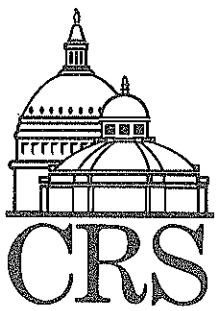
97-833 A

CRS Report for Congress

Information Privacy

Gina Marie Stevens
Legislative Attorney
American Law Division

September 15, 1997



Congressional Research Service • The Library of Congress

INFORMATION PRIVACY

SUMMARY

It is routinely acknowledged that the success of the Internet and electronic commerce depends upon the resolution of issues related to the privacy and security of information. Privacy is thus thrust to the forefront of policy discussions among businesses, governments, and citizens. Threats to the privacy of information arise primarily as the result of the widespread increase in the availability and use of computers and computer networks. The Congress, the executive branch, courts, businesses, privacy advocates, Web sites, Internet service providers, and professional organizations confront many privacy issues.

As the cost of storing electronic information becomes less expensive, more information is stored and linked by use of the same key, such as the social security number. Data-mining software facilitates the use of electronic information for commercial, unauthorized, and unlawful purposes. Because of the power of computer networks to compile, analyze, share, and match electronic information, electronic information is potentially much more invasive. One result of these technological advances has been the rapid growth of the information industry. There are three participants in the information industry: government entities, direct marketers, and reference services. Consumer reporting agencies are also a source of personal information. Generally each participant gathers and distributes personally identifying information. The information may be gathered for one purpose, and sold for another.

Threats to the privacy of information also come from criminals and hackers. Hackers are reported to be gathering sensitive consumer information in order to commit financial fraud. Financial fraud is committed when there is enough information to deceive a creditor about the perpetrator's true identity. This practice is commonly referred to as **identity theft** -- the illegal use of personal identifying information -- to commit financial fraud.

Constitutional protection extends only to the protection of the individual against government intrusions and does not address many recurring threats to the privacy of information by private entities. Existing federal statutes do not comprehensively protect the informational privacy interests of individuals and businesses either. However, there are several federal laws that extend protection to certain types of information on a sector-by-sector basis.

Individuals and businesses concerned with privacy are looking to encryption, the use of algorithms and ciphers to scramble and descramble information, to keep information private. Encryption can also impede the ability of law enforcement and national security agencies to access electronic information. The federal government has a strong interest in preserving its ability to intercept and interpret electronic communications. Currently there are no limits on what strength of encryption can be used in the United States, but there are limits on the strength of encryption products that can be sold internationally. The Congress is currently examining several proposals regulating the availability of encryption products.

TABLE OF CONTENTS

Information Privacy

INTRODUCTION

It is routinely acknowledged that the success of the Internet and electronic commerce depends upon the resolution of issues related to the privacy and security of information.[1] Privacy is thus thrust to the forefront of policy discussions among businesses, governments, and citizens. Twenty years ago the Privacy Protection Study Commission recommended steps be taken to strike a proper balance between the individual's personal privacy interests and society's information needs.[2] This paper discusses some recent threats to the privacy of information.[3] These threats arise primarily as the result of the widespread increase in the availability and use of computers and computer networks, the corresponding increase in the amount and type of information created, the availability and use of information for unauthorized secondary purposes, and the lack of adequate computer security. Technological safeguards, such as encryption, are viewed as tools to enhance computer security and protect privacy. Encryption also has the potential to impede the ability of law enforcement and national security agencies to access electronic communications.[4] Congress is currently examining several legislative proposals concerning the availability of encryption products. The Congress,[5] the

---

[1] See, U.S. Govt. Information Infrastructure Task Force, *A Framework for Global Electronic Commerce* 10-12. Available: http://www.iitf.nist.gov/eleccomm/ecomm.htm (1997).

[2] Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977).

[3] *"Are You For Sale?"* PC World Magazine, October 1996. Available: http://www.pcworld.com/workstyles/online/articles/oct96/1410forsale.html. *"Internet Opens Your Windows to Everyone: Invasion Sorely Tests Right to be Let Alone,"* N.Y. Times, Aug. 3, 1997, at 1A. *"Privacy on the Web,"* TIME Magazine, Aug. 19, 1997. Available: http://www.pathfinder.com. *"Privacy for Sale: Peddling Data on the Internet,"* The Nation, June 23, 1997, at 11. The complex issues related to the privacy of medical information are beyond the scope of this report.

