Order Code RL30322

CRS Report for Congress

Online Privacy Protection: Issues and Developments

September 28, 1999

Gina Marie Stevens
Legislative Attorney
American Law Division

ABSTRACT

This paper discusses some potential threats to the privacy of online personal information, and efforts by businesses, governments, and citizens to respond to them. The paper also provides an overview of the legal framework for the protection of personal information.

Online Privacy Protection: Issues and Developments

Summary

It is routinely acknowledged that the success of the Internet and electronic commerce depends upon the resolution of issues related to the privacy of online personal information. This paper discusses some potential threats to the privacy of online personal information, and efforts by businesses, governments, and citizens to respond to them. The paper also provides an overview of the legal framework for the protection of personal information. Individuals and businesses increasingly rely upon computers to transact business and to access the Internet. Online users may voluntarily disclose personal information, such information is often collected by Web sites for commercial purposes. The proliferation of online personal information has focused the attention of citizens, businesses, and governments on the issue.

Some advocate legal recognition of a right to "information privacy" for online transactions. The term "information privacy" refers to an individual's claim to control the terms under which personal information is acquired, disclosed, and used. In the United States there is no comprehensive legal protection for personal information. The Constitution protects the privacy of personal information in a limited number of ways, and extends only to the protection of the individual against government intrusions. However, many of the threats to the privacy of personal information occur in the private sector. Any limitations placed on the data processing activities of the private sector will be found not in the Constitution but in federal or state law. There is no comprehensive federal privacy statute that protects personal information held by both the public sector and the private sector. A federal statute exists to protect the privacy of personal information collected by the federal government. The private sector's collection and disclosure of personal information has been addressed by Congress on a sector-by-sector basis. With the exception of the Children's Online Privacy Protection Act of 1998, none of these laws specifically covers the collection of online personal information.

The federal government currently has limited authority over the collection and dissemination of personal data collected online. The President's Information Infrastructure Task Force supports industry standards for privacy protection. The Federal Trade Commission Act prohibits unfair and deceptive practices in commerce, and the Commission has brought enforcement actions to address deceptive online information practices. In June 1998, the Federal Trade Commission presented a report to Congress titled *Privacy Online* which examined the information practices of over 1400 commercial Web sites, and found that the vast majority of online businesses have yet to adopt even the most fundamental fair information practice. The Commission issued a new report to Congress in July 1999 *on Self-Regulation and Online Privacy* and found that the vast majority of the sites surveyed collect personal information from consumers online, and that the implementation of fair information practices is not widespread. The Commission believes, however, that legislation to address online privacy is not appropriate at this time.

The 105th Congress passed the Children's Online Privacy Protection Act of 1998. A listing of hearings on online privacy in the 105th and 106th Congress' follows, along with a selected list of bills introduced in the 106th Congress.

Contents

Online Privacy Protection: Issues and Developments

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 online personal information.[1] Privacy is thus thrust to the forefront of policy discussions among businesses, governments, and citizens. Twenty-two 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 potential threats to the privacy of online personal information,[3] and efforts by businesses, governments, and citizens to respond to them. The paper also provides an overview of the legal framework for the protection of personal information.

Threats to the privacy of personal information arise primarily as a result of the widespread increase in the availability and use of computers and computer networks, the corresponding increase in the disclosure of personal information by Internet users to Web sites, the routine collection of personal information about online users by Web sites, and the utilization of online personal information for direct marketing and advertising purposes. The potential harm that can occur from unauthorized disclosures of such information has been well documented.[4] Increased availability of online personal information has contributed to the growth of the information industry.

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

---

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

communications.[5] Congress is currently examining several legislative proposals concerning the availability of encryption products. For a discussion of encryption legislation introduced in the 106th Congress and other related developments, see the CRS Issue Brief 96039, *Encryption Technology: Congressional Issues*.[6]

The Congress,[7] the executive branch,[8] courts,[9] businesses,[10] privacy advocates,[11] Web sites and Internet service providers,[12] and trade associations[13] continue to confront many issues associated with the security and privacy of online personal information.

