Order Code RL31408

CRS Report for Congress

Internet Privacy: Overview and Pending Legislation

Updated April 1, 2004

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



Prepared for Members and Committees of Congress



Internet Privacy: Overview and Pending Legislation

Summary

Internet privacy issues encompass concerns about the collection of personally identifiable information (PII) from visitors to government and commercial 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, 2001 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. The 21st Century Department of Justice Appropriations Authorization Act (P.L. 107-273) required the Justice Department to report to Congress on its use of Internet monitoring software. On the other hand, Congress also passed the USA PATRIOT Act (P.L. 107-56) that, *inter alia*, makes it easier for law enforcement to monitor Internet activities. The Homeland Security Act (P.L. 107-296) expanded upon that Act, loosening restrictions on Internet Service Providers as to when, and to whom, they can voluntarily release information about subscribers if they believe there is a danger of death or injury.

The parallel debate over Web site information policies concerns whether industry self regulation or legislation is the best approach to protecting consumer privacy. Congress has considered legislation that would require *commercial* Web site operators to follow certain fair information practices, but none has passed. Legislation has passed, however, regarding information practices for *federal government* Web sites. For example, the E-Government Act (P.L. 107-347) sets requirements on how government agencies assure the privacy of personally identifiable information in government information systems and establishes guidelines for privacy policies for federal Web sites.

This report provides a brief overview of Internet privacy issues (including "spyware"), tracks Internet privacy legislation pending before the 108th Congress, and describes the four laws that were enacted in the 107th Congress (listed above). For more detailed discussion of the issues, see CRS Report RL30784, *Internet Privacy: An Analysis of Technology and Policy Issues* (December 21, 2000), and CRS Report RL31289, *The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government.* For information on wireless privacy issues, see CRS Report RL31636, *Wireless Privacy: Availability of Location Information for Telemarketing.*

Identity theft is not an Internet privacy issue per se, but is often debated in the context of whether the Internet makes identity theft more prevalent. Thus, identity theft is briefly discussed in this report. For more information on that topic, see CRS Report RL31919, *Remedies Available to Victims of Identity Theft*, and CRS Report RL32121, *Fair Credit Reporting Act: A Side-by-Side Comparison of House, Senate and Conference Versions.*

This report will be updated.

Contents

Introduction 1

Internet: Commercial Web Site Practices 1
Children's Online Privacy Protection Act (COPPA), P.L. 105-277 1
FTC Activities and Fair Information Practices 2
Advocates of Self Regulation 2
Advocates of Legislation 3
107th Congress Action 4
Legislation in the 108th Congress 4

Internet: Federal Government Web Site Information Practices 6

Monitoring of E-mail and Web Usage 7
By Government and Law Enforcement Officials 7
By Employers 9

Spyware 10

Identity Theft 12

Pending Legislation in the 108th Congress 14

Appendix: Internet Privacy-Related Legislation Passed by the 107th Congress 18

List of Tables

Table 1: Major Provisions of H.R. 1636 (Stearns) 5
Table 2: Pending Internet Privacy-Related Legislation 14

Internet Privacy: Overview and Pending Legislation

Introduction

Internet privacy issues encompass concerns about the collection of personally identifiable information (PII) from visitors to government and commercial Web sites, as well as debate over law enforcement or employer monitoring of electronic mail and Web usage. This report provides a brief discussion of Internet privacy issues and tracks pending legislation. More information on Internet privacy issues is available in CRS Report RL30784, *Internet Privacy: An Analysis of Technology and Policy Issues*, and CRS Report RL31289, *The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government.*

Internet: Commercial Web Site Practices

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 (COPPA, see below) to protect the privacy of children under 13 as they use commercial Web sites. Many bills have been introduced since that time regarding protection of those not covered by COPPA, but the only legislation that has passed concerns federal government, not commercial, Web sites.

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 commercial 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/os/1999/10/64fr59888.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. FTC Chairman Muris stated in testimony to the Senate Commerce Committee on June 11, 2003 that the FTC has brought eight COPPA cases, and obtained agreements requiring payment of civil penalties totaling more than $350,000.[1]

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. Some include **enforcement** as a fifth fair information practice. Regarding choice, the term "**opt-in**" refers to a requirement that a consumer give affirmative consent to an information practice, while "**opt-out**" means that permission is assumed unless the consumer indicates otherwise. See CRS Report RL30784 for more information on the FTC surveys and fair information practices. 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.