[4] Denning and Baugh, *Encryption and Evolving Technologies: Tools of Organized Crime and Terrorism* (1997).

[5] For a list of privacy legislation introduced in the 105th Congress see, *EPIC (Electronic Privacy Information Center) Online Guide to 105th Congress Privacy and Cyber-liberties Bills.* Available: http://epic.org/privacy/bill_track.html. (July 10, 1997).

executive branch,[6] courts, businesses,[7] privacy advocates,[8] Web sites and Internet service providers,[9] and professional organizations[10] continue to confront many other issues associated with the security and privacy of information.

BACKGROUND

Privacy has become a "broad, all-encompassing concept that envelops a whole host of human concerns about various forms of intrusive behavior, including wiretapping, surreptitious physical surveillance, and mail interception. Individuals claim a right of privacy for an enormously wide range of issues from the right to practice contraception or have an abortion to the right to keep bank

---

[6] See, Federal Trade Commission, *Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure* (December 1996). Available: http:www.ftc.gov/bcp/conline/pubs/privacy/privacy.htm. In June of 1997, the FTC held four days of hearings on technology tools and industry self-regulation regimes designed to enhance personal privacy on the Internet. Available: http://www.ftc.gov/bcp/privacy2/index.html. U.S. Govt. Information Infrastructure Task Force, Information Policy Committee, *Options for Promoting Privacy on the National Information Infrastructure* (April 1997). Available: http://www.iitf.nist.gov/ipc/privacy.htm. Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud (March 1997).* Available: http://www.bog.frb.fed.us/boarddocs/RptCongress/privacy.pdf. U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments*, OTA-TCT-606 (Sept. 1994) and *Issue Update on Information Security and Privacy in Network Environments* (June 1995). Social Security Administration, *Privacy and Customer Service in the Electronic Age* (September 1997). Available: http://www.ssa.gov.

[7] Privacy and American Business, *Handbook of Company Privacy Codes* Vol. 3 (1996).

[8] See, American Civil Liberties Union, *Take Back Your Data Campaign* (July 1997). Available: www.aclu.org/action/tbyd.html. Center for Democracy and Technology, *CDT Privacy Demonstration*. Available: http:www.cdt.org/privacy. Electronic Frontier Foundation, *PrivacyArchive*. Available: http://www.eff.org/pub/Publications/CuD/Privacy. Electronic Privacy Information Center, *Surfers Beware: Personal Privacy and the Internet (June 1997). Available: http:www.epic.org/reports/surfer-beware.html.*

[9] Netscape Comm., *Netscape, Firefly and Verisign Propose Open Profiling Standard (OPS) to Enable Broad Personalization of Internet Services: More Than 60 Companies and Organizations Support Uniform Architecture that Protects Users' Privacy* (May 27, 1997). Available: http://search.netscape.com/newsref/pr/newsrelease411.html. World Wide Web Consortium (W3C), *Platform Privacy Preferences (P3) Project* (June 1997). Available: http://www.w3.org/P3/overview.html.

[10] Direct Marketing Association, *Guidelines for Personal Information Protection*. Available: http:www.the-dma.org; Interactive Services Association, *Protecting Your Privacy When You Go Online*. Available: http://www.isa.net/project-open/priv-broch.html.

records confidential."[11] Some advocate the expansion of this concept to include the right to "information privacy" for online transactions and personally identifiable information.[12] The term "information privacy" refers to an individual's claim to control the terms under which "personal information" -- information that can be linked to an individual or distinct group of individuals (e.g., a household) -- is acquired, disclosed, and used.[13] The right to privacy has also been characterized as the "the right to be let alone."[14] There is a perception among many that in our information driven society this right is under attack. The potential harm that can occur from unauthorized disclosures of such information has been well documented.[15]

Individuals and businesses increasingly rely upon computers and computer networks to transact business and to access the Internet. There are estimated to be over 9,400,000 host computers worldwide, of which approximately 60 percent are located within the United States, and are estimated to be linked to the Internet. This count does not include the personal computers people use to access the4 Internet using modems. In all, reasonable estimates are that as many as 40 million people around the world can and do access the Internet. This figure is expected to grow to 200 million Internet users by the year 1999.[16] Computers are used for many transactions today: electronic uniform product code (UPC) scanners, telephones, email, Caller ID, ATMs, credit cards, electronic tolls, video surveillance cameras, health insurance filings, catalog shopping, pharmacy records, and Internet access. The use of computers and computer networks for personal and business transactions has resulted in the creation of vast amounts of information. Information stored or transmitted via computers includes credit and financial information, health information, tax information, employment information, business information, trade secrets, proprietary information, and customer information.

