Order Code RS21221
May 21, 2002

Privacy Protection for Online Information

Gina Marie Stevens
Legislative Attorney
American Law Division

Summary

This report focuses on one aspect of online privacy – collection, use, and dissemination of data via the Internet, and discusses related federal privacy laws and selected legislation. This report will be updated as developments warrant.

At the end of the 19th century, a seminal law review article was published that developed the basic principle of American privacy law – the "right to be let alone." The article was written in response to invasions of personal privacy caused by the technological innovations of mass printing (newspapers) and the portable camera (photographs). Following this article, American common law jurisprudence developed four distinct tort remedies to protect personal privacy: false light; misappropriation; public disclosure of private facts; and intrusion upon seclusion. With the late 20th century technological innovations of the Internet and the World Wide Web, the collection, use, and dissemination of electronic personal information is potentially much more invasive. The unique aspects of information collection via the Internet, the ability to create detailed profiles of Internet users, and the capability of computer networks to quickly and inexpensively compile, analyze, share, and match digitized information, are some of the reasons that online privacy[1] has become the subject of so much concern.

Background. Individuals and businesses increasingly rely upon computers and computer networks for personal and business transactions. This has resulted in the creation of vast amounts of individually identifying personal information. Online users may voluntarily disclose personally identifying information, for example, to an Internet 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. Privacy

[1] The term "online privacy" includes several different subjects such as government surveillance of online activities, the rights of employers to monitor employee activities, the collection, use, and dissemination of data via the Internet, and computer security issues. This report focuses on one aspect of online privacy – collection, use, and dissemination of data via the Internet. For information on other internet privacy issues, see CRS Report RL31408, *Internet Privacy: Overview and Pending Legislation*; CRS Report RL31377, *The USA Patriot Act: A Legal Analysis*; CRS Report RL30322, *Online Privacy Protection: Issues and Developments.*

advocates typically object to the misuse of this "actively collected" information. Information about online users is also collected, sometimes without the user's knowledge or consent, by Web sites through technology that routinely tracks, traces and makes portraits of every interaction with the network. This is accomplished through the use of passive collection technologies such as cookies or clear graphic interchange formats (GIFs). Technology like data-mining software and the practice of online profiling[2] facilitate the use of online personal information for commercial purposes. Privacy advocates have expressed a great deal of concern over the collection, use, or dissemination of personal information online, and over the fact that the common law remedies for invasion of privacy generally do not provide adequate protection of personal privacy on the Internet. The inadequacy of common law remedies for redressing privacy "wrongs" has led to efforts to seek government regulation of data collection through new legislation and existing statutes.

Accidental or intentional invasions of privacy by an Internet Service Provider, an online service provider, or an online advertiser might result in Federal Trade Commission enforcement actions, state attorneys general investigations, private lawsuits, negative publicity, deflated stock prices, or diminished revenues. The courts have recently addressed many online privacy issues in cases brought by individuals alleging that various online activities have violated the privacy rights of Internet users.[3] The cases illustrate some of the challenges courts face as they apply statutory and common law concepts of privacy to these new technologies. With respect to federal claims, plaintiffs have alleged violations of the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and the Federal Wiretap Act. State law claims are based upon Unfair Trade Practices Acts, consumer protection acts, invasion of privacy torts, and trespass.

Federal Privacy Laws, and Online Privacy Laws. There are three major privacy laws that regulate nongovernmental use of personal data that are applicable to the online environment. The Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and the Children's Online Privacy Protection Act. The Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C. §§ 2701 *et seq.*, prohibits 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

---

[2] Online profiling refers to 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. See Federal Trade Commission, *Online Profiling: A Report to Congress* (Pts. 1 and 2)(2000),
[http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf]