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

---

[1] Prepared statement, p. 10, available at [http://commerce.senate.gov/hearings/index.cfm].

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.

Technological solutions also are being offered. P3P (Platform for Privacy Preferences) is one often-mentioned technology. It gives individuals the option to allow their web browser to match the privacy policies of websites they access with the user's selected privacy preferences. Its goal is to put privacy in the hands of the consumer. P3P is one of industry's attempts to protect privacy for online users. Josh Freed from the Internet Education Foundation says there is strong private sector backing for P3P as a first step in creating a common dialogue on privacy, and support from Congress, the Administration, and the FTC as well (see the IEF web site [http://www.p3ptoolbox.org/tools/papers/IEFP3POutreachforDMA.ppt]). The CATO Institute, argues that privacy-protecting technologies are quite effective [http://www.cato.org/pubs/briefs/bp-065es.html]. However, complaints are arising from some industry participants as P3P is implemented. One concern is that P3P requires companies to produce shortened versions of their privacy policies to enable them to be machine-readable. To some, this raises issues of whether the shortened policies are legally binding, since they may omit nuances, and "sacrifice accuracy for brevity."[2]

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. TRUSTe and BBBOnline have been criticized for becoming corporate apologists rather than defenders of privacy. In the case of TRUSTe, for example, Esther Dyson, who is credited with playing a central role in the establishment of the seal program, reportedly is disappointed with it. Wired.com reported in April 2002 that "Dyson agreed that...Truste's image has slipped from consumer advocate to corporate apologist. 'The board ended up being a little too corporate, and didn't have any moral courage,' she said." Truste subsequently announced plans to strengthen its seal program by more stringent licensing requirements and increased monitoring of compliance.

Some privacy interest groups, such as EPIC, also feel that P3P is insufficient, arguing that it is too complex and confusing and fails to address many privacy issues. An EPIC report from June 2000 further explains its findings [http://www.epic.org/reports/prettypoorprivacy.html].

Privacy advocates are particularly concerned about online profiling, where companies collect data about what Web sites are visited by a particular user and

---

[2] Clark, Drew. Tech, Banking Firms Criticize Limitations of Privacy Standard. NationalJournal.com, November 11, 2002.

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. As noted, the current FTC Chairman's position is that broad legislation is not needed at this time.

107th Congress Action

Many Internet privacy bills were considered by, but did not clear, the 107th Congress. H.R. 89, H.R. 237, H.R. 347, and S. 2201 dealt specifically with commercial Web site practices. H.R. 4678 was a broader consumer privacy protection bill. The Bankruptcy Reform bill (H.R. 333/S. 420) would have prohibited (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. H.R. 2135 would have limited the disclosure of personal information (defined as PII and sensitive personal information) by information recipients in general, and S. 1055 would have limited the commercial sale and marketing of PII. In a related measure, S. 2839 sought to protect the privacy of children using elementary or secondary school or library computers that use "Internet content management services," such as filtering software to restrict access to certain Web sites.

During the second session of the 107th Congress, attention focused on S. 2201 (Hollings) and H.R. 4678 (Stearns). (H.R. 4678 has been reintroduced in the 108th Congress, see below.) A fundamental difference was that H.R. 4678 affected privacy for both "online" and "offline" data collection entities, while S. 2201's focus was online privacy. During markup by the Senate Commerce Committee, a section was added to S. 2201 directing the FTC to issue recommendations and propose regulations regarding entities other than those that are online. Other amendments also were adopted. The bill was reported on August 1, 2002 (S.Rept. 107-240). A House Energy and Commerce subcommittee held a hearing on H.R. 4678 on September 24, 2002. There was no further action on either bill.

Legislation in the 108th Congress

Representative Frelinghuysen introduced H.R. 69 on the opening day of the 108th Congress. The bill would require the FTC to prescribe regulations to protect the privacy of personal information collected from and about individuals not covered by COPPA

On April 3, 2003, Representative Stearns introduced H.R. 1636, which is similar to H.R. 4678 from the 107th Congress. It addresses privacy for both online and offline entities. Its major provisions are shown in Table 1.