Online users may voluntarily disclose personally identifying information, for example, to an online service provider for registration or subscription purposes, to a Web site, to a marketer of merchandise, in a chat room, on a

---

[11] See, David Flaherty, *Protecting Privacy in Surveillance Societies*, University of North Carolina Press, Chapel Hill, 1989.

[12] See, Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*" 44 Fed. Comm. L.J. 195 (1992).

[13] See, U.S. Govt. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, Commentary ¶ 2 (1995). Available: http://www.iitf.nist.gov/ipc/ipc-pubs/niiprivprin_final.html.

[14] *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[15] See, J. Rothfeder, *Privacy for Sale: How Computerization Has Made Everyone's Private Life an Open Secret* 175-95 (1992).

[16] *ACLU v. Reno*, 117 S. Ct. 2329, 2334 (1997).

bulletin board, or to an email recipient.[17] Information about online users is also collected by Web sites through technology which tracks traces and portraits of every interaction with the network.[18]

When a person accesses a Web site, the site's server requests a unique ID from the person's browser (e.g., Netscape, Microsoft Internet Explorer). If the browser does not have an ID the server delivers one in a "cookie" file to the user's computer. This process is called "passing a cookie." Cookies are similar to the Caller ID feature on phone systems. Web sites can use cookies to track information about user behavior.[19] Web sites contend that the primary purpose for the use and collection of user data is so that the computer receiving the data can send the information file requested by a user to the user's computer, to permit Web site owners to understand activity levels at various areas within sites, and to build new Web applications tailored to individual customers. One widely criticized feature of "cookies" is that this activity is generally invisible to the user, and often occurs without user consent.

Information that is stored electronically often can be linked by use of the same key, such as the social security number. The widespread use of the social security number for secondary purposes (e.g., credit, financial, motor vehicle licensing, health insurance, etc.) has contributed to this phenomenon. A person's social security number, by itself, may have little value since it in and of itself does not convey information about a person's characteristics, interests, buying habits, etc. It may be useful though to a credit card company (to help verify an applicant's identity) and also to a direct marketer (to ensure that a solicitation is sent to the right person).

---

[17] A report by the National Telecommunications and Information Administration (NTIA) addressed the private sector collection, use, and dissemination of telecommunications-related personal information (TRPI) created in the course of an individual's subscription or use of a telecommunications service; and concluded that as the cost of digitally storing personal information becomes less expensive, the accumulation of personal information from disparate sources will become more cost-effective for users. U.S. Dept. of Commerce, *National Telecommunications and Information Administration, Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (1995). Available: http://www.ntia.doc.gov/ntiahome/privwhitepaper.html.

[18] A recent survey of the current practices of 70 federal agency web sites regarding the use of personal information collected from online users found that 31 federal agencies collect personal identifying information primarily from guest books, comment forms, or feedback forms. It found that 11 of the 31 agencies that collect personally-identifiable information reportedly give notice of use on their sites. See, OMB Watch, "*A Delicate Balance: The Privacy and Access Practices of Federal Government World Wide Web Sites,*" (Aug. 1997). Available: http://ombwatch.org/ombw/info/balance.html.

[19] See, Vanderbilt University Owen Graduate School of Management, Commercialization of the World Wide Web: The Role of Cookies. Available: http://www2000.ogsm.vanderbilt.edu/cb3/mgt565a/group5/paper.group5.paper2.htm.

Technologies like data-mining software facilitate the use of this information for commercial, unauthorized, and unlawful purposes. Because of the power of computer networks to quickly and inexpensively compile, analyze, share, and match digitized information, electronic information is potentially much more invasive. Computers make information multi-functional as vast amounts of consumer information are collected, generated, sorted, and disseminated electronically, and perhaps then sold, with or without consent. A wealth of personal information about individuals can be harvested. How valuable the information is depends in part on how descriptive it is and how it can be used. One result of these technological advances has been the rapid growth and expansion of the information industry.

