Order Code RL31408

CRS Report for Congress
Received through the CRS Web

Internet Privacy: Overview and Pending Legislation

Updated March 16, 2005

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

Internet Privacy: Overview and Pending Legislation

Summary

Internet privacy issues generally encompass two types of concerns. One is the collection of personally identifiable information (PII) by website operators from visitors to government and commercial websites, or by software that is surreptitiously installed on a user's computer ("spyware") and transmits the information to someone else. The other is the monitoring of electronic mail and Web usage by the government or law enforcement officials, employers, or Internet Service Providers.

The September 11, 2001 terrorist attacks intensified debate over the issue of law enforcement monitoring, with some advocating increased tools for law enforcement officials to track down terrorists, and others cautioning that fundamental tenets of democracy, such as privacy, not be endangered in that pursuit. Congress passed the 2001 USA PATRIOT Act (P.L. 107-56) that, *inter alia*, makes it easier for law enforcement to monitor Internet activities. That act was later amended by the Homeland Security Act (P.L. 107-296), loosening restrictions as to when, and to whom, Internet Service Providers may voluntarily release the content of communications if they believe there is a danger of death or injury. The report of the 9/11 Commission called for a full and informed debate on the USA PATRIOT Act, and creation of a board to ensure that privacy and civil liberties are protected. Congress directed that a Privacy and Civil Liberties Oversight Board be established as part of the law that implements many of the Commission's recommendations (P.L. 108-457, the Intelligence Reform and Terrorism Prevention Act).

The debate over website 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* website operators to follow certain fair information practices, but none has passed. Legislation has passed, however, regarding information practices for *federal government* websites e.g, the E-Government Act (P.L. 107-347).

The growing controversy about how to protect computer users from "spyware" without creating unintended consequences is discussed in CRS Report RL32706. Another issue, 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. For example, a practice called "phishing" may contribute to identity theft. Those topics are briefly discussed in this report, but more information is available in CRS Report RS22082, CRS Report RL31919, and CRS Report RL32535. Wireless privacy issues are discussed in CRS Report RL31636.

This report tracks Internet privacy-related legislation in the 109th Congress, and provides an overview of Internet privacy issues and related laws passed in the previous two Congresses.

This report will be updated.

Contents

Introduction 1

Internet: Commercial Website 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
Congressional Action 4

Internet: Federal Government Website Information Practices 4

Monitoring of E-mail and Web Usage 5
By Government and Law Enforcement Officials 5
The USA PATRIOT Act 5
Concerns about the USA PATRIOT Act 6
Sunset Clause of the USA Patriot Act 7
The 9/11 Commission Report, and Creation of the Privacy and Civil Liberties Oversight Board 7
By Employers 8
By E-Mail Service Providers: The "Councilman Case" 8

Spyware 10

Identity Theft (Including Phishing) 10
Identity Theft Statistics 11
"Phishing" 11
Existing Laws 12
Congressional Action 14

Summary of 109th Congress Internet Privacy-Related Legislation 14

Appendix A. Internet Privacy-Related Legislation Passed by the 108th Congress 17

Appendix B. Internet Privacy-Related Legislation Passed by the 107th Congress 17

List of Tables

Table 1: Pending Legislation in the 109th Congress 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 websites, as well as debate over law enforcement or employer monitoring of electronic mail and Web usage. This report discusses Internet privacy issues and tracks legislation. Background 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 Website 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 website operators collect "personally identifiable information" (PII) and share that data with third parties without their knowledge. 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 websites. 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, websites.

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 websites. 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 websites 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

websites to comply with the law. The FTC approved self-regulatory guidelines proposed by the Better Business Bureau on January 26, 2001. On June 11, 2003, then-FTC Chairman Timothy Muris stated in testimony to the Senate Commerce Committee that the FTC had 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 conducted or sponsored several surveys between 1997 and 2000 to determine the extent to which commercial website operators abided 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 website [http://www.ftc.gov].

Briefly, the first two FTC surveys (December 1997 and June 1998) created concern about the information practices of websites directed at children and led to the enactment of COPPA (see above). The FTC continued monitoring websites 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 websites and 42% of the 100 most popular websites had implemented all four fair information practices. The FTC voted to recommend that Congress pass legislation requiring websites to adhere to the four fair information practices, but the 3-2 vote indicated division within the Commission. On October 4, 2001, Timothy Muris, who had recently become FTC Chairman, stated that he did not see a need for additional legislation at that time. (Mr. Muris was succeeded as FTC Chairman on August 16, 2004 by Deborah Platt Majoras.)

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 websites. To display a seal from one of those organizations, a website 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

---

[1] Prepared statement of Timothy Muris, Chairman, Federal Trade Commission, p. 10, available at [http://commerce.senate.gov/hearings/witnesslist.cfm?id=807].