Table 1: Major Provisions of H.R. 1636 (Stearns)

(Explanation of Acronyms at End)

Provision	H.R. 1636 (Stearns) As Introduced
Title	Consumer Privacy Protection Act
Entities Covered	Data Collection Organizations, defined as entities that collect (by any means, through any medium), sell, disclose for consideration, or use, PII. Excludes governmental agencies, not-for-profit entities if PII not used for commercial purposes, certain small businesses, certain providers of professional services, and data processing outsourcing entities.
Differentiation Between Sensitive and Non-Sensitive PII	No
Adherence to Fair Information Practices Notice Choice Access Security	 Yes, with exceptions Yes (Opt-Out) No Yes
Enforcement	By FTC
Private Right of Action	No
Relationship to State Laws	Preempts state statutory laws, common laws, rules, or regulations, that affect collection, use, sale, disclosure, retention, or dissemination of PII in commerce.
Relationship to Other Federal Laws	Does not modify, limit, or supersede specified federal privacy laws, and compliance with relevant sections of those laws is deemed compliance with this Act.
Permitted Disclosures	Consumer's choice to preclude sale, or disclosure for consideration, by an entity applies only to sale or disclosure to another data collection organization that is not an information-sharing affiliate (as defined in the Act) of the entity.
Establishes Self-Regulatory "Safe Harbor"	Yes
Requires Notice to Users If Entity's Privacy Policy Changes	Yes
Requires Notice to Users if Privacy is Breached	No
Identity Theft Prevention and Remedies	Yes

Provision	H.R. 1636 (Stearns) As Introduced
Requires GAO study of impact on U.S. interstate and foreign commerce of foreign information privacy laws, and remediation by Secretary of Commerce if GAO finds discriminatory treatment of U.S. entities	Yes
Requires Secretary of Commerce to notify other nations of provisions of the Act, seek recognition of its provisions, and seek harmonization with foreign information privacy laws, regulations, or agreements.	Yes

FTC = Federal Trade Commission
GAO = General Accounting Office
PII = Personally Identifiable Information

Senator Feinstein introduced S. 745 on March 31, 2003. Title 1 of that bill requires commercial entities to provide notice and choice (opt-out) to individuals regarding the collection and disclosure or sale of their PII, with exceptions. She also introduced S. 1350 on June 26, 2003, which would require federal agencies and persons engaged in interstate commerce, who possess electronic data containing personal information, to disclose any unauthorized acquisition of that data. These bills are summarized in Table 2 below.

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 must 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 FTC's four fair information practices. The incident sparked interest in whether federal Web sites should adhere to the same requirements. In the

FY2001 Transportation Appropriations Act (P.L. 106-346), Congress prohibited funds in the FY2001 Treasury-Postal Appropriations Act from being used 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. Similar language is in the FY2002 Treasury-Postal Appropriations Act (P.L. 107-67). The FY2003 Treasury-Postal appropriations bills (sec. 634 in both H.R. 5120 and S. 2740) also contained similar language, though the bill did not clear the 107th Congress.

Section 646 of the FY2001 Treasury-Postal Appropriations Act (P.L. 106-554) required Inspectors General (IGs) to report to Congress on activities by those agencies or departments relating to their own collection of PII, or entering into agreements with third parties to obtain PII about use of Web sites. Then-Senator Fred 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) concluded that most of the 65 sites it reviewed were following OMB's guidance.

The107th Congress passed the E-Government Act (P.L. 107-347), which sets requirements on government agencies regarding how they assure the privacy of personal information in government information systems and establish guidelines for privacy policies for federal Web sites. The law requires federal Web sites to include a privacy notice that addresses what information is to be collected, why, its intended use, what notice or opportunities for consent are available to individuals regarding what is collected and how it is shared, how the information will be secured, and the rights of individuals under the 1974 Privacy Act and other relevant laws. It also requires federal agencies to translate their Web site privacy policies into a standardized machine-readable format, enabling P3P to work (see above discussion of P3P), for example. According to a February 2004 Federal Computer Week article, agency implementation of that provision is proceeding slowly.[3]

Monitoring of E-mail and Web Usage

By Government and Law Enforcement Officials

Another 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. 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 (later renamed DCS 1000), to intercept e-mail and monitor Web activities of certain suspects. The FBI installs the software on the equipment of Internet Service Providers (ISPs). Privacy advocates are concerned whether Carnivore-like systems can differentiate between e-mail and Internet usage by a

---

[3] Michael, Sara. Privacy Safeguard Proves Elusive. Federal Computer Week, February 23, 2004 (via Factiva).

subject of an investigation and similar usage by other people. Section 305 of the 21st Century Department of Justice Appropriations Authorization Act (P.L. 107-273) required the Justice Department to report to Congress on its use of Carnivore/DCS 1000 or any similar system.