INFORMATION INDUSTRY

Basically, there are three participants in the information industry -- government entities (federal, state, local), direct marketers, and reference services.[20] Generally each of them gathers and distributes personally identifying information. The information may be gathered for one purpose, and sold for another.

Examples of public records held by **government entities** that contain personally identifying information such as name, address, and social security number are: driver's licenses', driving records, marriage and divorce records, motor vehicle title and registration, vital statistics, voter registration records, political contribution records, firearm permits, property tax records, land records, SEC filings, court and law enforcement records, postal service address records, boat and aircraft records, financial and ethics disclosures, occupational and recreational licenses. Government records are generally available to anyone, and often represent significant sources of revenue for government agencies.

To determine who should be solicited for a particular product, service, or fund raiser, **direct marketers** rely on lists designed to target individuals who are likely to respond to solicitations. The list may be obtained from consumer surveys, warranty or response cards, and customer purchase data. The lists may also be merged with other lists or with information from other sources, such as public records and magazine subscriptions. Frequently, they rent preexisting lists from list brokers who group information such as similar interests, characteristics, and purchasing habits. The cost of renting a list varies depending upon the number of addresses on the list and the amount of information given.

---

[20] The section is derived from the report of the Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud (March 1997).* Available: http://www.bog.frb.fed.us/boarddocs/RptCongress/privacy.pdf.

Reference services gather information from a variety of sources, compile it, and then make it commercially available.[21] Common users of reference services include law firms, private investigators, and law enforcement officials. There are generally no federal laws on who can access information through a reference service. The service may require users to subscribe. The price of the information depends on how detailed the information is, how quickly it can be provided, and how frequently the subscriber uses the service.

Consumer reporting agencies are a source of a great deal of information about the consumer's finances: employer, credit card and loan account numbers, amount of available credit, amount of outstanding debt, payment histories, and default, judgment and bankruptcy information.

FAIR CREDIT REPORTING ACT

The Fair Credit Reporting Act (FCRA) regulates the credit reporting industry, places certain responsibilities on users of consumer reports, limits the circumstances in which consumer reporting agencies may disclose consumer reports, and requires consumer reporting agencies to investigate and report information the consumer claims is inaccurate or incomplete.[22] Under the FCRA consumer reporting agencies are prohibited from disclosing consumer reports to anyone who does not have a permissible purpose. FCRA defines "consumer report" as:

> "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under § 1681b."[23]

There are three key elements. First, the information must be reported by a consumer reporting agency. Second, the information that is collected must be used, or must be expected to be used, or collected in whole or in part for the purpose of serving as a factor in determining the consumer's eligibility for consumer credit or insurance, employment, or for another permissible purpose.

---

[21] See, *The Lexis-Nexis P-TRAK Service*, Library of Congress, Congressional Research Service Rep. No. 96-795A by Gina Marie Stevens, Sep. 30, 1996.

[22] Extensive amendments were made to the FCRA in September 1996, which generally become effective September 30, 1997. Pub. L. No. 104-208, §§2401-2422, 110 Stat. 3009 (1996).

[23] 15 U.S.C. § 1681a(d)(1).

Third, the information must bear on at least one of the seven enumerated characteristics.[24]

A consumer report contains identifying information, credit information,[25] public record information,[26] and information on inquiries.[27] Identifying information in the consumer report includes the consumer's name (and any prior name), current and previous addresses, birth date and social security number. This identifying information about consumers is often called "header information" in reference to its placement at the "head" of the consumer report. Consumer reporting agencies sell credit header information because it is not considered a consumer report and is therefore not subject to the FCRA.[28]

The Federal Trade Commission's commentaries to the FCRA have been interpreted not to prohibit the disclosure of credit header information for purposes other than credit, insurance, employment, or any of the other permissible purposes. The Commentaries state that "a report limited solely to the consumer's name and address alone, with no connotations as to credit worthiness or other characteristic, does not constitute a 'consumer report,' if it does not bear on any of the seven factors."[29] Recently a federal district court held that information disclosed by a consumer reporting agency containing names, current and former addresses, and social security numbers is not a consumer report within the meaning of the FCRA because the information did not bear on plaintiffs' credit or general character, nor was it used to establish their eligibility for credit, employment or any of the other permissible purposes.[30]

---

[24] 16 C.F.R. Part 600, Ax. section 603(d).

[25] Credit information in the consumer report typically includes bank, retail, credit card, and other lender account information.

[26] Public record information includes records concerning bankruptcy, tax liens, and judgments.

