Order Code RL30322

CRS Report for Congress

Received through the CRS Web

Online Privacy Protection: Issues and Developments

Updated January 11, 2001

Gina Marie Stevens
Legislative Attorney
American Law Division

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.

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. President Clinton'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 FTC issued a new report in May 2000 after another survey of web sites. Notwithstanding measurable gains since the 1999 report to Congress, a majority of the Commission found that self-regulation alone, without some legislation, is unlikely to provide online consumers with the level of protection they seek and deserve, and recommended that Congress consider legislation to complement self-regulation.

This report does not track legislation pending before 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 communications.[5] For a discussion of encryption legislation introduced in the 106th

---

[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] The complex issues related to the privacy of medical information are beyond the scope of this report. For further information see CRS Issue Brief 98002, *Medical Records Privacy*.

[4] See, J. Rosen, The Unwanted Gaze: The Destruction of Privacy in American (2000).

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

Congress and other related developments, see the CRS Issue Brief IB96039, *Encryption Technology: Congressional Issues*.[6]

The Congress,[7] the executive branch,[8] courts,[9] state attorney generals,[10] businesses,[11] privacy advocates,[12] and industry groups.[13] continue to confront many issues associated with the security and privacy of online personal information.

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?

---

[6] See CRS Issue Brief IB96039, *Encryption Technology: Congressional Issues*, by Richard M. Nunno.

[7] For a list of Internet privacy legislation introduced in the 106th Congress see, CRS Report RL30784, *Internet Privacy: An Analysis of Technology and Policy Issues*, by Marcia S. Smith.

[8] See following discussion of the Clinton Administration's Regulation of Privacy.

[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] Michigan Department of Attorney General, Consumer Protection Division, *In the Matter of Doubleclick, Inc.* AG File No. 200002052, Feb. 17, 2000; New York State Office of Attorney General, Bureau of Consumer Frauds and Protection, *In the Matter InfoBeat LLC.*, Jan. 25, 2000; New York Senate Majority *Task Force on the Invasion of Privacy*, Mar. 2000; Washington *Consumer Privacy Workgroup Report to the Attorney General*, Jan. 10, 2000.

[11] See, American Bankers Association, "Financial Privacy in America: A Review of Consumer Financial Issues," (June 1998). [http://www.aba.com/aba/ABANews&Issues/PR_012298pp.asp.8). [http://www.aba.com].

[12] 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].

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

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 72 million host computers worldwide in 2000, with 103.6 million U.S. households online.[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 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.

---

[14] *See,* J. Eisenach *et al.,* The Digital Economy Fact Book 2-8, (2d Ed. 2000).

[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].

[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].

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 held a Public Workshop on Online Profiling 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 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.

---

[18] U.S. Federal Trade Commission, *Online Profiling: A Report to Congress* (June 2000) [http://www.ftc.gov/privacy/index.html].

[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].

[20] See CRS Report 96-795, *The Lexis-Nexis P-TRAK Service*, by Gina Marie Stevens.

Legal Framework for 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 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]

---

[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).

[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).

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.

In the Supreme Court’s October 1999 term, it addressed the constitutionality of the Driver’s Privacy Protection Act of 1994 (DPPA), which regulates the use and disclosure by state motor vehicle departments of personal information from motor vehicle records.[33] In *Reno v. Condon*, the Court unanimously held that the DPPA is a valid exercise of the commerce power, and does not violate the Tenth Amendment.[34] The DPPA prohibits state departments of motor vehicles (DMVs) and others to whom the DMVs provide information from disclosing a driver’s personal information (name, address, phone number, vehicle description, social security number, etc.) without the driver’s consent. DMVs that violate the Act are subject to civil penalties. The driver’s information that the DPPA regulates is used by insurers, marketers, and others engaged in interstate commerce to contact drivers with customized solicitations, and therefore this information in this context constitutes “an article of commerce” subject to regulation under the commerce power. The Court held that the DPPA does not violate the federalism principles reflected in the Tenth Amendment. Although the Court found that compliance with the DPPA will require time and effort on the part of state employees, the DPPA did not “commander” states in enforcing federal law applicable to private entities. The DPPA regulates state activities directly rather than seeking to control the manner in which states regulate private parties.

---

[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] 18 U.S.C. § 2721.

[34] 120 S. Ct. 666, 68 USLW 4138 (2000)

Also, the DPPA is generally applicable, regulating both the states as initial suppliers and private entities that resell drivers' information.

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.[35] The **Privacy Act of 1974** (5 U.S.C. § 552a) places limitations on the collection, use, and dissemination of information about an individual maintained by federal agencies. It is not limited to online personal information. It provides that "[a]n agency may not disclose any record regarding an individual to any person or another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains."[36] 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.