On the other hand, following the terrorist attacks, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism (USA PATRIOT) Act (P.L. 107-56), which expands law enforcement's ability to monitor Internet activities. *Inter alia*, the law modifies the definitions of "pen registers" and "trap and trace devices" to include devices that monitor addressing and routing information for Internet communications. Carnivore-like programs may now fit within the new definitions. The Internet privacy-related provisions of the USA PATRIOT Act, included as part of Title II, are as follows:

- Section 210, which expands the scope of subpoenas for records of electronic communications to include records commonly associated with Internet usage, such as session times and duration.

- Section 212, which allows ISPs to divulge records or other information (but not the contents of communications) pertaining to a subscriber if they believe there is immediate danger of death or serious physical injury or as otherwise authorized, and requires them to divulge such records or information (excluding contents of communications) to a governmental entity under certain conditions. It also allows an ISP to divulge the contents of communications to a law enforcement agency if it reasonably believes that an emergency involving immediate danger of death or serious physical injury requires disclosure of the information without delay. [This section was amended by the Homeland Security Act, see below.]

- Section 216, which adds routing and addressing information (used in Internet communications) to dialing information, expanding what information a government agency may capture using pen registers and trap and trace devices as authorized by a court order, while excluding the content of any wire or electronic communications. The section also requires law enforcement officials to keep certain records when they use their own pen registers or trap and trace devices and to provide those records to the court that issued the order within 30 days of expiration of the order. To the extent that Carnivore-like systems fall with the new definition of pen registers or trap and trace devices provided in the Act, that language would increase judicial oversight of the use of such systems.

- Section 217, which allows a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from a protected computer under certain circumstances, and

- Section 224, which sets a 4-year sunset period for many of the Title II provisions. Among the sections excluded from the sunset are Sections 210 and 216.

The Cyber Security Enhancement Act, section 225 of the Homeland Security Act (P.L. 107-296), amends section 212 of the USA PATRIOT Act.[4] It lowers the threshold for when ISPs may voluntarily divulge the content of communications. Now ISPs need only a "good faith" (instead of a "reasonable") belief that there is an emergency involving danger (instead of "immediate" danger) of death or serious physical injury. The contents can be disclosed to "a Federal, state, or local governmental entity" (instead of a "law enforcement agency").

Privacy advocates are especially concerned about the new language added by the Cyber Security Enhancement Act. EPIC notes, for example, that allowing the contents of Internet communications to be disclosed voluntarily to any governmental entity not only poses increased risk to personal privacy, but also is a poor security strategy. Another concern is that the law does not provide for judicial oversight of the use of these procedures.[5]

S. 1695 (Leahy) would amend the PATRIOT Act to provide more oversight. *Inter alia,* it would amend the sunset provision (Sec. 224) such that all of the above cited sections would terminate on December 31, 2005, including Sections 210 and 216, which currently are not subject to the sunset clause. S. 1709 (Craig) would amend the USA PATRIOT Act, *inter alia* to include Section 216 in the sunset provision.

By Employers

There also is concern about the extent to which employers monitor the e-mail and other computer activities of employees. 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 2003 survey by the American Management Association [http://www.amanet.org/research/index.htm] found that 52% of the companies surveyed engage in some form of e-mail monitoring. A September 2002 General Accounting Office report (GAO-02-717) found that, of the 14 Fortune 1,000 companies it surveyed, all had computer-use policies, and all stored employee's electronic transactions, e-mail, information on Web sites visited, and computer file activity. Eight of the companies said they would read and review those transactions if they received other information than an individual might have violated company policies, and six said they routinely analyze employee's transactions to find possible inappropriate uses.

---

[4] The language originated as H.R. 3482, which passed the House on June 15, 2002.

[5] [http://www.epic.org/security/infowar/csea.html]

Spyware

The term "spyware" is not well defined. Jerry Berman, President of the Center for Democracy and Technology (CDT), explained in testimony to the Senate Commerce Committee in March 2004 that "The term has been applied to software ranging from 'keystroke loggers' that capture every key typed on a particular computer; to advertising applications that track users' web browsing; to programs that hijack users' system settings."[6] He noted that what these various types of software programs "have in common is a lack of transparency and an absence of respect for users' ability to control their own computers and Internet connections." The FTC plans to hold a workshop on spyware on April 19, 2004.

One example of spyware is software products that 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. Some products may collect personally identifiable information (PII). When the computer is connected to the Internet, the software periodically relays the information back to the software manufacturer or a marketing company. Some spyware traces a user's Web activity and causes advertisements to suddenly appear on the user's monitor — called "pop-up" ads — in response. Software programs that include spyware can be sold or provided for free, on a disk (or other media) or downloaded from the Internet. Typically, users have no knowledge that spyware is on their computers.