---

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

[6] See, *Encryption Technology: Congressional Issues,* Library of Congress, Congressional Research Service, CRS Issue Brief 96039 by Richard M. Nunno, Sept. 17, 1999.

[7] For a list of privacy legislation introduced in the 106th Congress see, *EPIC (Electronic Privacy Information Center) Bill Track: Tracking Privacy, Speech, and Cyber-Liberties Bills in the 106th Congress.* Available: [http://epic.org/privacy/bill_track.html]. (March 3, 1999).

[8] 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]; *Privacy Online: A Report to Congress* (June 1998). Available: [http://www.ftc.gov/reports/privacy3/index.htm]; *Self-Regulation and Online Privacy (July 1999).* Available: [http://www.ftc.gov/os/1999/9907/pt071399.htm]; U.S. Govt. Information Infrastructure Task Force, *Options for Promoting Privacy on the National Information Infrastructure* (April 1997). Available: [http://www.iitf.nist.gov/ipc/privacy.htm]; National Telecommunications and Information Administration, *Privacy and Self-Regulation in the Information Age* (June 1997). Available: [http://www.ntia.doc.gov/reports/privacy/privacy_rpt.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).

[9] See, e.g., *McVeigh v. Cohen*, 983 F.Supp. 215 (D.D.C. 1998) (the court held that the Electronic Communications Privacy Act forbids the federal government from seeking information about online communications system users unless: (1) it obtains a warrant issued under the Federal Rules of Criminal Procedure or state equivalent, or (2) it gives prior notice to the online subscriber and then issues a subpoena or receives a court order authorizing disclosure of that information).

[10] See, American Bankers Association, *Financial Privacy in America* (Appendix 3, Web Privacy Statements of Financial Institutions (1998). [Http://www.aba.com].

[11] See, American Civil Liberties Union, *Defend Your Data Campaign.* Available: [http://www.aclu.org/privacy]. Center for Democracy and Technology, *Data Privacy.* Available: [http//:www.cdt.org/privacy]. Electronic Frontier Foundation, *Privacy Archive.* Available: http://www.eff.org/Privacy. Electronic Privacy Information Center, *Surfer Beware II: Notice is not Enough* (June 1998). Available: [http://www.epic.org].

[12] See, Online Privacy Alliance, *Guidelines for Online Privacy Policies.* Available: http://www.privacyalliance.org/resources/ppguidelines.shtml.

[13] Direct Marketing Association, *The DMA's Privacy Promise.* Available: [http://www.the-dma.org]; Individual Reference Services Group, *Self-Regulatory Principles Governing the Dissemination and Use of Personal Data.* Available: http://www.irsg.org/html/industry_principles_principles.htm.

A host of questions are raised by the proliferation of online personal information. Does a business have a right to sell information about its customers without the customer's knowledge or consent? Do consumers desire privacy in online environments? Should the ability of commercial web sites to collect personal information about its customers be regulated? Is industry self-regulation of the privacy of online personal information effective? What enforcement mechanisms exist for online users to remedy unauthorized uses and disclosures of personal information? Are the lack of adequate privacy protections for online personal information a deterrent to consumer participation in electronic commerce?

Background

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 the 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.[14] 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 credit and financial information, health information, tax information, employment information, business information, 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 bulletin board, or to an email recipient.[15] Information about online users is also collected by Web sites through technology which tracks, traces and makes portraits of every interaction with the network.[16] 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

---

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

[15] A report by the National Telecommunications and Information Administration (NTIA) 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, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (1995). Available: [http://www.ntia.doc.gov/ntiahome/privwhitepaper.html].

[16] After a number of media reports and customer complaints, Amazon.com has agreed to modify its recently launched "Purchase Circles" feature which used purchasing data without the permission of customers. Purchase Circles was designed to show bestseller lists by geographic location, industrial and academic sector. Amazon.com agreed to allow individuals to exclude their data and let companies opt out of the company specific listings. See, *Amazon List Stirs Privacy Concerns*, www.washingtonpost.com/wp-srv/business/daily/aug99/amazon27.htm.

computer. Web sites use cookies to track information about user behavior.[17] Web sites contend that the purpose for the use and collection of user data is so the computer receiving the data can send the information file requested to the user's computer, to permit Web site owners to understand activity levels within sites, and to build new Web applications tailored to individual customers.