[3] See *In re DoubleClick, Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001); *In re Intuit Privacy Litigation*, 137 F. Supp. 2d 1272 (C.D.Cal. 2001); *In re American Online, Inc. Version 5.0 Software Litigation*, 2001 U.S. Dist. LEXIS 6595 (S.D. Fla. April 19, 2001); *In re Real Networks, Inc. Privacy Litigation*, Docket No. 1329, 2000 U.S. Dist. LEXIS 1458 (J.P.M.L. Feb. 10, 2000).; *Supnick v. Amazon.com*, No. C00-0221P, 2000 U.S. Dist. LEXIS 7073 (W.D. Wash. May 19, 2000); *In re Toys 'R Us, Inc., Privacy Litigation*, Docket No. 1381, 2000 U.S. Dist. LEXIS 18658 (J.P.M.L. Dec. 20, 2000); *In re Pharmatrak, Inc. Privacy Litigation*, Docket No. 1400, 2001 U.S. Dist. LEXIS 5228 (J.P.M.L. Apr. 18, 2001)

communication service from disclosing the contents of stored communications. The ECPA includes both civil and criminal penalties, authorizes private lawsuits and provides for the recovery of economic and in some cases punitive damages as well as costs and attorney fees. The federal wiretap statute, 18 U.S.C. §§ 2510 *et seq.* addresses disclosure of the contents of electronic mail, radio communications, data transmission and telephone calls. The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. §§ 1030 *et seq.*, pertains to federal and interstate computer crimes. It applies to any unauthorized access to computers of "federal interest." Essentially it applies to any computer when access is provided through the Internet. The CFAA provides both civil (economic damages only) and criminal penalties, and authorizes private lawsuits where damages exceed $5,000.

The Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. § 6501, applies to children under 13 years of age and requires parental consent to collect a child's age or address online, and requires sites collecting information from children to disclose how they plan to use the data. COPPA specifies that operators of websites or online services directed to children, must among other things, (1) provide parents notice of their information practices; (2) obtain prior parental consent for the collection, use, or disclosure of personal information from children; and (3) provide a parent, upon request, with the ability to review personal information collected from his/her child. The Act authorizes the Commission to bring enforcement actions for violations as unfair and deceptive trade acts or practices under section 5 of the Federal Trade Commission Act.[4] COPPA also authorizes state attorneys general to file federal actions.

There is no omnibus federal privacy statute that protects online personal information.[5] Rather, a patchwork of industry-specific federal laws exists to protect the privacy of certain personal information.[6] The Privacy Act of 1974 (5 U.S.C. § 552a) protects the privacy of personal information collected by the federal government, and places limitations on the collection, use, and dissemination of information about an individual maintained by federal agencies. Congress has enacted the following laws for the protection of credit, education, bank, video, motor vehicle, health, and financial information: the Fair Credit Reporting Act of 1970 (15 U.S. C. §§ 1681 *et seq.*) regulates the credit industry;[7] the Family Educational Rights and Privacy Act of 1974 (20 U.S.C. § 1232g) governs access to and disclosure of education records; the Right to Financial Privacy Act of 1978 (12 U.S.C. § 3401 *et seq.*) regulates the disclosure of bank records

---

[4] For information on FTC enforcement action under COPPA, see *Three Web Operators Agree to Pay Civil Penalties to Settle Violations of the Children's Online Privacy Protection Act*, [http://www.ftc.gov/opa/2001/04/girlslife.htm].

[5] For information on other privacy statutes, see CRS Report RL30671, *Personal Privacy Protection: The Legislative Response*; CRS Report RS20185, *Privacy Protection for Customer Financial Information*; and CRS Report RS20934, *A Brief Summary of the Medical Privacy Rule*.

[6] Note that there maybe constitutional limitations on the ability of the government to regulate personal privacy. See *U.S. West v. FCC*, 182 F.3d 1224 (10th Cir. 1999)(held that FTC order restricting use and disclosure of customer proprietary information by telecommunications carriers by violated the free speech clause of the First Amendment).

[7] In 1999 U.S. Bancorp settled a complaint for $7 million brought by the Minnesota Attorney General under the FCRA. The company was accused of sharing credit card information, some of which was gathered online via the company's web site, with third party marketing companies. U.S. Bancorp subsequently settled a similar complaint with the attorneys general of 38 states and the District of Columbia, [http://www.ag.state.mn.us/consumer/Privacy/PR/pr_usbank_0609] 1999.html.