Two spyware bills are pending before the 108th Congress. H.R. 2929 (Bono) requires the FTC to establish regulations prohibiting the transmission of spyware programs via the Internet to computers without the user's consent, and notification to the user that the program will be used to collect PII. S. 2145 (Burns-Wyden) requires notice and consent to a user before anyone installs software on a user's computer (not including pre-installed software, and certain other exceptions). It also requires the user's affirmative consent to each information collection feature, advertising feature, distributed computing feature, and setting modification feature in the software. The software also must be able to be easily uninstalled.

The Senate Commerce Committee's Communications Subcommittee held a hearing on S. 2145 on March 23, 2004. Witnesses discussed the difficulties in legislating in an area where definitions are unclear, and the pace of technology might quickly render any such definitions obsolete. Mr. Robert Holleyman, representing the Business Software Alliance, testified that the focus of legislation should be regulating bad behavior, not technology. He expressed reservations about S. 2145, and called on Congress not to preclude the evolution of tools and marketplace solutions to the problem. Mr. John L. Levine, author of *The Internet for Dummies* and similar books, concluded that the legislation should ban spyware banned entirely, or consumers should be able to give a one-time permanent notice (akin to the telemarketing Do Not Call list) that they do not want spyware on their computers.

---

[6] Testimony to the Senate Committee on Commerce, Science, and Transportation, Subcommittee on Communications, March 23, 2004. Available on CDT's spyware site [http://www.cdt.org/privacy/spyware/] along with a November 2003 CDT report entitled Ghosts in Our Machines: Background and Policy Proposals on the "Spyware" Problem.

He also said that the legislation should allow consumers to sue violators, rather than relying only on the FTC and state Attorneys General to enforce the law. Mr. Berman of CDT noted that three existing laws (including the FTC Act) can be used to address spyware concerns, and that technology measures, self-regulation and user education also are important to dealing with spyware. He concluded that CDT believes that new legislation specifically targeted at spyware would be useful, but that Congress also should pass broad Internet privacy legislation that could address the privacy aspects of the spyware debate.

While there is concern generally about any software product installed without the user's knowledge or consent, one particular area of controversy is programs that cause pop-up ads to appear. Many users object to pop-up ads as vigorously as they do to unsolicited commercial e-mail ("spam"— see CRS Report RL31953). The extent to which pop-up ads are, or should be, included in a definition of spyware was discussed at the Senate Commerce Committee hearing. Mr Avi Naider, President and CEO of WhenU.com, argued that although his company's WhenU software does create pop-up ads, it is not spyware because users are notified that the program is about to be installed, must affirmatively consent to a license agreement, and may decline it. Mr. Naider explained that his program often is "bundled" with software that users obtain for free (called "free-ware"), or a software developer may offer users a choice between paying for the software or obtaining it for free if they agree to receive ads from WhenU. While agreeing that spyware is a serious concern, and that Congress and the FTC should regulate in this area, Mr. Naider urged that legislation be written carefully to exclude products like his that offer notice and choice and therefore should not be considered spyware.

On March 23, 2004, the Governor of Utah signed an anti-spyware law, which will become effective on May 3, 2004.[7] The definition of spyware in that law includes certain pop-up ads. It prohibits, for example, certain pop-up ads that partially or wholly cover or obscure paid advertising or other content on a Web site in a way that interferes with a user's ability to view the Web site. A media report stated that passage of the law was "driven by a Utah company in a legal fight with a pop-up company."[8] The Utah law also defines spyware, inter alia, as software installed on a computer without the user's consent and that cannot be easily disabled and removed. Several high-tech companies reportedly argued that the law could have unintended consequences, for example, prohibiting parents from installing software to block access by their children to certain Websites because the software monitors Web activities, may have been installed without the child's consent, and the child may not be able to uninstall it easily.[9]

As noted, spyware also can refer to "key logging" software that records a person's keystrokes. All typed information thus can be obtained by another party,

---

[7] See [http://www.le.state.ut.us/~2004/bills/hbillenr/hb0323.pdf] for the enrolled text of the law.

[8] Tech Companies Lobby Utah Governor Against Broad Anti-Spyware Bill. Warren's Washington Internet Daily, March 22, 2004 (via Factiva).