Technologies like data-mining software facilitate the use of online personal information for commercial 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. 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, health insurance, etc.) has contributed to this phenomenon. Computers make information multi-functional as vast amounts of consumer information are collected, generated, sorted, disseminated electronically, and perhaps sold, with or without consent. How valuable the information is depends in part on how descriptive it is and how it can be used. The Federal Trade Commission and the Department of Commerce recently announced a Public Workshop on Online Profiling to be held November 8, 1999 to assess the impact of "online profiling" — the practice of aggregating information about consumers' interests, gathered primarily by tracking their movements online, and using the profiles to create targeted advertising on Web sites.[18]

One result of these technological advances has been the rapid growth and expansion of the information industry. Basically, there are three major participants in the information industry -- government entities (federal, state, local), direct marketers, and reference services.[19] Generally each of them gathers and distributes personally identifying information. The information may be gathered for one purpose, and sold for another. Public records held by **government entities** contain personally identifying information such as name, address, and social security number. Government records are generally publicly available, and often represent significant sources of revenue for government agencies. **Direct marketers** rely on lists designed to target individuals who are likely to respond to solicitations to determine who should be solicited for a particular product, service, or fund raiser. Frequently, they rent preexisting lists from list brokers who group information such as similar interests, characteristics, and purchasing habits. 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. **Reference services** gather information from a

---

[17] 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].

[18] [http://www.ntia.doc.gov/ntiahome/privacy/workshop/frn-workshop.htm].

[19] This 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].

variety of sources, compile it, and then make it commercially available.[20] Common users of reference services include law firms, private investigators, and law enforcement officials. **Consumer reporting agencies** are also a source of a great deal of information about the consumer's finances.

The proliferation of online personal information, along with several well publicized unauthorized disclosures of and intrusions into online personal information has focused the attention of consumers, privacy advocates, online service providers, Web sites, businesses, trade associations, courts, the Clinton Administration, and the Congress on the protection of online personal information.

The right to privacy has also been characterized as the "the right to be let alone."[21] Some advocate the expansion of this concept to include the right to "information privacy" for online transactions and personally identifiable information.[22] 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.[23] Others urge the construction of a market for personal information, to be viewed no differently than other commodities in the market.[24]

Constitutional Protections. In the United States there is no comprehensive legal protection for personal information. The Constitution protects the privacy of personal information in a limited number of ways, and extends only to the protection of the individual against government intrusions. Constitutional guarantees are not applicable unless "state action" has taken place. Many of the threats to the privacy of personal information addressed in this paper occur in the private sector, and are unlikely to meet the requirements of the "state action" doctrine. As a result, any limitations placed on the data processing activities of the private sector will be found not in the federal Constitution but in federal or state statutory law or common law.

The federal Constitution makes no explicit mention of a 'right of privacy,' and the 'zones of privacy' recognized by the Supreme Court are very limited. 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. 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

---

[20] See, *The Lexis-Nexis P-TRAK Service*, Library of Congress, CRS Report 96-795, by Gina Marie Stevens, Sep. 30, 1996.

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

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

[23] 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].

[24] See, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stanford L. Rev. 1193, 1201 (1998).

go further, and often have nothing to do with privacy at all."[25] 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,[26] but the Court has refused to interpret the self-incrimination clause as a source of privacy protection.[27] First Amendment principles also bear on privacy, both in the sense of protecting it,[28] but more often in terms of overriding privacy protection in the interests of protecting speech and press.[29] 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 in cases that implicate "fundamental rights," or those "implicit in the concept of ordered liberty" such as marriage, procreation, contraception, family relationships, child rearing, and education.[30]

In an important decision in *Whalen v. Roe*,[31] the Supreme Court recognized a 'right of informational privacy.' *Whalen* concerned a New York law that created a centralized state computer file of the names and addresses of all persons who obtained medicines containing narcotics pursuant to a doctor's prescription. Although the Court upheld the state's authority, it found this gathering of information to affect two interests. The first was an "individual interest in avoiding disclosure of personal matters"; the other, "the interest in independence in making certain kinds of important decisions."[32] These two interests rest on the substantive due process protections found in the Fifth and Fourteenth Amendments. The Court commented that it was "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[33]