[27] Inquiry information includes the names of parties who have recently obtained copies of the consumer report.

[28] Reference services often purchase header information which is then put into a searchable database. Often the reference service will also have merged information from public records with credit header information.

[29] 16 C.F.R. Part 600 Ax. section 603.

[30] *Dotzler v. Perot, Laughlin v. Perot*, 914 F. Supp. 328 (E.D. Mo. 1996); see also *Hoke v. Retail Credit Corp.*, 521 F.2d 1079, 1081 (4th Cir, 1975), cert. denied, 423 U.S. 1087 (1976).

FINANCIAL FRAUD

Threats to the privacy of digital information also come from criminals and hackers.[31] In 1995 a hacker was arrested and accused of stealing millions of dollars worth of files and more than 20,000 credit-card account numbers from the Internet.[32] A recent GAO report on Information Security concluded that unknown and unauthorized persons are increasingly attacking and gaining access to highly sensitive information in the Department of Defense's computer systems.[33]

Hackers are reported to be gathering sensitive consumer information in order to commit financial fraud. The information most commonly used to commit financial fraud includes the social security number, mother's maiden name, prior addresses, date of birth, employment information (including salary), and credit card, loan, and other financial account numbers. There is a great deal of concern about the availability of any one of these pieces of information because of the ease with which additional pieces of information can be obtained. A mother's maiden name may be considered valuable information in the credit granting process in order to verify a consumer's identity, but not considered sensitive in the context of genealogical research. Financial fraud is committed when there is enough information to deceive a creditor about the perpetrator's true identity.

This practice is commonly referred to as **identity theft** -- the illegal use of personal identifying information -- including name, address, social security numbers, and date of birth -- to commit financial fraud. One particular type of identity theft occurs when the criminal "takes over" a consumer's account by changing the consumer's address for an existing account or submitting a fraudulent credit application to open an account in the consumer's name, but giving a different address as the place to send the card. Financial fraud includes obtaining a credit card under an assumed name, using another person's credit or debit card without authorization, applying for and receiving a loan using an assumed identity, or making unauthorized withdrawals or transfers from another person's checking or deposit account.

The Report of the Board of Governors of the Federal Reserve Board (FRB) indicated that there is little available data on aggregate losses to insured depository institutions due to fraud. Gross fraud charge-offs for

---

[31] Lohr, Steve, *Feeling Insecure Are We? Go Ahead, Be Paranoid. Hackers Are Out to Get You*, New York Times, B1, Mar. 17, 1997.

[32] *Business Technology: Security is Lost in Cyberspace*, N.Y. Times, Feb. 22, 1995, § D, at 1, col. 3.

[33] U.S. General Accounting Office, *Information Security: Computer Attacks at Department of Defense pose Increasing Risks:* Testimony before the Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate. (May 22, 1996) GAO/T-AIMD-96-92.

Mastercard/Visa in 1995 were $790 million. The FRB estimated that check fraud for commercial banks, savings institutions, and credit unions totalled $615 million in 1995. Losses due to identity theft are not tracked separately from other types of fraud. In the opinion of the FRB, fraud losses related to the use of sensitive information likely play a small role in overall fraud losses and pose no significant threat to insured depository institutions.

As criminals take advantage of the Internet, federal investigative authorities expect to make increased use of electronic on-line surveillance.[34]

THE PRESIDENT'S INFORMATION INFRASTRUCTURE TASK FORCE

A host of questions are raised by the proliferation of personal and business information. Does a firm have a right to sell information about its customers? With or without its customers knowledge or consent? Do consumers have a right to privacy in online environments? Should commercial web providers' ability to collect information about its customers be regulated? Can industry self-regulation work? Is the information available secure? How frequent are violations occurring? What the penalties are for those who abuse the system? What is the likelihood of detecting those who commit fraud or abuse?

The President's Information Infrastructure Task Force recommends a market-oriented non-regulatory strategy to promote global electronic commerce on the Internet, and supports industry developed standards for privacy protection based on the following principles: data-gatherers should inform consumers what information they are collecting, and how they intend to use such data; data-gatherers should provide consumers with a meaningful way to limit use and re-use of personal information; consumers also would be entitled to redress if they are harmed by improper use or disclosure of personal information, if it is based on inaccurate, outdated, incomplete, or irrelevant personal information; and special protections for children's data and sensitive data (medical) should exist. To ensure that disparate privacy policies around the world provide adequate privacy protection and do not impede the flow of data on the Internet, the United States plans to engage its major trading partners in discussions to build support for a market based approach to privacy, and to continue discussions with European Union nations to resolve any problems that could threaten data flows.[35]

---

[34] *See* Prepared Testimony of Charles L. Owens, Chief Financial Crimes Section Federal Bureau of Investigation Before Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information, Mar. 19, 1997.