[9] Utah Anti-Spyware Bill Opposed by High-Tech Becomes Law. Warren's Washington Internet Daily, March 25, 2004 (via Factiva).

even if the author modifies or deletes what was written, or if the characters do not appear on the monitor (such as when entering a password). Commercial key logging software has been available for some time, but its existence was highlighted in 2001 when the FBI, with a search warrant, installed the software on a suspect's computer, allowing them to obtain his password for an encryption program he used, and thereby evidence. Some privacy advocates argue wiretapping authority should have been obtained, but the judge, after reviewing classified information about how the software works, ruled in favor of the FBI. Press reports also indicate that the FBI is developing a "Magic Lantern" program that performs a similar task, but can be installed on a subject's computer remotely by surreptitiously including it in an e-mail message, for example. Privacy advocates question what type of legal authorization should be required.

Identity Theft

Identity theft is not an Internet privacy issue, but the perception that the Internet makes identity theft easier means that it is often discussed in the Internet privacy context. The concern is that the widespread use of computers for storing and transmitting information is contributing to the 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.[10]

Whether the Internet is responsible for the increase in cases is debatable. Some attribute the rise instead to carelessness by businesses in handling personally identifiable information, and by credit issuers that grant credit without proper checks. In a 2003 survey for the FTC, Synovate found that 51% of victims do not know how their personal information was obtained by the thief; 14% said their information was obtained from lost or stolen wallets, checkbooks, or credit cards;13% said the personal information was obtained during a transaction; 4% cited stolen mail; and 14% said the thief used "other" means (e.g. the information was misused by someone who had access to it such as a family member or workplace associate).[11]

Several laws have been passed regarding identity theft (P.L. 105-318, P.L. 106-433, and P.L. 106-578), but Congress continues to assess ways to reduce the incidence of identity theft and help victims.

On December 4, 2003, the President signed the most recent law, the Fair and Accurate Credit Transactions Act (H.R. 2622, P.L. 108-159). It is discussed in detail in CRS Report RL32121, *Fair Credit Reporting Act: A Side-By-Side Comparison of House, Senate, and Conference Versions*. Among its identity theft-related provisions, the law —

---

[10] See also CRS Report RS21162, *Remedies Available to Victims of Identity Theft*; and CRS Report RS21083, *Identity Theft and the Fair Credit Reporting Act: an Analysis of TRW v. Andrews and Current Legislation*.

[11] Synovate. Federal Trade Commission—Identity Theft Survey Report. September 2003. P. 30-31. [http://www.ftc.gov/opa/2003/09/idtheft.htm]

- requires consumer reporting agencies to follow certain procedures concerning when to place, and what to do in response to, fraud alerts on consumers' credit files;

- allows consumers one free copy of their consumer report each year from nationwide consumer reporting agencies as long as the consumer requests it through a centralized source to be established by the FTC;

- allows consumers one free copy of their consumer report each year from nationwide specialty consumer reporting agencies (medical records or payments, residential or tenant history, check writing history, employment history, and insurance claims) upon request pursuant to regulations to be established by the FTC;

- requires credit card issuers to follow certain procedures if additional cards are requested within 30 days of a change of address notification for the same account;

- requires the truncation of credit card numbers on electronically printed receipts;

- requires business entities to provide records evidencing transactions alleged to be the result of identity theft to the victim and to law enforcement agencies authorized by the victim to take receipt of the records in question;

- requires consumer reporting agencies to block the reporting of information in a consumer's file that resulted from identity theft and to notify the furnisher of the information in question that it may be the result of identity theft;

- requires federal banking agencies, the FTC, and the National Credit Union Administration to jointly develop guidelines for use by financial institutions, creditors and other users of consumer reports regarding identity theft;

- extends the statute of limitations for when identity theft cases can be brought; and

- allows consumers to request that the first five digits of their Social Security Numbers not be included on a credit report provided to the consumer by a consumer reporting agency.

A number of other bills have been introduced in the 108th Congress regarding identity theft and protection of Social Security Numbers. They are described in Table 2 below.

Pending Legislation in the 108th Congress

The following table summarizes legislation pending before the 108th Congress concerning Internet privacy and identity theft (including protection of Social Security Numbers).

