Order Code RS20035
Updated November 13, 2001

Internet Privacy: Overview and Pending Legislation

Marcia S. Smith
Specialist in Aerospace and Telecommunications Policy
Resources, Science, and Industry Division

Summary

Internet privacy issues encompass concerns about the collection of personally identifiable information from visitors to Web sites, as well as debate over law enforcement or employer monitoring of electronic mail and Web usage. In the wake of the September 11 terrorist attacks, debate over the issue of law enforcement monitoring has intensified, with some advocating increased tools for law enforcement to track down terrorists, and others cautioning that fundamental tenets of democracy, such as privacy, not be endangered in that pursuit. Language in the House-passed Department of Justice authorization bill (H.R. 2215) requires the Justice Department to report to Congress on its use of Internet monitoring software such as Carnivore/DCS 1000, but Congress also has passed, and the President signed into law, anti-terrorism legislation (H.R. 3162, P.L. 107-56) that would make it easier for law enforcement to monitor Internet activities. The parallel debate over Web site information policies concerns whether industry self regulation or legislation is the best approach to protecting consumer privacy. Several bills are pending. This report provides a brief overview of Internet privacy issues and tracks pending legislation. For more detailed discussion of the issues, see CRS Report RL30784. This report will be updated.

Internet: Collection of Data by Commercial Web Site Operators

One aspect of the Internet ("online") privacy debate focuses on whether industry self regulation or legislation is the best route to assure consumer privacy protection. In particular, consumers appear concerned about the extent to which Web site operators collect "personally identifiable information" (PII) and share that data with third parties without their knowledge. Repeated media stories about privacy violations by Web site operators have kept the issue in the forefront of public debate about the Internet. Although many in Congress and the Clinton Administration preferred industry self regulation, the 105th Congress passed legislation to protect the privacy of children under 13 (see below). More than 30 bills in the 106th Congress addressed Internet privacy in whole or in part, but the only legislation that passed were amendments to two appropriations bills dealing with information collected by certain federal Web sites (see

below). Many bills are pending in the 107th Congress (see table at end of this report) and several hearings have been held.

Children's Online Privacy Protection Act (COPPA), P.L. 105-277. Congress, the Clinton Administration, and the Federal Trade Commission (FTC) initially focused their attention on protecting the privacy of children under 13 as they visit Web sites. Not only are there concerns about information children might divulge about themselves, but also about their parents. The result was the Children's Online Privacy Protection Act (COPPA), Title XIII of Division C of the FY1999 Omnibus Consolidated and Emergency Supplemental Appropriations Act, P.L. 105-277. The FTC's final rule implementing the law became effective April 21, 2000 [http://www.ftc.gov/opa/1999/9910/childfinal.htm]. Commercial Web sites and online services directed to children under 13 or that knowingly collect information from them must inform parents of their information practices and obtain verifiable parental consent before collecting, using, or disclosing personal information from children. The law also provides for industry groups or others to develop self-regulatory "safe harbor" guidelines that, if approved by the FTC, can be used by Web sites to comply with the law. The FTC approved self-regulatory guidelines proposed by the Better Business Bureau on January 26, 2001. In April 2001, the FTC fined three companies for violating COPPA [http://www.ftc.gov/opa/2001/04/girlslife.htm].

FTC Activities and Fair Information Practices. The FTC has conducted or sponsored several Web site surveys since 1997 to determine the extent to which commercial Web site operators abide by four fair information practices—providing *notice* to users of their information practices before collecting personal information, allowing users *choice* as to whether and how personal information is used, allowing users *access* to data collected and the ability to contest its accuracy, and ensuring *security* of the information from unauthorized use. See CRS Report RL30784 for more information on these surveys. The FTC's reports are available on its Web site [http://www.ftc.gov.].

Briefly, the first two FTC surveys (December 1997 and June 1998) created concern about the information practices of Web sites directed at children and led to the enactment of COPPA (see above). The FTC continued monitoring Web sites to determine if legislation was needed for those not covered by COPPA. In 1999, the FTC concluded that more legislation was not needed at that time because of indications of progress by industry at self-regulation, including creation of "seal" programs (see below) and by two surveys conducted by Georgetown University. However, in May 2000, the FTC changed its mind following another survey that found only 20% of randomly visited Web sites and 42% of the 100 most popular Web sites had implemented all four fair information practices. The FTC voted to recommend that Congress pass legislation requiring Web sites to adhere to the four fair information practices, but the 3-2 vote indicated division within the Commission. On October 4, 2001, FTC's new chairman, Timothy Muris, revealed his position on the issue, saying that he did not see a need for additional legislation now.