to the federal government; the Video Privacy Protection Act of 1988 (18 U.S.C. § 2710) regulates the use and disclosure of personal information collected in connection with video rentals; the Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721) regulates the use and disclosure of personal information from state motor vehicle records; the Health Insurance and Portability and Accountability Act of 1996 (P.L. 104-191, §§ 262, 264, 45 C.F.R.§§160-164) regulates the use and disclosure of individually identifiable health information; and the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. §§ 6801 *et seq.)* regulates the privacy of personally identifiable, nonpublic financial information. Other federal privacy laws address particular types of communications media: telecommunications privacy is addressed in the Communications Act of 1934 which limits the use and disclosure of customer proprietary network information by telecommunications service providers (47 U.S.C. § 222); cable privacy is addressed in the Cable Communications Policy Act of 1984, which limits the disclosure of cable television subscriber names, addresses, and utilization information (47 U.S.C. § 551); and telephone privacy is addressed in the Telephone Consumer Protection Act of 1991, which requires telephone solicitors to maintain do not call lists (47 U.S.C. § 227).

Although it is not a privacy statute, section 5 of the Federal Trade Commission Act (the "FTC Act"), 15 U.S.C. §§ 41 *et seq.*, has been successfully used to address a company's failure to comply with its stated information privacy practices. The FTC Act prohibits unfair and deceptive practices in and affecting commerce, and authorizes the Federal Trade Commission to seek injunctive and other equitable relief, including redress, for violations. The Commission has brought enforcement actions to address deceptive online information practices. In 1998, GeoCities, 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. The settlement prohibits GeoCities from misrepresenting the purposes for which it collects personal identifying information, requires GeoCities to post a privacy notice on its site, and to establish a system to obtain parental consent before collecting personal information from children.[8] The Commission also entered into a consent agreement with Liberty Financial Companies, Inc., operator of the Young Investor Web site, requiring Liberty Financial to post a privacy policy on its children's sites and obtain verifiable consent before collecting personal identifying information from children.[9] In January 2000, the FTC settled a complaint against Reverseauction.com, Inc., alleging that it 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.[10] The FTC also settled charges against Toysmart.com 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.[11] In July 200l several online pharmacies settled charges that they had violated their privacy

---

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

[9] *In re Liberty Financial*, Case No.9823522 (May 1999), [http://www.ftc.gov/os/1999/9905/lbtyord.htm].

[10] *FTC v. Reverseauctions.com, Inc.*, Civil Action No. 000032 (D.D.C. 2000), [http://www.ftc.gov/os/2000/01/reversecmp.htm].

[11] *FTC v. Toysmart.com, LLC, and Toysmart.com, Inc.* (Civil Action 00-11341-RGS) (D. Mass. 2000), [http://www.ftc.gov/opa/2000/07/toysmart2.htm].

policies.[12] A February 2000 complaint filed with the FTC charged DoubleClick, Inc. with violations of the Federal Trade Act.[13] In response to market pressures and pending lawsuits, DoubleClick discontinued its allegedly unfair and deceptive trade practices.

Legislation. Notwithstanding the existence of many federal privacy laws (and several state initiatives and laws), there is a perception held by consumers, privacy advocates, and some legislators and regulators that there is a need for a federal online privacy law to regulate the collection, use, and disclosure of online personal information. The crux of the online privacy debate is whether industry self-regulation of online personal information through implementation of privacy policies is effective or whether a uniform national law to regulate the privacy of online personal information should exist. The Federal Trade Commission has extensively studied this question, and issued a series of reports to Congress.[14] Initially the Commission preferred a self-regulatory approach to online privacy through adoption and adherence to privacy policies. In its 2000 Report to Congress, however, a majority of the Commission (3-2) concluded that notwithstanding measurable gains, self-regulation alone was unlikely to provide online consumers with an adequate level of protection, and recommended that Congress consider online privacy legislation to supplement self-regulatory methods. In 2001, the new FTC Chairman Timothy Muris announced a new pro- privacy agenda including greater FTC regulatory efforts to enforce both online and offline privacy promises. In April 2002, Chairman Muris wrote that enactment of broad, general legislation governing online privacy issues is premature at this time in light of the FTC's new pro-privacy agenda.[15]

