

Report for Congress

Received through the CRS Web

Internet Privacy: Overview and Pending Legislation

Updated July 18, 2002

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 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 Department of Justice authorization bill (H.R. 2215) requires the Justice Department to report to Congress on its use of Internet monitoring software such as Carnivore/DCS 1000, but Congress also passed the USA PATRIOT Act (P.L. 107-56) that, *inter alia*, makes it easier for law enforcement to monitor Internet activities.

The parallel debate over Web site information policies concerns whether industry self regulation or legislation is the best approach to protecting consumer privacy.

This report provides a brief overview of Internet privacy issues and tracks pending legislation. For more detailed discussion of the issues, see CRS Report RL30784, *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).

Contents

Introduction	1
Internet: Collection of Data by	
Commercial Web Site Operators	1
Children’s Online Privacy Protection Act (COPPA), P.L. 105-277	1
FTC Activities and Fair Information Practices	2
Advocates of Self-Regulation	3
Advocates of Legislation	3
Internet: Federal Government Web Site Information Practices	4
Spyware	5
Monitoring E-mail and Web Usage by Law Enforcement or Employers	5
Identity Theft and Protecting Social Security Numbers	6
Appendix: Brief Comparison of H.R. 4678 and S. 2201	10

List of Tables

Table 1: Pending Legislation Concerning Internet Privacy and Related Issues ...	8
Table 2: Brief Comparison of H.R. 4678 and S. 2201	10

Internet Privacy: Overview and Pending Legislation

Introduction

Internet privacy issues encompass concerns about the collection of personally identifiable information (PII) from visitors to 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: Collection of Data by Commercial Web Site Operators

One aspect of the Internet (“online”) privacy debate focuses on whether industry self regulation or legislation is the best route to assure consumer privacy protection. In particular, consumers appear concerned about the extent to which Web site operators collect “personally identifiable information” (PII) and share that data with third parties without their knowledge. Repeated media stories about privacy violations by Web site operators have kept the issue in the forefront of public debate about the Internet. Although many in Congress and the Clinton Administration preferred industry self regulation, the 105th Congress passed legislation to protect the privacy of children under 13 as they use commercial Web sites (see below). Many bills have been introduced since that time, but the only legislation that has passed concerns federal, 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.

Four bills (H.R. 89, H.R. 237, H.R. 347, and S. 2201) are pending specifically on this topic; H.R. 4678 is a broader consumer privacy protection bill. Also, the Senate-passed version of the bankruptcy reform bill (S. 420) would prohibit (with exceptions) companies, including Web site operators, that file for bankruptcy from selling or leasing PII obtained in accordance with a policy that said such information would not be transferred to third parties, if that policy was in effect at the time of the bankruptcy filing. H.R. 2135 would limit the disclosure of personal information (defined as PII and sensitive personal information) by information recipients in general, and S. 1055 would limit the commercial sale and marketing of PII.

Congressional attention currently is focused on S. 2201 and H.R. 4678. A fundamental difference is that H.R. 4678 affects privacy for both “online” and “offline” data collection entities, while S. 2201’s focus is 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 ordered reported on May 17, 2002. The appendix to this report provides a brief comparison of H.R. 4678 as introduced and S. 2201 as ordered reported.

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>]). However, some privacy interest groups such as the Electronic Privacy Information Center (EPIC) feel that P3P is too complex and confusing and that it fails to address many privacy issues. An EPIC report from June 2000 further explains its findings [<http://www.epic.org/reports/pretypoorprivacy.html>]. The CATO Institute, however, argues that privacy-protecting technologies are quite effective (available on CATO’s web site [<http://www.cato.org/pubs/briefs/bp-065es.html>]).

Advocates of Legislation

Consumer, privacy rights and other interest groups believe self regulation is insufficient. They argue that the seal programs do not carry the weight of law, and that while a site may disclose its privacy policy, that does not necessarily equate to having a policy that protects privacy. The Center for Democracy and Technology (CDT, at [<http://www.cdt.org>]) and EPIC [<http://www.epic.org>]) each have released reports on this topic. A particular concern is online profiling where companies collect data about what Web sites are visited by a particular user and develop profiles of that user’s preferences and interests for targeted advertising. Following a one-day workshop on online profiling, FTC issued a two-part report in the summer of 2000 that also heralded the announcement by a group of companies that collect such data,

the Network Advertising Initiative (NAI), of self-regulatory principles. At that time, the FTC nonetheless called on Congress to enact legislation to ensure consumer privacy vis a vis online profiling because of concern that “bad actors” and others might not follow the self-regulatory guidelines. The current FTC Chairman’s position is that broad legislation is not needed at this time.

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), and in the FY2003 Treasury-Postal appropriations bills (sec. 634 in both H.R. 5120 and S. 2740).

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. S. 851 (Thompson) would establish an 18-month commission to study the collection, use, and distribution of personal information by federal, state, and local governments. H.R. 583 (Hutchinson) would create a commission to study privacy issues more broadly. Section 208 of S. 803 (Lieberman) as passed by the Senate on June 27, 2002, would set requirements on government agencies in how

they assure the privacy of PII in government information systems, and establish privacy guidelines for federal Web sites. S. 2201 *inter alia* requires 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 pending bills (H.R. 112 and S. 197) would require notification.