Three bills (H.R. 89, H.R. 237, and H.R. 347) are pending specifically on this topic. In addition, the Senate-passed version of the bankruptcy reform bill (S. 420) would prohibit (with exceptions) companies, including Web site operators, that file for bankruptcy from selling or leasing PII obtained in accordance with a policy that said such information would not be transferred to third parties, if that policy was in effect at the time of the bankruptcy filing. Also, H.R. 2135 would limit the disclosure of personal

information (defined as PII and sensitive personal information) by information recipients in general, and S. 1055 would limit the commercial sale and marketing of PII.

Advocates of Self-Regulation. In 1998, members of the online industry formed the Online Privacy Alliance (OPA) to encourage industry self regulation. OPA developed a set of privacy guidelines and its members are required to adopt and implement posted privacy policies. The Better Business Bureau (BBB), TRUSTe, and WebTrust have established "seals" for Web sites. To display a seal from one of those organizations, a Web site operator must agree to abide by certain privacy principles (some of which are based on the OPA guidelines), a complaint resolution process, and to being monitored for compliance. Advocates of self regulation argue that these seal programs demonstrate industry's ability to police itself. The CATO Institute also argues that privacy-protecting technologies are quite effective [http://www.cato.org/pubs/briefs/bp-065es.html].

Advocates of Legislation. Consumer, privacy rights and other interest groups believe self regulation is insufficient. They argue that the seal programs do not carry the weight of law, and that while a site may disclose its privacy policy, that does not necessarily equate to having a policy that protects privacy. The Center for Democracy and Technology (CDT, at [http://www.cdt.org]) and the Electronic Privacy Information Center (EPIC, at [http://www.epic.org]) each have released reports on this topic. A particular concern is online profiling where companies collect data about what Web sites are visited by a particular user and develop profiles of that user's preferences and interests for targeted advertising. Following a one-day workshop on online profiling, FTC issued a two-part report in the summer of 2000 that also heralded the announcement by a group of companies that collect such data, the Network Advertising Initiative (NAI), of self-regulatory principles. At that time, the FTC nonetheless called on Congress to enact legislation to ensure consumer privacy vis a vis online profiling because of concern that "bad actors" and others might not follow the self-regulatory guidelines. Now, the FTC Chairman's position is that legislation is not needed now.

Internet: Federal Government Web Site Information Practices

Under a May 1998 directive from President Clinton and a June 1999 Office of Management and Budget (OMB) memorandum, federal agencies are supposed to ensure that their information practices adhere to the 1974 Privacy Act. In June 2000, however, the Clinton White House revealed that contractors for the Office of National Drug Control Policy (ONDCP) had been using "cookies" (small text files placed on users' computers when they access a particular Web site) to collect information about those using an ONDCP site during an anti-drug campaign. ONDCP was directed to cease using cookies, and OMB issued another memorandum reminding agencies to post and comply with privacy policies and detailing the limited circumstances under which agencies should collect personal information. A September 5, 2000 letter from OMB to the Department of Commerce further clarified that "persistent"cookies, which remain on a user's computer for varying lengths of time (from hours to years), are not allowed unless four specific conditions are met. "Session" cookies, which expire when the user exits the browser, are permitted.

At the time, Congress was considering whether commercial Web sites should be required to abide by four fair information practices proposed by the FTC. The incident sparked interest in whether federal Web sites should be subject to the same requirements.

Following a hearing and three General Accounting Office (GAO) reports (GAO/GGD-00-191, B-286150, GAO-01-147R), Congress passed amendments to two appropriations bills regarding Web site information practices. Section 501 of the FY2001 Transportation Appropriations Act (P.L. 106-346) prohibits funds in the FY2001 Treasury-Postal Appropriations Act from being used by any federal agency to collect, review, or create aggregate lists that include PII about an individual's access to or use of a federal Web site or enter into agreements with third parties to do so, with exceptions. Section 646 of the FY2001 Treasury-Postal Appropriations Act (P.L. 106-554) requires Inspectors General (IGs) to report to Congress on activities by those agencies or departments relating to collection of PII about individuals who access any Internet site of that department or agency, or entering into agreements with third parties to obtain PII about use of government or non-government Web sites.

Senator Thompson released two reports in April and June 2001 based on the findings of agency IGs who discovered unauthorized persistent cookies and other violations of government privacy guidelines on several agency Web sites. An April 2001 GAO report (GAO-01-424) on implementation of federal guidance for agency use of cookies concluded that most of the 65 sites it reviewed were following OMB's guidance. S. 851 (Thompson) would establish an 18-month commission to study the collection, use, and distribution of personal information by federal, state, and local governments. H.R. 583 (Hutchinson) would create a commission to study privacy issues more broadly. Section 218 of S. 803 (Lieberman) would set requirements on government agencies in how they assure the privacy of PII in government information systems, and establish privacy guidelines for federal Web sites. The final version of the FY2002 Treasury-Postal Appropriations Act (H.R. 2590, H. Rept. 107-253) prohibits, with exceptions, federal funds from being used by a federal agency to collect, review, or create any aggregate list, derived from any means, that includes the collection of any PII related to an individual's access to or use of a federal Web site, or to enter into any agreement with a third party to collect, review, or obtain such information on use of any nongovernmental Web site.

