Updated March 20, 2001

RS20035

CRS Report for Congress

Internet Privacy—Protecting Personal Information: Overview and Pending Legislation

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

Summary

The privacy of information collected by operators of World Wide Web sites is a growing issue of concern. Many in Congress and the Clinton Administration prefer to rely on industry self regulation to protect consumer privacy, but frustration at industry's slow pace led to the 1998 passage of the Children's Online Privacy Protection Act in 1998 (P.L. 105-277). The 106th Congress devoted considerable attention to the issue of Internet privacy, but the only legislation that passed were amendments to two appropriations bills concerning the collection of data by certain federal agencies about visitors to their Web sites. The 107th Congress remains strongly interested in Internet privacy. This report provides a brief overview of Internet privacy issues and tracks pending legislation. More detailed discussion of the issues is provided in CRS Report RL30784. Financial records privacy and medical records confidentiality are not Internet privacy issues and are not discussed here. Those topics are addressed in CRS Report RS20185 and CRS Report RS20500, respectively. This report will be updated.

Introduction

Public concern about what information is being collected by Web site operators or third parties when consumers visit Web sites has stimulated debate in Congress about how to balance consumers' desire for privacy with needs of companies and the government to collect certain information on visitors to their Web sites. In addition, concerns have arisen about the extent to which electronic mail (e-mail) and Web activity are monitored by law enforcement agencies or employers.

Internet Privacy: Collection of Data by Web Site Operators

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 prefer industry self regulation, the 105th Congress passed legislation to protect the privacy of children under 13 (the Children's Online Privacy Protection Act). 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. New legislation has introduced in the 107th Congress. A House Energy and Commerce subcommittee held a hearing on broad privacy issues in the commercial sector on March 1, 2001.

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]. Under the rule, 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.

Clinton Administration Position on Online Privacy. In 1997, the Clinton Administration endorsed industry self regulation for protecting consumer Internet privacy, but stressed that if industry did not self regulate effectively the government might have to step in, particularly regarding children. Over the next several years, Vice President Gore and Clinton Administration officials reiterated their support for self regulation.

In the summer of 2000, controversy arose about federal agency information practices regarding visitors to their Web sites. Under a May 1998 presidential directive 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 and protect an individual's right to privacy. In June 2000, however, the White House announced that it had just learned 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. The White House directed ONDCP to cease using cookies. 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.

At the time, Congress was considering the FTC's recommendation to require commercial Web sites to adhere to the four fair information practices (see below). The

ONDCP incident sparked interest in whether federal Web sites should be subject to the same requirements. Following a hearing and three General Accounting Office reports in September and October 2000 (GAO/GGD-00-191, B-286150, GAO-01-147R), Congress passed amendments to two appropriations bills regarding Web site information practices in departments and agencies under the Treasury-General Government Appropriations Act. Section 501 of the FY2001 Transportation Appropriations Act (P.L. 106-346) prohibits funds in the FY2001 Treasury-General Government Appropriations Act from being used by any federal agency to collect, review, or create aggregate lists that include personally identifiable information (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-General Government Appropriations Act, as included in the FY2001 Consolidated Appropriations Act (P.L. 106-554), requires Inspectors General of agencies or departments in that Act to report to Congress within 60 days of enactment 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.

Federal Trade Commission (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. More information on these surveys is provided in CRS Report RL30784. FTC reports on the surveys are available on its Web site [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, in particular. The survey results led the FTC to call on Congress to pass legislation protecting children's privacy as they visit Web sites by requiring parental permission before a Web site could request information about a child. COPPA was enacted four months later.

The FTC continued monitoring Web sites to determine if additional legislation was needed to 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 recommended that Congress pass legislation requiring Web sites to adhere to the four fair information practices. The FTC vote to recommend new legislation was 3-2, indicating division within the Commission, however. Hearings were held on the FTC recommendation, and several bills in the 106th Congress would have required Web site operators to adhere to some or all of those practices. None passed, however. Three bills (H.R. 89, H.R. 237, and H.R. 347) have been introduced in the 107th Congress relating to that specific topic. Also, a provision in the Senate-passed version of the bankruptcy reform bill (S. 420) would prohibit companies, including Web site operators, that file for bankruptcy from selling or leasing personally identifiable information 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. Exceptions are made if the sale is consistent with the policy, or if a court, after notice and hearing and due consideration of the facts, circumstances, and conditions of the sale or lease, approves it. The bill would require the court to appoint an ombudsman to assist the court in that determination.

