Order Code RL31408

Internet Privacy: Overview and Pending Legislation

Updated January 14, 2003

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

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 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) requires the Justice Department to report to Congress on its use of Internet monitoring software such as Carnivore/DCS 1000. 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) expands 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, in the 107th Congress, 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, tracks Internet privacy legislation pending before the 108th Congress, and describes legislation that was considered by the 107th Congress, including the four bills that were enacted (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* (March 4, 2002). For information on wireless privacy issues, including wireless Internet, see CRS Report RL31636, *Wireless Privacy: Availability of Location Information for Telemarketing* (regularly updated).

This report will be updated.

Contents

List of Tables

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* (December 21, 2000), and CRS Report RL31289, *The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government* (March 4, 2002).

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 to protect the privacy of children under 13 as they use commercial Web sites (see below). 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/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.

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 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."[1]

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 EPIC [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 the Electronic Privacy Information Center (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 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

---

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

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.

Legislation in the 107th and 108th Congresses

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 The text is not publicly available yet, but based on its official title, it appears similar to H.R. 89 from the 107th Congress.

Many other Internet privacy bills were considered by, but did not clear, the 107th Congress. H.R. 89 and three others (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. H.R. 4678 and S. 2201 became the focus of debate last year and are discussed in more detail below and in Appendix 2. 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 (Cleland) 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 and H.R. 4678. 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 proposed 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. Appendix 2 provides a brief comparison of H.R. 4678 as introduced and S. 2201 as reported.

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. 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) 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.

The following bills did not clear the 107th Congress. S. 851 (Thompson) would have established 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 have created a commission to study privacy issues more broadly. S. 2846 (Edwards) also would have created a commission, in this case, to "evaluate investigative and surveillance technologies to meet law enforcement and national security needs in the manner that best preserves the personal dignity, liberty,

and privacy of individuals within the United States." S. 2629 (Torricelli) would have provided a framework for ensuring effective data and privacy management by federal agencies. S. 2201 would have required federal agencies that are Internet Service Providers or Online Service Providers, or operate Web sites, to provide notice, choice, access, and security in a manner similar to what the bill requires for non-governmental entities, with exceptions. (S. 2201 is discussed in more detail in the appendix to this report.)

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 bills (H.R. 112 and S. 197) in the 107th Congress would have required notification. There was no action on either bill.

Another use of the term spyware refers to software that can record a person's keystrokes. All typed information thus can be obtained by another party, 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 products have been available for some time, but the existence of such "key logging" software was highlighted in a 2001 case against Mr. Nicodemo Scarfo, Jr. on charges of illegal gambling and loan sharking. Armed with a search warrant, the FBI installed the software on Mr. Scarfo'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.

Monitoring E-mail and Web Usage by Law Enforcement or Employers

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 Internet Service

Providers' (ISP's) equipment. Privacy advocates are concerned whether Carnivore-like systems can differentiate between e-mail and Internet usage by a 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) requires the Justice Department to report to Congress on its use of 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 potential implications for Internet privacy of the new law are discussed in CRS Report RL31289. Privacy advocates complain that it is extremely difficult to monitor how the USA PATRIOT Act is being implemented because the Justice Department refuses to make information available either through Freedom of Information (FOIA) requests or to Congress. The American Civil Liberties Union (ACLU), EPIC, and others filed a complaint for injunctive relief in U.S. District Court for the District of Columbia on October 24, 2002, to force the Justice Department to state which records it will disclose in response to the FOIA requests, and to disclose those records.

As part of the Homeland Security Act (P.L. 107-296), Congress incorporated (as section 225) the text of H.R. 3482, which passed the House on June 15, 2002. The language amends the USA PATRIOT Act, lowering the threshold for when ISPs may divulge the content of communications, and to whom. Under H.R. 3482, the ISPs need only a "good faith" belief (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 concerned about the language for a number of reasons. For example, EPIC notes that allowing such information to be disclosed to any governmental entity not only poses increased risk to personal privacy, but also is a poor security strategy; and that the language does not provide for judicial oversight of the use of these procedures.[2]

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 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. 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

---

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

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.

Identity Theft and Protecting Social Security Numbers

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). A March 2002 GAO report (GAO-02-363) discusses the prevalence and cost of identify theft. The FTC has a toll free number (877-ID-THEFT) to help victims. (See also CRS Reports RS21162, *Remedies Available to Victims of Identity Theft*; and RS21083, *Identity Theft and the Fair Credit Reporting Act: an Analysis of TRW v. Andrews and Current Legislation*).

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 2001, the FTC found that less than 1% of identity theft cases are linked to the Internet *(Computerworld*, February 12, 2001, p. 7). Several laws already exist regarding identity theft (P.L. 105-318, P.L. 106-433, and P.L. 106-578).

A number of bills were introduced in the 107th Congress. One, S. 1742 (Cantwell), was reported, amended (no written report), from the Senate Judiciary Committee on May 21 and passed the Senate November 14. There was no further action, however. S. 848 (Feinstein) was reported, amended (no written report), from the Senate Judiciary Committee on May 16, 2002, and referred to the Senate Finance Committee, which held a hearing on July 11. A new bill, S. 3100, was introduced by Senator Feinstein on October 10, 2002, and placed on the Senate calendar. There was no further action. Senator Feinstein also introduced S. 2541, which would have created a separate crime of aggravated identity theft, and provided for additional penalties for certain crimes involving identity theft. The bill was reported from the Senate Judiciary Committee (no written report) on November 14, 2002, but there was no further action. Other related 107th Congress bills, on which there was no action, were: H.R. 91, H.R. 220, H.R. 1478, H.R. 2036/S. 1014, H.R. 3053/S. 1399, and H.R. 5424.