The first privacy interest that the Supreme Court identified in *Whalen* was in "avoiding disclosure of personal matters." In applying the nondisclosure interest, the Court found that the security measures employed by New York to protect the prescriptions were adequate to ensure that the personal information would be kept from public disclosure. The Court also found that the applicable statutory safeguards adequately protected the interest in avoiding public disclosure of personal information. The second interest identified in *Whalen* focuses on an individual's

---

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

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

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

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

[29] 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).

[30] See, e.g., *Paul v. Davis*, 424 U.S. 693, 713-14 (1976).

[31] 429 U.S. 589 (1977).

[32] *Id.* at 592-93.

[33] *Id.* at 605-06.

"independence in making certain kinds of important decisions."[34] The Court said that the important decision at issue was whether needed medicine would be acquired and utilized. The Court noted that although "some patients [were] reluctant to use, and some doctors reluctant to prescribe," drugs that were medically necessary because of a fear that information would become 'publicly known' and 'adversely affect' their reputation,"[35] "independence in making certain kinds of important decisions," was not violated by New York's data processing activities because the "decision to prescribe, or to use" remained with the physician and the patient.[36] Generally, courts have applied the first interest, that of nondisclosure of personal information in a mixed fashion. In contrast, courts have been reluctant to use the second interest as a bar to a state's information gathering practices.

Statutory Protections. A patchwork of federal laws exists to protect the privacy of certain personal information. There is no comprehensive federal privacy statute that protects personal information held by both the public sector and the private sector. A federal statute exists to protect the privacy of personal information collected by the federal government. The **Privacy Act of 1974** places limitations on the collection, use, and dissemination of information about an individual maintained by federal agencies. The Privacy Act regulates federal government agency recordkeeping and disclosure practices. The Act allows most individuals to seek access to records about themselves, and requires that personal information in agency files be accurate, complete, relevant, and timely. The subject of a record may challenge the accuracy of information. 5 U.S.C. § 552a.

The private sector's collection and disclosure of personal information has been addressed by Congress on a sector-by-sector basis. With the exception of the recently enacted, Children's Online Privacy Protection Act of 1998, none of these laws specifically covers the collection of online personal information. Federal laws extend protection to credit, electronic communications, education, bank account, cable, video, motor vehicle, health, telecommunications subscriber, and children's online information. Following is a description of each statutue.

- **The Fair Credit Reporting Act of 1970** ("FCRA") sets forth rights for individuals and responsibilities for consumer "credit reporting agencies" in connection with the preparation and dissemination of personal information in a consumer report.[37] Under the FCRA consumer reporting agencies are

---

[34] *Id.* at 599-600.

[35] *Id.* at 603.

[36] *Id.* at 603.

[37] 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." 15 U.S.C. § 1681a(d)(1).

prohibited from disclosing consumer reports to anyone who does not have a permissible purpose. 15 U.S.C. § 1681 - 81t;

A consumer report contains identifying information, credit information, public record information, and information on inquiries.

- **The Electronic Communications Privacy Act of 1986** ("ECPA") 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. The ECPA prohibits unauthorized access to stored electronic communications and prohibits the 'provider of an electronic communication service' from disclosing the contents of a communication it stores or transmits. The ECPA also limits a provider's disclosure of transactional data to the government, but not to private parties. 18 U.S.C. §§ 2510-2522, 2701-2711;[38]

- **The Family Educational Rights and Privacy Act of 1974** governs access to and disclosure of educational records to parents, students, and third parties. 20 U.S.C. § 1232g;

- **The Right to Financial Privacy Act of 1978** restricts the ability of the federal government to obtain bank records from financial institutions, and sets forth procedures for the federal government's access to bank customer records. 12 U.S.C. § 3401;

- **The 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 Video Privacy Protection Act of 1988** regulates the treatment of personal information collected in connection with video sales and rentals. 18 U.S.C. § 2710;