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 reportedly 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.

To help oversee FBI use of Carnivore/DCS 1000, the FY2002 Department of Justice authorization bill (H.R. 2215), as passed by the House and Senate, 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 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.

On July 15, 2002, the House passed H.R. 3482 which would amend P.L. 107-56 and, *inter alia*, lower the threshold for when ISPs may divulge the content of communications, and to whom. Under H.R. 3482, the ISP would need 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 governmental entity" (instead of a "law enforcement agency"). Privacy advocates are concerned about the language. The chairman and ranking Democrat of the House Judiciary Committee, Representatives Sensenbrenner and Conyers, wrote to the Attorney General on June 13, 2002 requesting information about implementation of the USA PATRIOT Act [www.house.gov/judiciary/ashcroft061302.htm].

There also is concern about the extent to which employers monitor the e-mail and other computer activities of employees. A 2001 survey by the American Management Association [<http://www.amanet.org/press/amanews/ems2001.htm>] found that 62.8% of the companies surveyed monitor Internet connections, 46.5% store and review e-mail, and 36.1% store and review computer files. The public policy concern appears to be not whether companies should be able to monitor activity, but whether they should notify their employees of that monitoring.

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 identity theft. The FTC has a toll free number (877-ID-THEFT) to help victims.

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 (P.L. 105-318, P.L. 106-433, and P.L. 106-578) and additional legislation is pending (H.R. 91, H.R. 220, H.R. 1478, H.R. 2036/S.1014, S. 848, H.R. 3053/S. 1399, S. 1742, and S. 2541). H.R. 4678 also has provisions regarding identity theft. Hearings have been held on some of these bills. S. 848 was reported, amended (no written report), from the Senate Judiciary Committee on May 16, 2002, and subsequently referred to the Senate Finance Committee, which held a hearing on July 11. S. 1742 was reported, amended (no written report), from Senate Judiciary on May 21.

Table 1: Pending Legislation Concerning Internet Privacy and Related Issues

H.R. 89 (Frelinghuysen)	Online Privacy Protection Act. Requires FTC to prescribe regulations to protect privacy of personal information collected from and about individuals not covered by COPPA. (Energy & Commerce)
H.R. 91 (Frelinghuysen)	Social Security Online Privacy Protection Act. Regulates use by interactive computer services of SSNs and related personally identifiable information. (Energy & Commerce)
H.R. 112 (Holt)	Electronic Privacy Protection Act. Makes it unlawful for any person to knowingly make, import, export, distribute, sell, offer for sale, install or use “spyware” without disclosure or notice. (Energy & Commerce)
H.R. 220 (Paul)	Identity Theft Prevention Act. Protects integrity and confidentiality of SSNs, prohibits establishment of a uniform national identifying number by federal governments, and prohibits federal agencies from imposing standards for identification of individuals on other agencies or persons. (Ways & Means, Government Reform)
H.R. 237 (Eshoo)	Consumer Internet Privacy Enhancement Act. Requires Web site operators to provide clear and conspicuous notice of their information practices and provide consumers with easy method to limit use and disclosure of their information. Preempts state and local laws if they are inconsistent with or more restrictive than this one. Directs FTC to enforce the law. State Attorneys General can bring suits in federal courts. Sets penalties. (Energy & Commerce).
H.R. 333 (Gekas)/ S. 420 (Grassley)	Bankruptcy Reform Act. S. 420 passed the Senate March 15, 2001. Sections 231 and 232 limit when companies can sell or lease PII collected in accordance with a policy in effect at the time of the bankruptcy filing. H.R. 333 as passed by the House March 1 does not have this provision. Senate passed H.R. 333 with amendment in the nature of a substitute July 17. House and Senate conferees appointed.
H.R. 347 (Green)	Consumer Online Privacy and Disclosure Act. Requires FTC to promulgate regulations requiring Web site or online service operators about notice, choice, and contact information for the operator. (Energy & Commerce)
H.R. 583 (Hutchinson)	Privacy Commission Act. Creates a Commission for the Comprehensive Study of Privacy Protection. (Government Reform)
H.R. 1478 (Kleczka)	Personal Information Privacy Act. Prohibits use of SSNs for commercial purposes without consent; prohibits sale or transfer of transaction or experience information without consent; and repeals certain provisions relating to distribution of consumer reports re certain transmissions not initiated by the consumer. (Ways & Means, Financial Services)
H.R. 2036 (Shaw)/ S. 1014 (Bunning)	Social Security Number Privacy and Identity Theft Protection Act. Restricts sale and display of SSNs by government agencies, with exceptions; and restrict sale, purchase, and display of SSNs in the private sector, with exceptions. (House Ways & Means, Energy & Commerce, Financial Services; Senate Finance)
H.R. 2135 (Sawyer)	Consumer Privacy Protection Act. Limits disclosure of personally identifiable information and sensitive personal information by information recipients. (Energy & Commerce)
H.R. 2215 (Sensenbrenner)/ S. 1319 (Leahy)	Department of Justice Authorization Act. Establishes congressional reporting requirements re use of DCS 1000/Carnivore. H.R. 2215 passed House July 23; passed Senate, amended, Dec. 20. (S. 1319 reported Nov. 8, S. Rept. 107-96).
H.R. 3053 (Hooley)/ S. 1399 (Feinstein)	Identity Theft Protection Act. Establishes certain requirements for credit card issuers and consumer reporting agencies. (House Financial Services; Senate Banking)