Two bills have been introduced so far in the 108th Congress: H.R. 70 (Frelinghuysen) and H.R. 220 (Paul). H.R. 70 would regulate the use by interactive computer services of SSNs and related PII. H.R. 220 would protect the integrity and confidentiality of SSNs, prohibit establishment of a uniform national identifying number by the federal government, and prohibit federal agencies from imposing standards for identification of individuals on other agencies or persons. The texts of those bills are not yet publicly available, but based on their official titles, they are similar to H.R. 91 and H.R. 220 from the 107th Congress.

Table 1: Legislation Pending in the 108th Congress

H.R. 69 Frelinghuysen	Requires the FTC to prescribe regulations to protect the privacy of personal information collected from and about individuals not covered by COPPA. (Energy and Commerce)
H.R. 70 Frelinghuysen	Regulates the use by interactive computer services of Social Security numbers (SSNs) and related personally identifiable information (PII). (Energy and Commerce)
H.R. 220 Paul	Protects the 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 and Means; Government Reform)

Appendix 1: 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).

Appendix 2: Brief Comparison of H.R. 4678 and S. 2201 From the 107th Congress

Of the many broad Internet privacy bills introduced in the 107th Congress, congressional attention focused on H.R. 4678 and S. 2201 (reported from the Senate Commerce Committee on August 1, 2002, S.Rept. 107-240). The following table provides a brief comparison of the two bills. One fundamental difference is that H.R. 4678 affects privacy for both "online" and "offline" entities, while S. 2201's focus is online entities. During markup of S. 2201, however, a provision was added requiring the FTC to provide recommendations and draft regulations for entities otherwise not covered by the bill.

Comparison of H.R. 4678 and S. 2201 From the 107th Congress (Explanation of Acronyms at End)

Provision	**H.R. 4678 (Stearns) As Introduced**	**S. 2201 (Hollings) As Reported**
Title	Consumer Privacy Protection Act	Online Personal Privacy Act
Entities Covered	Data Collection Organi-zations, defined as entities that collect (by any means, through any medium), sell, disclose for consideration, or use, PII. Excludes govern-mental agencies, certain not-for-profit entities, and certain small businesses.	ISPs, OSPs, and commercial Web Sites; certain third parties; federal agencies if they are ISPs, OSPs, or operate Web sites (with exceptions); and U.S. Senate (Sergeant at Arms shall develop conforming regulations for Senate). Excludes certain small businesses.
FTC Must Submit Recommendations and Proposed Regulations for Entities Not Covered by the Act	No [the Act already covers both "online" and "offline" entities]	Yes
Differentiation Between Sensitive and Non-Sensitive PII	No	Yes
Adherence to Fair Infor-mation Practices Notice Choice Access Security	 Yes, with exceptions Yes (Opt-Out) No Yes	 Yes, with exceptions Yes (Opt-In for sensitive PII; Opt-Out for non-sensitive PII) Yes, with exceptions Yes

Provision	H.R. 4678 (Stearns) As Introduced	S. 2201 (Hollings) As Reported
Enforcement	By FTC	Generally by FTC, but by other entities in some cases (e.g., Board of Directors of FDIC enforces for banks insured by FDIC under Federal Deposit Insurance Act).
Private Right of Action	No	Yes, for sensitive PII only. Creates affirmative defense if defendant takes certain steps to ensure compliance with Act, or complies with specified self regulatory requirements.
Relationship to State Laws	Preempts state privacy laws, regulations, etc. that affect collection, use, sale, disclosure, or dissemination of PII in commerce.	Supersedes state statutes, regulations, or rules regarding collection, use, or disclosure of PII obtained through the Internet.
Actions by States	No comparable provision.	A state attorney general may bring suit on behalf of residents of that state, but must notify FTC and FTC may intervene.
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.	Amends Communications Act of 1934 so cable operators of Internet services, online services, or commercial Websites are governed by this Act if there is a conflict between it and the 1934 Act. Remedies under safe harbor and private right of action are in addition to any other remedy under any provision of law. Certain disclosures to comply with FCA, COPPA, Gramm-Leach-Bliley are protected.

Provision	**H.R. 4678 (Stearns) As Introduced**	**S. 2201 (Hollings) As Reported**
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 partner (as defined in the Act) of the entity.	In addition to permitted disclosures under other laws (see above), disclosures also permitted to law enforcement agencies under certain conditions, under court order, for certain emergencies, or for professional services purposes.
Establishes Self-Regulatory "Safe Harbor"	Yes	Yes
Requires Notice to Users If Entity's Privacy Policy Changes	No	Yes
Requires Notice to Users if Privacy is Breached	No	Yes
Whistleblower Protection	No	Yes
Directs NIST to Encourage and Support Development of Internet Privacy Computer Programs, Protocols, or Other Software, Such as P3P	No	Yes
Identity Theft Prevention and Remedies	Yes	No
Requires GAO study of impact on U.S. interstate and foreign commerce of foreign information privacy laws, and rededication by Secretary of Commerce if GAO finds discriminatory treatment of U.S. entities	Yes	No
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	No

COPPA - Children's Online Privacy Protection Act
FCA = Fair Credit Reporting Act
FDIC = Federal Deposit Insurance Corporation
FTC = Federal Trade Commission
GAO = General Accounting Office
ISP = Internet Service Provider
NIST = National Institute of Standards and Technology (in the Department of Commerce)
OSP = Online Service Provider
PII = Personally Identifiable Information
P3P = Platform for Privacy Preferences (see text for explanation)