Online privacy legislation based upon core fair information practice principles attempts to provide solutions to privacy problems posed by online personal information. Fair information practice principles were first articulated in the United States Department of Health, Education and Welfare's 1973 report entitled *Records, Computers and the Rights of Citizens*. Since then, a canon of fair information practice principles has been developed.[16] Fair information practice codes include five core principles: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress. The most fundamental principle is that consumers should be given notice of an entity's information practices before any personal information is collected. The second widely accepted core principle is consumer choice or consent, which means giving consumers options as to how any personal information collected from them may be used. Access is the third core principle, and refers to an individual's ability both to access data about herself, and to contest that data's accuracy. The fourth principle is that data be accurate and secure. The fifth principle is that an effective enforcement and

---

[12] *FTC v. Sandra L. Rennart, et al.,* Civ. Action No. CV-S-000861-JBR (D. Nev. July 6, 2000), [http://www.ftc.gov/os/2000/07/iogstipmort.htm].

[13] See EPIC DoubleClick Complaint, [http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf]

[14] See, U.S. Federal Trade Commission, *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, [http://www.ftc.gov/privacy/reports.htm].

[15] Letter From Chairman Muris to the Senate Committee on Commerce, Science, and Transportation (April 24, 2002), [http://www.ftc.gov/os/2002/04/sb2201muris.htm].

[16] See also *The European Union Directive on the Protection of Personal Data* (1995); and Canadian Standards Association, *Model Code for the Protection of Personal Information* (1996).

redress mechanism exist to enforce the privacy principles. The alternative approaches are industry self-regulation; legislation that would create private remedies for consumers; or regulatory schemes enforceable through civil and criminal sanctions.

In the 107th Congress there are several bills which regulate online personal information. Differences among the bills relate to: the requirements established for sensitive vs. nonsensitive personal information; the type of notice required; whether individuals have the opportunity to opt-in or to opt-out of disclosures; whether opt-out or opt-in depends upon whether the disclosure is for financial consideration; whether or not individuals are given a right to sue for violations; whether the bill applies to online businesses alone, offline businesses, or both; whether federal preemption applies, and if so, whether the bill preempts all state privacy laws or only state statutes but not state common laws; whether enforcement is through the FTC and state attorneys general, or through industry self-regulation and redress; whether compliance with other federal privacy laws provides a safe harbor; and the effect of foreign privacy laws on U.S. businesses. The bills vary on notice, consent, access, security, and enforcement.

For example, H.R. 4678 (Rep. Stearns) applies to both online and offline entities – except government agencies, small businesses, and nonprofit groups – that collect, sell, disclose for consideration, or use personal information. It requires consumer notice, privacy policy statements, opportunity for consumer opt-out for sale of personal information, a self-regulatory program with appeal to the FTC, no private right of action, harmonization with other federal privacy laws, preemption of state privacy laws, identity theft prevention measures and remedies, GAO study on the effect of foreign privacy laws and whether they result in discriminatory treatment of U.S. businesses; and harmonization of international privacy laws. S. 2201 (Sen. Hollings) requires notice of collection and use practices; requires online entities to obtain consent prior to collecting sensitive information (opt-in); requires entities to post privacy notices on Web sites; requires companies to give user's the option to request that nonsensitive information not be collected (opt-out); authorizes user access and correction, preempts state statutes on Internet privacy; permits individuals to sue for actual damages or $5,000; authorizes FTC and state attorneys general enforcement and enforcement to by other federal regulators for certain classes of information. The Senate Commerce Committee mark-up of S. 2201 began May 16th. The bill manager's amendment was approved by the Committee 14-9, and would, among other things, restrict the private right of action to improper disclosures of sensitive information only, and direct the FTC to develop a rule to apply the bill to offline businesses. For information on other online privacy bills, see CRS Report RL31408, Internet Privacy: Overview and Pending Legislation.

Some stakeholders believe that online privacy legislation is premature, and will have a chilling effect on the Internet economy; others view the legislation as unfair to industries regulated by other privacy laws.[17] Industry representatives worry that the private right of action may result in class action lawsuits. Privacy advocates generally favor online privacy legislation with the right to sue, application to online entities, and opt-in consent for information disclosures. Many believe that absent a legislative solution problems surfacing today will get worse in the future.

---

[17] See *Hearings on S. 2201 Before the Senate Comm. On Commerce, Science and Transportation* 107th Cong., (Apr. 25, 2002), [http://www.commerce.senate.gov/hearings/hearings0202.htm].