- **Driver's Privacy Protection Act of 1994** regulates the use and disclosure of personal information from state motor vehicle records. 18 U.S.C. § 2721;[39]

---

[38] The ECPA was relied upon as the basis for finding that the Navy's actions were illegal in requesting the name of an AOL subscriber without a warrant. Specifically, the court held that the ECPA forbids the federal government from seeking information about online communications system users unless: (1) it obtains a warrant issued under the Federal Rules of Criminal Procedure or state equivalent, or (2) it gives prior notice to the online subscriber and then issues a subpoena or receives a court order authorizing disclosure of that information. *McVeigh v. Cohen*, 983 F.Supp. 215 (D.D.C. 1998).

[39] Several federal courts have considered the constitutionality of the Driver's Privacy Protection Act, see, e.g., *Travis v. Reno*, 163 F.3d 1000 (7th Cir.1998) Petition for Certiorari Filed (No. 98-18), 67 USLW 3717 (May 11, 1999) (restricting disclosure of personal

(continued...)

- **The Health Insurance Portability and Accountability Act of 1996** (P.L. 104-191, codified at 42 U.S.C. 1320d note). The Administration Simplification provisions of the Act set a deadline of August 1999 for congressional action on privacy legislation for electronically transmitted health information, and requires the Secretary of Health and Human Services to issue privacy regulations by February 2000 in the absence of congressional action;

- **Communications Act of 1934**, as amended by the Telecommunications Act of 1996 limits the use and disclosure of customer proprietary network information (CPNI) by telecommunications service providers, and provides a right of access for individuals. 47 U.S.C. § 222;[40]

- **Children's Online Privacy Protection Act of 1998**, requires parental consent to collect a child's age or address, and requires sites collecting information from children to disclose how they plan to use the data. 15 U.S.C. § 6501.

The Administration's Regulation of Internet Privacy

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

---

[39](...continued)
information that states maintain in drivers' records did not exceed Congress's authority under Commerce Clause or Tenth Amendment); *Condon v. Reno*, 155 F.3d 453 (4th Cir. 1998) Certiorari Granted 119 S.Ct. 1753 (May 17, 1999) (No. 98-1464); (Congressional enactment pursuant to its commerce clause power of Federal Driver's Privacy Protection Act violated Tenth Amendment because state officials would be required to administer DPPA, which was not a generally applicable statute); *Pryor v. Reno*, 998 F.Supp.1317 (M.D.Ala.1998) (Congress had rational basis to conclude that disclosure by states of personal motor vehicle records had substantial, apparent effect on interstate commerce, so that federal Driver's Privacy Protection Act came within Congress's authority under commerce clause); *State of Okl. ex rel. Oklahoma Dept. of Public Safety v. U.S.*,161 F.3d 1266 (10th Cir.1998) Petition for Certiorari Filed, 67 USLW 3684 (May 03, 1999)(No. 98-17)(Federal Driver's Privacy Protection Act did not violate Tenth Amendment by invading powers reserved to states; DPPA neither commandeered state legislative process nor conscripted state officials to enforce federal law, but rather involved exercise of Commerce Clause power to legislate regarding driver information, with statute having preemptive effect on contrary state legislation).

[40] Recently the United States Court of Appeals for the Tenth Circuit overturned the Federal Communication Commission's order and proposed rulemaking to restrict the use and disclosure of and access to customer proprietary network information, concluding that the FCC failed to adequately consider the constitutional ramifications of the regulations interpreting § 222 and that the regulations violate the First Amendment. *U.S. West v. F.C.C.*, Slip Op. No. 98-9518 (Aug. 18, 1999). Available: [http://www.kscourts.org/ca10/cases/1999/08/98-9518.htm].

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.[41]

This spring President Clinton named Professor Peter Swire as the Chief Counselor for Privacy in the Office of Management and Budget. Professor Swire previously acted as a consultant to the Department of Commerce. In 1998, Professor swire and Dr. Robert Litan of the Brookings Institution published a book entitled "None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive." The book analyzes the effects of the Data Protection Directive, and addresses other topics, including the effect of privacy laws on electronic commerce, and a general analysis of legal regulation on the Internet.