H.R. 3482 (Smith)	Cyber Security Enhancement Act. <i>Inter alia</i> , loosens restrictions on ISPs as to when, and to whom, they can voluntarily release information about subscribers if they believe there is a danger of death or injury. Passed House July 15.
H.R. 4678 (Stearns)	Consumer Privacy Protection Act. Requires data collection organizations to provide notice, choice, and security; and have privacy policies. (Bill is not Internet-specific). Participation in an approved self-regulatory program creates presumption of compliance with the Act. Preempts state privacy laws. Sets time limits for resolution of identity theft disputes. (Energy & Commerce, International Relations) See appendix for more detail.
H.R. 5120 (Istook)/ S. 2740 (Dorgan)	FY2003 Treasury-Postal Appropriations Act. Sec. 634 prohibits funds 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 to language in FY2001 and FY2002 acts.) Reported from House Appropriations Committee (H. Rept. 107-575).
S. 197 (Edwards)	Spyware Control and Privacy Protection Act. Requires that software made available to the public include clear and conspicuous notice if it includes spyware. Spyware may not be enabled unless the user provides affirmative consent, with exceptions. Sets restrictions on how information collected by spyware can be used and allows the user reasonable access to the information. (Commerce)
S. 803 (Lieberman)	E-Government Act. Sec. 208 sets requirements on government agencies in how they assure the privacy of personally identifiable information in government information systems and establish guidelines for privacy policies for federal Web sites. Passed Senate, amended, June 27, 2002.
S. 848 (Feinstein)	Social Security Number Misuse Prevention Act. Limits display, sale, or purchase of SSNs. Reported from Senate Judiciary May 16, 2002 (no written report); referred to Finance Committee (hearing held July 11).
S. 851 (Thompson)	Citizen's Privacy Commission Act. Would study the collection, use, and distribution of personal information by federal, state, and local governments. (Governmental Affairs)
S. 1055 (Feinstein)	Privacy Act of 2001. Restricts commercial sale and marketing of personally identifiable information, limits the use of SSNs, limits sale and sharing of nonpublic personal financial information, limits provision of protected health information. (Judiciary)
S. 1742 (Cantwell)	Restore Your Identity Act. Requires business entities with knowledge of an identity theft to share information with the victim or law enforcement and requires consumer reporting agencies to block dissemination of information resulting from an identity theft, with exceptions. Reported from Senate Judiciary May 21, 2002; no written report.
S. 2201 (Hollings)	Online Personal Privacy Act. Establishes requirements for ISPs, Online Service Providers (OSPs), and commercial Website operators to provide notice, choice, access, and security to protect PII, which is divided into "sensitive" and "non-sensitive" information for which different requirements apply. The Act applies to federal agencies that operate web sites or serve as ISPs and OSPs, with exceptions. Ordered reported from Senate Commerce May 17, 2002. See appendix for more detail.
S. 2541 (Feinstein)	Identity Theft Penalty Enhancement Act. <i>Inter alia</i> , creates a separate crime of "aggravated identity theft" if a person uses another person's identity to commit certain federal crimes; provides for additional 2 year penalty for committing certain federal crimes while using another person's identity, and additional 5 year penalty for a person using a stolen identity while committing specified federal terrorism crimes. Increases maximum penalty for identity theft from 3 years to 5 years. (Judiciary)

Appendix: Brief Comparison of H.R. 4678 and S. 2201

Of the many pending Internet privacy bills, congressional attention is currently focused on H.R. 4678 and S. 2201 (ordered reported from the Senate Commerce Committee on May 17, 2002). 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 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.

Table 2: Brief Comparison of H.R. 4678 and S. 2201
(Explanation of Acronyms at End)

Provision	H.R. 4678 (Stearns) As Introduced	S. 2201 (Hollings) As Ordered Reported
Title	Consumer Privacy Protection Act	Online Personal Privacy 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 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

Provision	H.R. 4678 (Stearns) As Introduced	S. 2201 (Hollings) As Ordered Reported
Adherence to Fair Information 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
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.

Provision	H.R. 4678 (Stearns) As Introduced	S. 2201 (Hollings) As Ordered Reported
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.
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
Whistle blower Protection	No	Yes
Directs NIST to Encourage and Support Development of Internet Privacy Computer Programs, Protocols, or Other Software, Such as P3P	No	Yes

Provision	H.R. 4678 (Stearns) As Introduced	S. 2201 (Hollings) As Ordered Reported
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)