Spyware

Some software products include, as part of the software itself, a method by which information is collected about the use of the computer on which the software is installed. When the computer is connected to the Internet, the software periodically relays the information back to the software manufacturer or a marketing company. The software that collects and reports is called "spyware." Software programs that include spyware can be obtained on a disk or downloaded from the Internet. They may be sold or provided for free. Typically, users have no knowledge that the software product they are using includes spyware. Some argue that users should be notified if the software they are using includes spyware. Two pending bills (H.R. 112 and S. 197) would require notification.

Monitoring E-mail and Web Usage

Another concern has been the extent to which electronic mail (e-mail) exchanges or visits to Web sites may be monitored by law enforcement agencies or employers. In the wake of the September 11 terrorist attacks, the debate over law enforcement monitoring has intensified. Previously, the issue had focused on the extent to which the Federal Bureau of Investigation (FBI), with legal authorization, uses a software program called

Carnivore (now renamed DCS 1000) to intercept e-mail and monitor Web activities of certain suspects. The FBI installs the software on Internet Service Providers' equipment to intercept e-mail and monitor other Internet activity. Privacy advocates are concerned whether Carnivore-like systems can differentiate between e-mail and Internet usage by a subject of an investigation and those of other people. To help oversee the extent to which the FBI uses Carnivore/DCS 1000, the FY2002 Department of Justice authorization bill (H.R. 2215/S. 1319) as passed by the House and reported from the Senate Judiciary Committee requires the Justice Department to report to Congress on its use of DCS 1000 or any similar system. Following the terrorist attacks, however, the Congress passed anti-terrorism legislation, the USA PATRIOT Act (P.L. 107-56), that expands law enforcement's ability to monitor Internet activities. See the Internet Privacy entry in the CRS Electronic Briefing Book for more information on the new law.

There also is concern about the extent to which employers monitor the e-mail and other computer activities of employees. A 2001 survey by the American Management Association [http://www.amanet.org/press/amanews/ems2001.htm] found that 62.8% of the companies surveyed monitor Internet connections, 46.5% store and review e-mail, and 36.1% store and review computer files. The public policy concern appears to be not whether companies should be able to monitor activity, but whether they should notify their employees of that monitoring. A hearing was held on this issue in the 106th Congress and two bills were introduced, but there was no action.

Identity Theft and Protecting Social Security Numbers

The widespread use of computers for storing and transmitting information is thought to be contributing to the sharply rising rates of identity theft, where one individual assumes the identity of another using personal information such as credit card and Social Security numbers (SSNs). The FTC has a toll free number (877-ID-THEFT) to help victims of identity theft. Whether the Internet is responsible for the increase in identity theft cases is debatable, however. Some attribute the rise instead to carelessness by businesses in handling personally identifiable information, and by credit issuers that grant credit without proper checks. The FTC found that less than 1% of identity theft cases are linked to the Internet *(Computerworld,* February 12, 2001, p. 7).

The 105th Congress passed the Identity Theft and Assumption Deterrence Act (P.L. 105-318), and the 106th Congress passed the Social Security Number Confidentiality Act (P.L. 106-433) and the Internet False Identification Act (P.L. 106-578). Several bills have been introduced in the 107th Congress relating to identity theft or protection of Social Security numbers (H.R. 91, H.R. 220, H.R. 1478, H.R. 2036/S.1014, S. 848, and H.R. 3053/S. 1399). In 2001, hearings have been held by a House Ways and Means subcommittee (May 22), a joint hearing between House Ways and Means and House Financial Services subcommittees (November 8), and a Senate Judiciary subcommittee (September 13).