Industry Activities and "Seals". 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. Advocates of legislation argue that while the seal programs are useful, they do not carry the weight of law, limiting remedies for consumers whose privacy is violated. They also point out that while a site may disclose its privacy policy, that does not necessarily equate to having a policy that protects privacy.

Concerns of Public Interest and Other Groups. Consumer, privacy rights and other interest groups continue to express concern that self regulation is insufficient. CDT and EPIC both have released reports questioning whether privacy policies actually ensure privacy. 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. 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.

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 it has collected back to the software manufacturer or a marketing company. The software that performs the collection and reporting function 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 bills (H.R. 112 and S. 197) have been introduced to require such notification.

E-mail and Web Usage Privacy

Another growing concern is the extent to which electronic mail (e-mail) exchanges or visits to Web sites may be monitored by law enforcement agencies or employers. One catalyst for this concern was the revelation in the summer of 2000 that the Federal Bureau of Investigation (FBI), with proper legal authorization, has been using a software program called Carnivore 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. (See CRS Report RL30677 for more on Carnivore. In February 2001, the FBI renamed Carnivore. It is now designated "DCS1000."). The extent to which Carnivore can differentiate between e-mail and Internet usage involving a subject of an investigation and those of other people is of considerable debate. Critics claim that Carnivore violates the privacy of innocent Internet users. Congressional hearings and legislation in the 106th Congress addressed these issues, but no new law was passed. This issue is expected to be debated by the 107th Congress.

At about the same time, concern arose about the extent to which employers monitor the e-mail and other computer activities of employees. A January 2000 survey by the American Management Association reported in the July 10, 2000 edition of *Business Week* (electronic version) found that 54.1% of the companies surveyed monitor Internet connections, 38.1% monitor e-mail, and 30.8% monitor computer files. To the extent that Congress has looked at this matter, the focus appears to be not whether companies should be able to monitor such activity, but whether they should provide notice to their employees of that monitoring. One hearing was held on this topic in the 106th Congress and two bills were introduced, but there was no action on the bills.

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. The Federal Trade Commission (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. According to *Computerworld* (February 12, 2001, p. 7), the FTC has found that less than 1% of identity theft cases are linked to the Internet.

The 105th Congress passed the Identity Theft and Assumption Deterrence Act (P.L. 105-318), which sets penalties for persons who knowingly, and with the intent to commit unlawful activities, possess, transfer, or use one or more means of identification not legally issued for use to that person. The 106th Congress passed the Social Security Number Confidentiality Act (P.L. 106-433), which prohibits display of SSNs on unopened checks or other Treasury-issued drafts. Separately, the 106th Congress passed S. 2924 (P.L. 106-578), which updates existing law against selling or distributing false IDs to include those sold or distributed through computer files, templates, and disks.

Two bills have been introduced in the 107th Congress relating to identity theft (H.R. 91 and H.R. 220).

107th Congress Legislation Concerning Internet Privacy and Related Issues

H.R. 89 (Frelinghuysen)	**Online Privacy Protection Act.** To require 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.** To regulate use by interactive computer services of SSNs and related personally identifiable information. (Energy & Commerce)
H.R. 112 (Holt)	**Electronic Privacy Protection Act.** To make 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.** To protect integrity and confidentiality of SSNs, prohibit establishment of a uniform national identifying number by federal governments, and prohibit 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.** (Energy & Commerce). To require 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.
H.R. 347 (Green)	**Consumer Online Privacy and Disclosure Act.** (Energy & Commerce) To require 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; provide meaningful and simple online process for individuals to opt-out of disclosure of information for purposes unrelated to why it was obtained; and give description of information that is provided to third parties. A state may bring action on behalf of resident of that state, but FTC may intervene.
H.R. 583 (Hutchinson)	**Privacy Commission Act.** To create a Commission for the Comprehensive Study of Privacy Protection. (Government Reform)
S. 197 (Edwards)	**Spyware Control and Privacy Protection Act.** (Commerce) To require 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.
S. 420 (Grassley)	**Bankruptcy Reform Act.** 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. (The House version of the bill, H.R. 333, does not have this provision.)