Federal Trade Commission. The federal government currently has limited authority over the collection and dissemination of personal data collected online. The Federal Trade Commission Act (the "FTC Act")[42] prohibits unfair and deceptive practices in and affecting commerce. The FTC Act authorizes the Commission to seek injunctive and other equitable relief, including redress, for violations of the Act, and provides a basis for government enforcement of certain fair information practices (e.g., failure to comply with stated information practices may constitute a deceptive practice or information practices may be inherently deceptive or unfair). However, as a general matter, the Commission lacks authority to require firms to adopt information practice policies.

The Federal Trade Commission has brought enforcement actions under Section 5 of the Federal Trade Commission Act to address deceptive online information practices. In 1998, GeoCities, operator of one of the most popular sites on the World Wide Web, agreed to settle Commission charges that it had misrepresented the purposes for which it was collecting personal identifying information from children and adults through its online membership application form and registration forms for children's activities. The settlement, which was made final in February 1999, prohibits GeoCities from misrepresenting the purposes for which it collects personal identifying information from or about consumers, including children. It also requires GeoCities to post a prominent privacy notice on its site, to establish a system to obtain parental consent before collecting personal information from children, and to offer individuals from whom it had previously collected personal information an opportunity to have that information deleted.[43] In its second Internet privacy case, the Commission recently announced for public comment a settlement with Liberty Financial Companies, Inc., operator of the Young Investor Web site. The Commission alleged, among other things that the site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously. The consent agreement would require Liberty Financial to post a

---

[41] 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).

[42] 15 U.S.C. §§ 41 et seq.

[43] *GeoCities*, Docket No. C-3849 (Feb. 12, 1999). Available at [http://www.ftc.gov/os/1999/9902/9823015d&o.htm]).

privacy policy on its children's sites and obtain verifiable consent before collecting personal identifying information from children.[44]

In June 1998, the Federal Trade Commission presented its findings in a report to Congress titled *Privacy Online*[45] from an examination of the information practices of over 1400 commercial sites on the World Wide Web, and assessed private industry's efforts to implement self-regulatory programs to protect consumers' online privacy. This report included an analysis of 212 sites directed to children. The FTC identified five core principles of privacy protection which represent 'fair information practices': (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress. The core principles require that: (1) consumers should be given *notice* of an entity's information practices before any personal information is collected from them; (2) consumers should be given *choice* as to how any personal information collected from them may be used; (3) individual's should be given the ability both to *access* data about him or herself and to contest that data's accuracy and completeness; (4) data collectors must take reasonable steps to ensure that data be *accurate and secure*; and (5) an effective *enforcement* mechanism must be in place to enforce the core principles of privacy protection. With these fair information practice principles and industry guidelines as background, the Commission conducted a survey of commercial sites on the World Wide Web.

Although the Commission has encouraged industry to address consumer concerns regarding online privacy through self-regulation, the Commission did not find an effective self-regulatory system. The survey results found that the vast majority of online businesses have yet to adopt even the most fundamental fair information practice (notice/awareness). Moreover, trade association guidelines submitted to the Commission did not reflect industry acceptance of the basic fair information practice principles, nor contain with limited exception the enforcement mechanisms needed for an effective self-regulatory regime. In the specific area of children's online privacy, the Commission recommended that Congress develop legislation placing parents in control of the online collection and use of personal information from their children.

The Commission issued a new report to Congress in July 1999 on *Self-Regulation and Online Privacy*[46] that assessed the progress made in self-regulation to protect consumers' online privacy since its June 1998 report, and set out an agenda of Commission actions to encourage implementation of online privacy protections. The Commission found that there has been notable progress in self-regulatory initiatives, and that surveys of commercial Web sites suggest that online businesses are providing significantly more notice of their information practices. However, it found that the vast majority of the sites surveyed collect personal information from consumers online, and that the implementation of fair information practices is not widespread. In light of these results, the Commission believes that

---

[44] *Liberty Financial*, Case No. 9823522. Available at [http://www.ftc.gov/os/1999/9905/lbtyord.htm]).