The **Freedom of Information Act** (5 U.S.C. § 552) requires federal agencies, subject to certain exceptions, to make their records available upon request. Exempted from this requirement are "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[37]

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, children's online information, and financial information. Following is a description of each statute.

- **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.[38] Under the FCRA consumer reporting agencies are

---

[35] See CRS Report RL30671, *Personal Privacy Protection: The Legislative Response*, by Harold C. Relyea.

[36] 5 U.S.C. § 552a(b).

[37] *Id.* at § 552(b)(6).

[38] 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

(continued...)

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

- **The Electronic Communications Privacy Act of 1986** ("ECPA") added "electronic communications" to the federal 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. 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, 3121-3126;[39]

- **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;

---

[38](...continued)
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). A consumer report contains identifying information, credit information, public record information, and information on inquiries.

[39] 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).

- **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 required the Secretary of Health and Human Services to issue final privacy regulations by February 2000 in the absence of congressional action. The Secretary of DHHS issues the final privacy rule on December 26, 2000 to become effective on February 26, 2001;[40]

- **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;[41]

- **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 Gramm-Leach-Bliley Act of 1999**,[42] in Title V of Subtitle A, requires financial institutions to disclose their privacy policies to their customers. Customers may opt out of sharing of personal information, and the institutions may not share account numbers with non-affiliated telemarketers and direct marketers.[43]

The Clinton Administration's Regulation of Internet Privacy

In 1995, the Privacy Working Group of the White House's Information Infrastructure Task Force issued a White Paper outlining "Principles for Providing and Using Personal Information."[44] In 1997 the Information Infrastructure Task Force recommended a market-oriented non-regulatory strategy to promote global electronic commerce on the Internet,[45] and supported industry developed standards for privacy protection.[46] In March 1997, the Federal Reserve issued a Report to Congress on the

---

[40] 65 F.R. 82462-82829 (Dec. 28, 2000).

[41] *U.S. West v. F.C.C.*,182 F.3d 1224 (10th Cir. 1999)(Court held that Federal Communication Commission's order and proposed rulemaking to restrict the use and disclosure of and access to customer proprietary network information violated the First Amendment).

[42] Pub. L. No. 106-202, 113 Stat. 1338.

[43] *Id*. at §§ 501, 502, 503. *See*, CRS Report RS20185, *Privacy Protection for Customer Financial Information*, by M. Maureen Murphy.

[44] *See* http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html.

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

[46] U.S. Govt. Information Infrastructure Task Force, *Options for Promoting Privacy*

(continued...)

availability of consumer financial information,[47] and issued another report in November 1999 on bank and savings associations web sites and their posted privacy policies and information practices.[48]

Federal Trade Commission. The federal government currently has limited authority over the collection and dissemination of personal data collected online. [49] The Federal Trade Commission Act (the "FTC Act")[50] 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, the Commission has noted that, as a general matter, it lacks authority to require firms to adopt information practice policies.[51]

Beginning in 1995, the Federal Trade Commission held a series of public workshops on the issues of privacy and the Internet. In part based upon these workshops, the FTC has issued several reports to Congress in connection with its efforts to encourage self-regulation by industry of its privacy practices.[52]

In June 1998, the Federal Trade Commission presented a report to Congress titled *Privacy Online*[53] based upon its 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. The report included an analysis of 212 sites directed to children. The FTC examined the privacy practices of the surveyed web sites in light of five core principles of

---

[46](...continued)
on the National Information Infrastructure, April 1997. Available at [http://www.iitf.nist.gov/ipc/privacy.htm]privacy.pdf].

[47] 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 at [http:// www.bog.frb.fed.us/boarddocs/RptCongress/

[48] [http://www.federalreserve.gov/Board/docs/Press/General/1999/19991109/privacy.pdf].

[49] Note that there may be constitutional limitations on the ability of government to legislate and regulate personal privacy. *See U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1234-36 (10th Cir. 1999) (Court holds that FTC order restricting the use and disclosure of and access to "customer proprietary network information" violated the First Amendment).

[50] 15 U.S.C. §§ 41 et seq.

[51] 1998 FTC Report to Congress at 41.

[52] See, U.S. Federal Trade Commission, *Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure*, December 1996; *Privacy Online: A Report to Congress*, June 1998; *Self-Regulation and Online Privacy, July 1999; Privacy Online: Fair Information Practices in the Electronic Marketplace – A Report to Congress*, May 2000. Reports and transcripts are available at http://www.ftc.gov/privacy/reports.htm.

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

privacy protection: (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 had 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 1998 report the Commission concluded that greater incentives were needed to encourage self-regulation and ensure widespread implementation of the basic privacy principles. 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.

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[54] 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 Act specifies that operators of websites or online services directed to children or an operator 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.