Table 2: Pending Internet Privacy-Related Legislation

INTERNET PRIVACY (GENERAL)	
Bill	**Summary**
H.R. 69 Frelinghuysen	**Online Privacy Protection Act.** Requires the FTC to prescribe regulations to protect the privacy of personal information collected from and about individuals not covered by COPPA. (Energy & Commerce)
H.R. 1636 Stearns	**Consumer Privacy Protection Act.** See Table 1 for summary of provisions. (Energy & Commerce)
S. 745 Feinstein	**Privacy Act.** Title I requires commercial entities to provide notice and choice (opt-out) to individuals regarding the collection and disclosure or sale of their PII, with exceptions. (Judiciary)
S. 1695 Leahy	**PATRIOT Oversight Restoration Act.** *Inter alia*, would sunset Sections 210 and 216 of the USA PATRIOT Act on Dec. 31, 2005 (those sections are not subject to the sunset provisions now included in the Act). (Judiciary)
S. 1709 Craig	**Security and Freedom Ensured (SAFE) Act.** *Inter alia* would sunset Section 216 of the USA PATRIOT Act on December 31, 2005. (Judiciary)
SPYWARE	
H.R. 2929 Bono	**Safeguard Against Privacy Invasions Act.** Requires the FTC to establish regulations prohibiting the transmission of spyware programs via the Internet to computers without the user's consent, and notification to the user that the program will be used to collect personally identifiable information (PII). (Energy & Commerce)
S. 2145 Burns	**SPY BLOCK** (Software Principles Yielding Better Levels of Consumer Knowledge). To regulate the authorized installation of computer software, and to require clear disclosure to computer users of certain computer software features that may pose a threat to user privacy. (Commerce) Hearing held March 23, 2004.
IDENTITY THEFT/SOCIAL SECURITY NUMBER PROTECTION	
H.R. 70 Frelinghuysen	**Social Security On-Line Privacy Protection Act.** Regulates the use by interactive computer services of Social Security numbers (SSNs) and related personally identifiable information (PII). (Energy & Commerce)

Bill	Summary
H.R. 220 Paul	**Identity Theft Protection Act.** Protects the integrity and confidentiality of SSNs, prohibits establishment of a uniform national identifying number by federal government, and prohibits federal agencies from imposing standards for identification of individuals on other agencies or persons. (Ways & Means; Government Reform)
H.R. 637 Sweeney **S. 228** Feinstein	**Social Security Misuse Prevention Act.** Limits the display, sale, or purchase of SSNs. H.R. 637 referred to House Ways & Means Committee. S. 228 placed on Senate calendar. [The Senate bill was reintroduced from the 107th Congress, where it was reported from the Senate Judiciary Committee on May 16, 2002—no written report. The bill number in that Congress was S. 848.]
H.R. 818 Kleczka	**Identity Theft Consumers Notification Act.** Requires financial institutions to notify consumers whose personal information has been compromised. (Financial Services)
H.R. 858 Tanner	**Identity Theft Penalty Enhancement Act.** Increases penalties for aggravated identity theft. (Judiciary)
H.R. 1729 Carson	**Negative Credit Information Act.** Requires consumer reporting agencies to notify consumers if information adverse to their interests is added to their files. (Financial Services)
H.R. 1731 Carter	**Identity Theft Penalty Enhancement Act.** Establishes penalties for aggravated identity theft. (Judiciary) Forwarded by subcommittee to full committee March 30, 2004.
H.R. 1931 Kleczka	**Personal Information Privacy Act.** Protects SSNs and other personal information through amendments to the Fair Credit Reporting Act. (Ways & Means, Financial Services)
H.R. 2035 Hooley	**Identity Theft and Financial Privacy Protection Act.** Requires credit card issuers to confirm change of address requests if received within 30 days of request for additional card; requires consumer reporting agencies to include a fraud alert in a consumer's file if the consumer has been, or suspects he or she is about to become, a victim of identity theft; requires truncation of credit and debit card numbers on receipts; requires FTC to set rules on complaint referral, investigations, and inquiries. (Financial Services)
H.R. 2617 Shadegg	**Consumer Identity and Information Security Act.** Prohibits the display of SSNs, with exceptions, and restricts the use of SSNs; prohibits the denial of products or services because an individual will not disclose his or her SSN; requires truncation of credit and debit card numbers on receipts; requires card issuers to verify a consumer's identity if a request for an additional credit card is made, or for a debit card or any codes or other means of access associated with it; requires FTC to set up a centralized reporting system for consumers to report suspected violations. (Financial Services, Ways & Means, Energy & Commerce)