[35] *President's Adviser on Electronic Commerce to Raise U.S. Concerns Over EU Privacy Rule* 14 BNA Intl Trade Rptr 1479 (Sept. 3. 1997).

The European Union Directive on the Protection of Personal Data will become effective October 1998.[36] It comprises a general framework of data protection practices for the processing of personal data, which it defines as "any information relating to an identified or identifiable natural person." The Directive is extraordinarily comprehensive.[37] It will require each of the sixteen EU member states to enact laws governing the "processing of personal data." The Directive defines "processing" as "any operation or set of operations" whether automated or not, including but not limited to "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." The Directive obligates EU Member States to prohibit data transfers to non-European countries that do not have "adequate levels of protection" for personal data. The European Commission has recently released a paper expressing concern that the data protection practices of the United States (self-regulatory codes of conduct) will not be deemed "adequate protection" under the Directive.[38]

PRIVACY LAW

Informational privacy is protected by the Constitution in a limited number of ways. However, constitutional protection extends only to the protection of the individual against government intrusions and does not extend to many of the information privacy threats addressed in this paper. The Fourth Amendment search-and-seizure provision protects a right of privacy by requiring warrants before government may invade one's internal space or by requiring that warrantless invasions be reasonable. A "'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[39] However, "the Fourth Amendment cannot be translated into a general constitutional 'right to privacy.' That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all."[40] Similarly, the Fifth Amendment's self-incrimination clause was once thought of as a source of protection from governmental compulsion to reveal one's private papers,[41] but

---

[36] *Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data, Eur. O.J. L281/31 (Nov. 23, 1995).*

[37] See, *Symposium: Data Protection Law and the European Union's Directive: The Challenge for the United States*, 80 Iowa L.J. 431-734 (1995).

[38] European Commission, *First Orientations on Transfers of Data to Third Countries -- Possible Ways Forward in Assessing Adequacy,* 14 BNA Intl. Trade Rptr. 1338 (July 30, 1997).

[39] *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

[40] *Katz v. United States*, 389 U.S. 347, 350 (1967).

[41] *Boyd v. United States*, 116 U.S. 616, 627-630 (1886).

the Court has refused to interpret the self-incrimination clause as a source of privacy protection.[42] First Amendment principles also bear on privacy, both in the sense of protecting it,[43] but more often in terms of overriding privacy protection in the interests of protecting speech and press.[44] Finally, the due process clause of the Fifth and Fourteenth Amendments, to some degree, may be construed to protect the "liberty" of persons in their privacy rights.[45]

A patchwork of federal statutory laws exists to protect the privacy of certain information. Existing federal statutes do not comprehensively protect the informational privacy interests of individuals and businesses. However, there are several federal laws that extend protection to certain types of information such as credit, cable, video, financial, and federal agency

---

[42] Fisher v. United States, 425 U.S. 391, 399 (1976).

[43] See, e.g., *Frisby v. Schultz*, 487 U.S. 474 (1988)(using privacy rationale in approving governmentally-imposed limits on picketing of home).

[44] See, e.g., *Florida Star v. B. J. F.*, 491 U.S. 524 (1989)(newspaper could not be liable for violating state privacy statute when it published the name of a rape victim that it had lawfully obtained through public sources).

[45] *Whalen v. Roe*, 429 U.S. 589 (1977).

information.[46] There is no comprehensive federal privacy statute, rather Congress has adopted a sector-by-sector approach.