---

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

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. The final rule was issued in October 1999, and became effective April 21, 2000.[55]

The Commission issued a new report to Congress in July 1999 on *Self-Regulation and Online Privacy*[56] that assessed the progress made since its 1998 report, and set an agenda for Commission actions to encourage implementation of online privacy protections. The Commission found notable progress in self-regulatory initiatives, and that online businesses were providing significantly more notice of their information practices. However, it also found that the vast majority of the sites surveyed collected personal information from consumers online, and that the implementation of fair information practices was not widespread. The FTC found the emergence of online privacy seal programs (TRUSTe,[57] BBBOnLine,[58] and other online privacy seal programs) to be 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 was too early to judge how effective these programs will be. In light of its preferred approach to privacy protection through self-regulation, the Commission concluded that legislation to address online privacy was not appropriate at the time.
Instead, the Commission developed an agenda to address online privacy issues, and identified areas where industry could improve on: continue to encourage widespread adoption of fair information practices; ensure that companies adhere to the core privacy principles; and educate consumers about privacy protection on the Internet.

The FTC issued a new report in May 2000 after another survey of web sites.[59] As Chairman Pitofsky stated in the report the issue before the Commission was not whether self-regulation succeeded or failed but rather "whether the progress of online implementation of Fair Information Practice Principles continues to suggest that no legislation is warranted." Notwithstanding measurable gains since the 1999 report to Congress, a majority of the Commission found that self-regulation alone, without some legislation, is unlikely to provide online consumers with the level of protection they seek and deserve. Accordingly, a majority of the Commission recommended that Congress consider legislation to complement self-regulation.

---

[55] 16 C.F.R. § 312.

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

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

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

[59] *Privacy Online: Fair Information Practices in the Electronic Marketplace – A Report to Congress*, May 2000. [http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf].

Enforcement Actions Under § 5 of the Federal Trade Commission Act. 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.[60]

In its second Internet privacy case, the Commission settled 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 requires Liberty Financial to post a privacy policy on its children's sites and obtain verifiable consent before collecting personal identifying information from children.[61] In January 2000, the FTC filed a complaint against Reverseauction.com, Inc. alleging that Reverseauction.com had improperly obtained the email addresses, user identification names and feedback ratings of various eBay customers, and then allegedly sent out unsolicited emails to those customers.[62] In February 2000, the privacy organization EPIC filed a complaint with the FTC charging DoubleClick, Inc. with violations of the Federal Trade Act. Several other groups also filed statements in support of the complaint.[63] In response to market pressures and pending lawsuits, DoubleClick discontinued its allegedly unfair and deceptive trade practices.

The FTC also settled charges against Toysmart.com[64] that the company had violated Section 5 of the FTC Act by misrepresenting to consumers that personal information would never be shared with third parties and then disclosing, selling, or offering that information for sale in violation of the company's own privacy statement. The agreement forbids the sale of this customer information except under very limited circumstances. The company, currently in Chapter 11 bankruptcy, made a motion to

---

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

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

[62] *Federal Trade Commission v. Reverseauctions.com, Inc.*, Civil Action No. 000032 (D.D.C.) Available at http://www.ftc.gov/os/2000/01/reversecmp.htm.

[63] EPIC Complaint, available at http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf.

[64] *FTC v. Toysmart.com, LLC, and Toysmart.com, Inc.* (Civil Action 00-11341-RGS) (D. Mass. 2000).

sell its assets, including the customer information. Under the settlement agreement, Toysmart was required to file an order in Bankruptcy Court prohibiting Toysmart from selling the customer list as a stand-alone asset. The settlement only allows a sale of such lists as a package which includes the entire Web site, and only to a "Qualified Buyer"-- an entity that is in a related market and that expressly agrees to be Toysmart's successor-in-interest as to the customer information. The Qualified Buyer must abide by the terms of the Toysmart privacy statement. If the buyer wishes to make changes to that policy, it must follow certain procedures to protect consumers. It may not change how the information previously collected by Toysmart is used, unless it provides notice to consumers and obtains their affirmative consent ("opt-in") to the new uses. In the event that the Bankruptcy Court does not approve the sale of the customer information to a Qualified Buyer or a plan of reorganization within the next year, Toysmart must delete or destroy all customer information. In the interim, Toysmart is obligated to abide by its privacy statement.

The European Union Directive on the Protection of Personal Data. The European Union Directive on the Protection of Personal Data became effective October 1998.[65] 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 requires 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 some of the data protection practices of the United States (e.g., self-regulatory privacy initiatives) will not be deemed "adequate protection" under the Directive.[66] U.S. and EU officials engaged in informal dialogue concerning implementation of the directive. The dialogue focused on the goals of enhancing data protection for European citizens while maintaining the free flow of personal information between Europe and the United States.