Pending Legislation Concerning Internet Privacy and Related Issues

H.R. 89 (Frelinghuysen)	**Online Privacy Protection Act.** Requires FTC to prescribe regulations to protect privacy of personal information collected from and about individuals not covered by COPPA. (Energy & Commerce)
H.R. 91 (Frelinghuysen)	**Social Security Online Privacy Protection Act**. Regulates use by interactive computer services of SSNs and related personally identifiable information. (Energy & Commerce)
H.R. 112 (Holt)	**Electronic Privacy Protection Act**. Makes it unlawful for any person to knowingly make, import, export, distribute, sell, offer for sale, install or use "spyware." (Energy & Commerce)
H.R. 220 (Paul)	**Identity Theft Prevention Act**. Protects integrity and confidentiality of SSNs, prohibits establishment of a uniform national identifying number by federal governments, and prohibits federal agencies from imposing standards for identification of individuals on other agencies or persons. (Ways & Means, Government Reform)
H.R. 237 (Eshoo)	**Consumer Internet Privacy Enhancement Act**. Requires Web site operators to provide clear and conspicuous notice of their information practices and provide consumers with easy method to limit use and disclosure of their information. Preempts state and local laws if they are inconsistent with or more restrictive than this one. Directs FTC to enforce the law. State Attorneys General can bring suits in federal courts. Sets penalties. (Energy & Commerce).
H.R. 333 (Gekas)/ **S. 420** (Grassley)	**Bankruptcy Reform Act.** S. 420 passed the Senate March 15, 2001. Sections 231 and 232 limit when companies can sell or lease publicly identifiable information collected in accordance with a policy in effect at the time of the bankruptcy filing that prohibits transfer of such information to third parties. H.R. 333 as passed by the House March 1 does not have this provision. Senate passed H.R. 333 with amendment in the nature of a substitute July 17. House and Senate conferees appointed.
H.R. 347 (Green)	**Consumer Online Privacy and Disclosure Act**. Requires FTC to promulgate regulations requiring Web site or online service operators to provide clear, conspicuous, understandable notice about what information is collected and contact information for the operator; provides meaningful and simple online process for individuals to opt-out of disclosure of information for purposes unrelated to why it was obtained; and gives description of information that is provided to third parties. (Energy & Commerce)
H.R. 583 (Hutchinson)	**Privacy Commission Act**. Creates a Commission for the Comprehensive Study of Privacy Protection. (Government Reform)
H.R. 1478 (Kleczka)	**Personal Information Privacy Act**. Prohibits use of SSNs for commercial purposes without consent; prohibits sale or transfer of transaction or experience information without consent; and repeals certain provisions relating to distribution of consumer reports re certain transmissions not initiated by the consumer. (Ways & Means, Financial Services)
H.R. 2036 (Shaw)/ **S. 1014** (Bunning)	**Social Security Number Privacy and Identity Theft Protection Act.** Restricts sale and display of SSNs by government agencies, with exceptions; and restrict sale, purchase, and display of SSNs in the private sector, with exceptions. (House Ways & Means, Energy & Commerce, Financial Services; Senate Finance)
H.R. 2135 (Sawyer)	**Consumer Privacy Protection Act**. Limits disclosure of personally identifiable information and sensitive personal information by information recipients. (Energy & Commerce)
H.R. 2215 (Sensenbrenner)/ **S. 1319** (Leahy)	**Department of Justice Authorization Act**. Establishes congressional reporting requirements re use of DCS 1000/Carnivore. H.R. 2215 passed House July 23. S. 1319 reported from Judiciary Committee October 30 (written report filed November 8, S. Rept. 107-96).
H.R. 2590 (Istook)	**FY2002 Treasury-Postal Appropriations Act.** Sets prohibitions, with exceptions, on federal agencies re collecting, reviewing, or creating any aggregate list that includes collection of PII relating to an individual's use of federal or nongovernmental Web sites. Presented to President November 2.
H.R. 3053 (Hooley)/ **S. 1399** (Feinstein)	**Identity Theft Protection Act**. Establishes certain requirements for credit card issuers and consumer reporting agencies. (House Financial Services; Senate Banking)
S. 197 (Edwards)	**Spyware Control and Privacy Protection Act**. Requires that software made available to the public include clear and conspicuous notice if it includes spyware. Spyware may not be enabled unless the user provides affirmative consent, with exceptions. Sets restrictions on how information collected by spyware can be used and allows the user reasonable access to the information. (Commerce)
S. 803 (Lieberman)	**E-Government Act**. Sect. 218 would set requirements on government agencies in how they assure the privacy of personally identifiable information in government information systems and establish guidelines for privacy policies for federal Web sites. (Governmental Affairs)
S. 848 (Feinstein)	**Social Security Number Misuse Prevention Act**. Limits display, sale, or purchase of SSNs. (Judiciary)
S. 851 (Thompson)	**Citizen's Privacy Commission Act.** Would study the collection, use, and distribution of personal information by federal, state, and local governments. (Governmental Affairs)
S. 1055 (Feinstein)	**Privacy Act of 2001.** Restricts commercial sale and marketing of personally identifiable information, limits the use of SSNs, limits sale and sharing of nonpublic personal financial information, limits provision of protected health information. (Judiciary)