. Subcommittee on Telecommunications, Trade, and Consumer Protection.
The Security and Freedom Through Encryption (SAFE) Act. Hearing, 106th Congress, 1st session on H.R. 850. May 25, 1999. Washington, G.P.O., 1999. 89 p.
"Serial no. 106-28"

The Wireless Privacy Enhancement Act of 1999 and the Wireless Communications and Public Safety Enhancement Act of 1999. Hearing, 106th Congress, 1st session. Feb. 3, 1999. Washington, G.P.O., 1999. 55 p.
"Serial no. 106-2"

U.S. Congress. House. Committee on Judiciary.
Security and Freedom Through Encryption (SAFE) Act; report together with additional views to accompany H.R. 850 including the cost estimate of the Congressional Budget Office. Apr. 27, 1999. Washington, G.P.O., 1999. 34 p. (Report, House, 106th Congress, 1st session, no. 106-117, part 1)

U.S. Congress. Senate. Committee on Commerce, Science, and Transportation.
Children's Internet Protection Act; report on S. 97. Washington, G.P.O., 1999. 24 p. (Report, Senate, 106th Congress, 1st session, no. 106-141)

U.S. Congress. Senate. Committee on the Judiciary.
Privacy in the digital age: discussion of issues surrounding the internet. Hearing, 106th Congress, 1st session. Apr. 21, 1999. Washington, G.P.O., 2001. 234 p.
"S. Hrg. 106-815"

U.S. Federal Bureau of Investigation. Carnivore diagnostic tool: Internet file.
URL: *http://www.fbi.gov/programs/carnivore/carnivore.htm*
(As of Jan. 26, 2001)
This Web site includes statements and reports on the FBI's Carnivore system, which "provides the FBI with a 'surgical' ability to intercept and collect the communications which are the subject of the lawful order while ignoring those communications which they are not authorized to intercept."

Whitaker, Reginald.
The end of privacy: how total surveillance is becoming a reality. New York, New Press; distributed by W.W. Norton, c1999. 195 p.
Explores the impact of surveillance technology on political power. Also discusses how consumers willingly give up their personal information and privacy for the sake of convenience.

Wimmer, Kurt A
E-litigation: Internet privacy. National law journal, v. 22, Mar. 20, 2000: A17.
Legal issues involving Internet privacy litigation are examined. The most important watchword for a company that posts a privacy policy is monitoring, for posting and forgetting may be a costly mistake.

Zimmermann, Philip R.
Cryptography for the Internet. Scientific American, v. 279, Oct. 1998: 110-115.
"E-mail and other information sent electronically are like digital postcards -- they afford little privacy. Well-designed cryptography systems can ensure the secrecy of such transmissions."

○