[45] [http://www.ftc.gov/reports/privacy3/index.htm].

[46] [http://www.ftc.gov/os/1999/9907/pt071399.htm].

further improvements are required to effectively protect consumers' online privacy. In the Commission's view, the emergence of online privacy seal programs (TRUSTe,[47] BBBOnLine,[48] and other online privacy seal programs) is a promising development in self-regulation. These programs require their licensees to abide by codes of online information practices and to submit to compliance monitoring in order to display a privacy seal on their Web site. However, the Commission found that only a handful of all Web sites currently participate in online privacy seal programs, and that as a result it is too early to judge how effective these programs will be. The Commission believes that legislation to address online privacy is not appropriate at this time.

In response to these findings, the Commission developed an agenda to address online privacy issues, and to assess progress in self-regulation to protect consumer online privacy:

- The Commission will hold a public workshop on "online profiling," jointly sponsored by the Department of Commerce, to examine online advertising firms' use of tracking technologies to create user profile-based advertising.

- The Commission will hold a public workshop on the privacy implications of electronic identifiers that enhance Web sites' ability to track consumers' online behavior.

- The Commission will convene task forces of industry representatives and privacy and consumer advocates to develop strategies for furthering the implementation of fair information practices in the online environment.

- The Commission, in partnership with the Department of Commerce, will promote private sector business education initiatives designed to encourage new online entrepreneurs to adopt fair information practices.

- The Commission will conduct an online survey to reassess progress in Web sites' implementation of fair information practices, and will report to Congress.

The European Union Directive on the Protection of Personal Data. The European Union Directive on the Protection of Personal Data became effective October 1998.[49] 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," about European Union citizens. It will require each of the sixteen EU member states to enact laws governing the "processing of personal data." Significantly, 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 expressed concern that

---

[47] [http://www.truste.org/about/about_committee.html].

[48] [http://www.bbbonline.com].

[49] *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).*

the data protection practices of the United States (e.g., self-regulatory privacy initiatives) will not be deemed "adequate protection" under the Directive.[50]

U.S. and EU officials have been engaged in informal dialogue concerning implementation of the directive. The dialogue focuses on the goals of enhancing data protection for European citizens while maintaining the free flow of personal information between Europe and the United States. The European Commission has stated that while it will try to avoid disruptions of transborder data flows, the directive is still in force during this dialogue period.

On November 4, 1998, U.S. Department of Commerce Undersecretary for Internal Trade David L. Aaron issued a memorandum explaining the EU Data Protection Directive, and also issued "safe harbor" privacy principles. The safe harbors were created to permit industries that adhere to the principles to continue transborder data transfers with EU Member states. They are to be used solely by U.S. organizations transferring personal information from the European Union to the United States. There are seven safe harbor privacy principles: notice, choice, onward transfer, security, data integrity, access, and enforcement. The principles are not intended to govern or affect U.S. privacy regimes.

Undersecretary Aaron stated that organizations that are within the safe harbor would have a presumption of adequacy and data transfers from the European Community to them would continue. Organizations can come within the safe harbor by self certifying that they adhere to these privacy principles. A joint report from the European Commission's services and the US Department of Commerce on the EU/US Data Protection Dialogue was presented to the EU/US Summit in June.[51]

Congressional Initiatives

The Children's Online Privacy Protection Act of 1998. In response to the concerns over the privacy of children's online personal information, the 105th Congress passed the Children's Online Privacy Protection Act of 1998[52] to prohibit unfair and deceptive acts and practices in connection with the collection and use of personally identifiable information from and about children on the Internet. The goals of the Act are: to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; to help protect the safety of children in online fora such as chat rooms, home pages, and pen-pal services in which children may make public postings of identifying information; to maintain the security of children's personal information collected online; and to limit the collection of personal information from children without parental consent.

---

[50] 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).

[51] [http://www.ita.doc.gov/ecom/jointreport2617.htm].

[52] Title XIII, Omnibus Consolidated and Emergency Supplemental Appropriations Act, P.L. 105-277, 112 Stat. 2681, 15 U.S.C. § 6501 (Oct. 21, 1998).