ENCRYPTION

Increasingly individuals and businesses concerned with the privacy and security of information are looking to encryption, the use of highly sophisticated algorithms and ciphers to scramble and descramble information, to provide data security and protection from privacy intrusions and abuses of access to their data. A major purpose of encryption technology is to prevent crimes like industrial espionage and fraud. Although use of encryption products is likely to increase with increased use of personal computers, the need for privacy and security in business communications, referred to as "corporate privacy", is motivating the routine use of encryption software on a widespread global basis. Encryption is likely needed and can be used in any business that conducts commerce electronically.[47]

---

[46] Title III of the **Omnibus Crime Control and Safe Streets Act of 1968** addresses the interception of wire and oral communications. 18 U.S.C. §§ 2510-2521; **The Fair Credit Reporting Act of 1970** (FCRA) regulates the dissemination of consumer credit reports by consumer reporting agencies. 15 U.S.C. § 1681 (amended by Pub. L. No. 104-208); **The Privacy Act of 1974** places limitations on the collection, use, and dissemination of information about an individual maintained by federal agencies. 5 U.S.C. § 552a.; **The Family Educational Rights and Privacy Act of 1974** governs access to student records. 20 U.S.C. § 1232g; **The Tax Reform Act of 1976** restricts the ability of the Internal Revenue Service to disclose individual tax return information. 26 U.S.C. § 6103; **The Right to Financial Privacy Act of 1978** restricts the ability of the federal government to obtain bank records from financial institutions. 12 U.S.C. § 3401; **Cable Communications Policy Act of 1984** limits the disclosure of cable television subscriber names, addresses, and utilization information for mail solicitation purposes. 47 U.S.C. § 551; **The Electronic Communications Privacy Act of 1986** (ECPA) amended the 1968 wiretap statute. It outlaws electronic surveillance, possession of electronic surveillance equipment, and use of information secured through electronic surveillance. The ECPA regulates stored wire and electronic communications (such as voice mail or electronic mail), transactional records access, pen registers, and trap and trace devices. 18 U.S.C. §§ 2510-2522, 2701-2710, 2711; Video Privacy Protection Act of 1988 covers the disclosure of video rental records, 18 U.S.C. § 2710; **Driver's Privacy Protection Act of 1994** (effective October 1997) restricts disclosure of information contained in state motor vehicle records. 18 U.S.C. § 2721; **Health Insurance Portability and Accountability Act of 1996** (Pub. L. No. 104-191, codified at 42 U.S.C. 1320d note) mandates the establishment of uniform standards for the electronic transmission of financial and administrative health information, sets a deadline for congressional action on privacy legislation, and requires the Secretary of Health and Human Services to recommend privacy legislation by August 1997; **Telecommunications Act of 1996** (Pub. L. No. 104-104), section 702 limits the use and disclosure of customer proprietary network information (CPNI) by telecommunications service providers, and provides a right of access for individuals.

[47] See, *Encryption and Banking*, Library of Congress, Congressional Research Service, Rep. No. 97-835A by M. Maureen Murphy, Sep. 15, 1997.

Satisfying the security and privacy needs of businesses and individuals can result in the establishment of barriers to surveillance by government agents seeking to execute wiretap orders. The federal government has a strong interest in preserving its ability to intercept and interpret electronic communications for national security or law enforcement reasons.[48] As encryption technology becomes increasingly available, less expensive and easier to use, the government's access to electronic communications is constricted. The federal government has sought to control the use of encryption technology. Prior to the 1980's, control of the availability and use of cryptography was viewed as a national security issue focused on the U.S. maintaining a technological advantage over other countries and preventing encryption products from becoming available to criminals internationally.[49] Today the availability and use of cryptography has also become a domestic law enforcement issue. Thus, export controls and key recovery encryption are intended to preserve U.S. law enforcement and national security capabilities. Although there is no limit on what kind of encryption can be used in the United States, the government has imposed export controls, limiting the strength of the encryption products that can be sold internationally, on encryption products.[50] These export controls by extension may affect what type of encryption is available domestically.[51]

---

[48] See, *Encryption, Key Recovery & Law Enforcement: Selected Legal Issues and Legislative Proposals*, Library of Congress, Congressional Research Service, by Charles Doyle, Sep. 12, 1997.

[49] U.S. Congress, Office of Technology Assessment, *Issue Update on Information Security and Privacy in Network Environments* at 7, OTA-BP-ITC-147 (Washington, D.C: U.S. Government Printing Office, June 1995).

[50] See, *Encryption Export Controls*, Library of Congress, Congressional Research Service, Rep. No. 97-837A by Jeanne J. Grimmett, Sep. 15, 1997.

[51] See, *Encryption Technology: Congressional Issues,* Library of COngress, Congressional Research Service, IB96039 by Marcia Smith, Sep. 11, 1997.