On November 4, 1998, former U.S. Department of Commerce Undersecretary for International Trade David L. Aaron proposed a “safe harbor” for U.S. companies that choose to adhere to certain privacy principles. The safe harbor was created to permit U.S. companies that voluntarily adhere to the principles to continue transborder data transfers with EU Member states. The principles are designed to serve as guidance to U.S. organizations seeking to comply with the "adequacy" requirement of the directive, and would provide organizations within the safe harbor with a presumption of adequacy and data transfers from the European Community to them could continue. Organizations would come into the safe harbor by self-certifying that they adhere to these privacy principles. In April 1999, the Department issued revised draft principles and a set of frequently asked questions (FAQs)

---

[65] *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).*

[66] 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).

providing guidance for the implementation of the principles as well as an enforcement overview that would form the basis of the safe harbor arrangement.

On November 15, 1999, the Department of Commerce posted on its website documents related to the safe harbor.[67] The seven International Safe Harbor Privacy Principles proposed by the Department of Commerce are: notice, choice, onward transfer, security, data integrity, access, and enforcement.

The "notice" principle requires an organization to inform individuals about the personal information it collects about them. The "choice" principle requires organizations to give individuals the opportunity to choose whether and how their personal information is used. The "onward transfer" principle gives individuals the choice over whether and the manner in which their information is used by a third party. The "security" principle requires reasonable measures to be taken to assure information is used for its intended purpose and to protect it. The "data integrity" principle requires that data be accurate, complete, current, and relevant. The "access" principle provides individuals with reasonable access to their information and the opportunity to correct, amend, or delete inaccurate information except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy, or where the rights of another would be violated. The "enforcement" principle establishes mechanisms for ensuring compliance with the principles that include independent recourse mechanisms, systems to verify the privacy practices of businesses, and obligations to remedy implementation problems arising from the principles. The principles are not intended to govern or affect U.S. privacy regimes.

On December 3, 1999, the Data Protection Working Party of the European Commission released its opinion on the Level of Data Protection provided by the "Safe Harbor" Principles and the Frequently Asked Questions issued on November 15 and 16, 1999 by the Department of Commerce. The Working Party concluded that the proposed "Safe Harbor" arrangements in the various documents remain unsatisfactory. The Working Party invited the Commission to urge the U.S. to make a number of improvements[68]

On March 14, 2000, the European Commission and the United States finalized the "safe harbor agreement". The EU's Article 31 Committee, which represents Member states, failed to approve the agreement at its March 30 meeting. It decided to delay a vote until its May meeting on the agreement. On May 31, the European Union's Member states voted unanimously to approve the U.S. proposed safe harbor principles at a U.S.-EU summit held in Lisbon, Portugal.[69] The European Parliament rejected the safe harbor agreement. The safe harbor agreement went into effect on November 1, 2000.[70]

---

[67] [http://www.ita.doc.gov/td/ecom/menu.html].

[68] [http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp27en.htm].

[69] [http://www.ita.doc.gov/td/ecom/menu.html].

[70] [http://www.europa.eu.int/internal_market/en/media/dataprot/news/safeharbor.htm].

Decisions to qualify for the safe harbor privacy are entirely voluntary, and organizations may qualify for the safe harbor in different ways. In order to obtain and retain recognition that they provide an adequate level of protection for the transfer of data from the EU to the United States, organizations must comply with the Principles and FAQs, and publicly disclose that they do so. For example, according to the principles, if an organization joins a self regulatory privacy program that adheres to the principles, it qualifies for the safe harbor. They may also qualify for the safe harbor by developing their own self regulatory privacy policies that adhere to the safe harbor principles.

Where an organization relies on self regulation to comply with the principles, failure to comply with self regulation is actionable under § 5 of the Federal Trade Act prohibiting unfair or deceptive trade practices or another law or regulation prohibiting such acts. With respect to air carriers, the principles and FAQs will be enforced by the Department of Transportation. In addition, organizations subject to a statutory, regulatory, administrative or other body of law (or of rules) that protects personal privacy may also qualify for safe harbor benefits. Sectors and/or data processing not subject to the jurisdiction of any of the government entities listed fall outside the scope of agreement. The Department of Commerce has agreed to maintain and make available to the public a list of organizations self-certifying their adherence to the principles, and will update the list on an annual basis. Safe harbor benefits are assured from the date on which an organization self-certifies to the Department of Commerce its adherence to the principles. It would be up to either a U.S. government body (*e.g.*, the Federal Trade Commission or the courts) or a U.S. self-regulatory body (*e.g.*, BBB Online or Trust-E) to enforce the terms of the safe harbor. U.S. companies have one year from implementation of the directive to apply the safe harbor principles.