Section 1303 of the Act directs the FTC to adopt regulations prohibiting unfair and deceptive acts and practices in connection with the collection and use of personal information from and about children on the Internet. Section 1303(b) sets forth a series of privacy protections to prevent unfair and deceptive online information collection from or about children. The Act specifies that operators of websites directed to children or who knowingly collect personal information from children (1) provide parents notice of their information practices; (2) obtain prior parental consent for the collection, use and/or disclosure of personal information from children (with certain limited exceptions for the collection of online information e.g., email address); (3) provide a parent, upon request, with the ability to review personal information collected from his/her child; (4) provide a parent with the opportunity to prevent the further use of personal information that has already been collected, or the future collection of personal information from that child; (5) limit collection of personal information for a child's online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity; and (6) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected.

The Act authorizes the Commission to bring enforcement actions for violations of the final rule in the same manner as for other rules defining unfair and deceptive trade acts or practices under section 5 of the Federal Trade Commission Act. In addition, section 1305 of the Act authorizes state attorneys general to enforce compliance with the final rule by filing actions in federal court after serving prior written notice upon the Commission when feasible. On April 20, 1999, the Commission published a Federal Register notice seeking public comment on its proposed regulations under the Children's Online Privacy Protection Act of 1998.[53] The proposed rule states that "[a]n operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent." The Commission expects to issue a final rule this fall.

Congressional Hearings. A chronological listing of congressional hearings on online privacy in the 105th and 106th Congress' follows. Hearing testimony can be found at www.senate.gov and www.house.gov.

Online Privacy hearing before the Senate Subcommittee on Communications, Committee on Commerce, Science, and Transportation, 106th Cong., July 27, 1999.

Electronic Commerce: Current Status of Privacy Protections for Online Consumers hearing before the House Subcommittee on Telecommunications, Trade and Consumer Protection, Committee on Commerce , 106th Cong., July 13, 1999.

Website Privacy Disclosure hearing before the House Subcommittee on Courts and Intellectual Property, Committee on the Judiciary, 106th Cong., May 27, 1999.

---

[53] 64 Fed. Reg. 22750 (April 27, 1999).

Privacy in the Digital Age: Discussion of Issues Surrounding the Internet hearing before the Senate Judiciary Committee, 106th Cong., Apr. 21, 1999.

Internet Privacy hearing before the Senate Communications Subcommittee, Committee on Commerce, Science, and Transportation, 105th Cong., September. 23, 1998.

Privacy in Cyberspace hearing before the House Subcommittee on Telecommunications, Trade, and Consumer Protection, Committee on Commerce, 105th Cong., July 21, 1998

Privacy in Electronic Communications hearing before the House Subcommittee on Courts and Intellectual Property, Committee on the Judiciary, 105th Cong., March 26, 1998.

Privacy in the Digital Age: Encryption and Mandatory Access hearing before the Senate Subcommittee on the Constitution, Federalism, and Property Rights, Committee on the Judiciary, 105th Cong., March 17, 1998

Legislation in the 106th Congress. A list of selected bills introduced in the 106th Congress which focus on the protection of online personal information follows:

H.R.313 *Consumer Internet Privacy Protection Act of 1999* (Rep. Bruce Vento) to regulate the use by interactive computer services of personally identifiable information provided by subscribers to such services.

H.R.367 *Social Security On-line Protection Act of 1999* (Rep. Bob Franks) to regulate the use by interactive computer services of Social Security account numbers and related personally identifiable information.

H.R. 369 *Children's Privacy Protection and Parental Empowerment Act of 1999* (Rep. Bob Franks) to prohibit the sale of personal information about children without their parents' consent, and for other purposes.

S.809 *Online Privacy Protection Act* (Sen. Conrad Burns and Sen. Ron Wyden) to require the Federal Trade Commission to prescribe regulations to protect the privacy of personal information collected from and about private individuals who are not covered by the Children's Online Privacy Protection Act of 1998 on the Internet, to provide greater individual control over the collection and use of that information, and for other purposes. Hearings held July 27, 1999.