Bill	Summary
H.R. 2633 Emmanuel	**Identity Theft Protection and Information Blackout Act.** Restricts the sale of SSNs and prohibits the display of SSNs by governmental agencies; prohibits the display, sale or purchase of SSNs in the private sector, with exceptions; and makes refusal to do business with anyone who will not provide an SSN an unfair or deceptive act or practice under the FTC Act, with exceptions. (Ways & Means, Energy & Commerce, Judiciary, Financial Services)
H.R. 2971 Shaw	**Social Security Number Privacy and Identity Theft Protection Act.** Restricts the sale of SSNs and prohibits the display of SSNs by governmental agencies; prohibits the display, sale or purchase of SSNs in the private sector, with exceptions; makes refusal to do business with anyone who will not provide an SSN an unfair or deceptive act or practice under the FTC Act; and requires certain methods of verification of identity when issuing or replacing SSNs and cards. (Ways & Means, Financial Services, Energy & Commerce)
H.R. 3233 Gutierrez	**Identity Theft Notification and Credit Restoration Act.** Requires financial institutions and financial services providers to notify customers of the authorized use of personal information, amends the Fair Credit Reporting Act to require fraud alerts to be included in consumer credit files, and provides consumers with enhanced access to credit reports in such cases. (Financial Services)
H.R. 3693 Scott	**Identity Theft Investigation and Prosecution Act.** Provides additional resources to the Department of Justice for investigating and prosecuting identity theft and related credit card and other fraud. (Judiciary)
S. 153 Feinstein	**Identity Theft Penalty Enhancement Act.** Increases penalties for identity theft. (Judiciary) [This bill was reintroduced from the 107th Congress where it was reported by the Senate Judiciary Committee on November 14, 2002—no written report. The bill number in that Congress was S. 2541.] **Passed Senate without amendment March 19, 2003.**
S. 223 Feinstein	**Identity Theft Prevention Act.** Requires credit card numbers to be truncated on receipts; imposes fines on credit issuers who issue new credit to identity thieves despite the presence of a fraud alert on the consumer's credit file; entitles each consumer to one free credit report per year from the national credit bureaus; and requires credit card companies to notify consumers when an additional credit card is requested on an existing credit account within 30 days of an address change request. (Banking)
S. 745 Feinstein	**Privacy Act.** Title II is the Social Security Misuse Prevention Act (S. 228, see above H.R. 637/S. 228 above).

Bill	Summary
S. 1533 Cantwell	**Identity Theft Victims Assistance Act.** Requires business entities with knowledge of an identity theft to share information with the victim or law enforcement agencies and requires consumer reporting agencies to block dissemination of information resulting from an identity theft, with exceptions. This bill is reintroduced from the 107th Congress where it was S 1742. (Judiciary)
S. 1581 Cantwell	**Identity Theft Victims Assistance Act.** Similar to S. 1533, but *inter alia* expressly states that the bill does not provide for private right of action, establishes an affirmative defense, and excludes consumer reporting agencies that are reselling information from some of the Act's provisions under specified conditions. (Judiciary)
S. 1633 Corzine	**Identity Theft and Credit Restoration Act.** Requires financial institutions and financial service providers to notify customers of the unauthorized use of personal information, requires fraud alerts to be included in consumer credit files in such cases, and provides customers with enhanced access to credit reports in such cases. (Banking)
S. 1749 Specter	**Prevent Identity Theft From Affecting Lives and Livelihoods (PITFALL) Act.** Amends the Consumer Protection Act to provide relief for victims of identity theft. (Banking)

Appendix: Internet Privacy-Related Legislation Passed by the 107th Congress

H.R. 2458 (Turner)/ **S. 803** (Lieberman) **P.L. 107-347**	**E-Government Act**. *Inter alia*, sets requirements on government agencies in how they assure the privacy of personal information in government information systems and establish guidelines for privacy policies for federal Web sites.
H.R. 5505 (Armey) **P.L. 107-296**	**Homeland Security Act.** Incorporates **H.R. 3482, Cyber Security Enhancement Act,** as Sec. 225. Loosens restrictions on ISPs, set in the USA PATRIOT Act, as to when, and to whom, they can voluntarily release information about subscribers.
H.R. 2215 (Sensenbrenner) **P.L. 107-273**	**21st Century Department of Justice Authorization Act.** Requires the Justice Department to notify Congress about its use of Carnivore (DCS 1000) or similar Internet monitoring systems.
H.R. 3162 (Sensenbrenner) **P.L. 107-56**	**USA PATRIOT Act.** Expands law enforcement's authority to monitor Internet activities. See CRS Report RL31289 for how the Act affects use of the Internet. Amended by the Homeland Security Act (see P.L. 107-296).