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 such technology. It essentially creates machine-readable privacy policies through which users can match their privacy preferences with the privacy policies of the websites they visit. One concern is that P3P requires companies to produce shortened versions of their privacy policies, which could raise issues of whether the shortened policies are legally binding, since they may omit nuances and "sacrifice accuracy for brevity."[2] For more information on P3P, see [http://www.w3.org/P3P/].

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 released reports on this topic. EPIC's most recent report, *Privacy Self Regulation: A Decade of Disappointment*, argues that the National Do Not Call list, which restricts telemarketing phone calls, demonstrates that government regulation can be more effective than industry self regulation. Calling telemarketing a 20th Century problem, the report concludes that the FTC has given self regulation a decade to work in the Internet privacy arena, and it is time for the agency "to apply the lessons from telemarketing and other efforts to address the 21st century [sic] problem of Internet privacy."[3]

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 websites 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.

---

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

[3] EPIC. Privacy Self Regulation: A Decade of Disappointment, by Chris Jay Hoofnagle. March 4, 2005. [http://www.epic.org/reports/decadedisappoint.pdf] p.5.

Congressional Action

Many Internet privacy bills were considered by, but did not clear, the 107th and 108th Congresses. Other than extending an existing prohibition regarding federal websites (see next section), none cleared Congress. Legislation is pending again in the 109th Congress. H.R. 84 (Frelinghuysen) would extend the protections in COPPA to those not currently covered by that act.

Internet: Federal Government Website 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 website) 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 websites should be required to abide by FTC's four fair information practices. The incident sparked interest in whether federal websites 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 website or enter into agreements with third parties to do so, with exceptions. Similar language has been included in subsequent appropriations bills. For FY2005, it is Sec. 633 of the Transportation-Treasury Appropriations Act (incorporated into P.L. 108-447, the FY2005 Consolidated Appropriations Act).

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 websites. 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 websites. An April 2001 GAO report (GAO-01-424) concluded that most of the 65 sites it reviewed were following OMB's guidance.

The E-Government Act (P.L. 107-347) 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 websites. The law requires federal websites 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 website privacy policies into a standardized machine-readable format, enabling P3P to work (see above discussion of P3P), for example.

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 websites 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, used a software program, called Carnivore (later renamed DCS 1000), to intercept e-mail and monitor Web activities of certain suspects. The FBI would install the software on the equipment of Internet Service Providers (ISPs). Privacy advocates were concerned about whether Carnivore-like systems can differentiate between e-mail and Internet usage by a subject of an investigation and similar usage by other people. Technical details of the system were not publicly available, meaning that privacy groups were unable to independently determine exactly what the system could or could not do, leading to their concerns. Section 305 of the 21st Century Department of Justice Appropriations Authorization Act (P.L. 107-273) required the Justice Department to report to Congress at the end of FY2002 and FY2003 on its use of Carnivore/DCS 1000 or any similar system. EPIC obtained the reports in January 2005 under the Freedom of Information Act and placed them on its website.[4] The reports indicate that the Justice Department no longer uses Carnivore/DCS 1000 commercially available software instead. The Justice Department reported that it used commercial software to conduct court-ordered electronic surveillance five times in FY2002 and eight times in FY2003.

The USA PATRIOT Act. 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:

---

[4] See:[http://www.epic.org/privacy/carnivore/2002_report.pdf] and [http://www.epic.org/privacy/carnivore/2003_report.pdf]

- 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 2002 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 four-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 2002 Homeland Security Act (P.L. 107-296), amends section 212 of the USA PATRIOT Act. 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").

Concerns about the USA PATRIOT Act. Privacy advocates are especially concerned about the 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] A Senate Judiciary Committee hearing on September 23, 2004 explored some of these concerns.

Sunset Clause of the USA Patriot Act. As noted, several sections of the USA PATRIOT Act are covered by a "sunset" provision (Sec. 224) under which they will expire on December 31, 2005. Three bills were introduced in the 108th Congress that would have affected the sunset clause, but none passed. For more on the sunset clause, see CRS Report RL32186.

The 9/11 Commission Report, and Creation of the Privacy and Civil Liberties Oversight Board. On July 22, 2004, the "9/11 Commission" released its report on the terrorist attacks.[6] The Commission concluded (pp. 394-395) that many of the USA PATRIOT Act provisions appear beneficial, but that "Because of concerns regarding the shifting balance of power to the government, we think that a full and informed debate on the Patriot Act would be healthy." The Commission recommended that "The burden of proof for retaining a particular governmental power should be on the executive, to explain (a) that the power actually materially enhances security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties. If the power is granted, there must be adequate guidelines and oversight to properly confine its use." The Commission also called for creation of a board within the executive branch "to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties." The commissioners went on to say that "We must find ways of reconciling security with liberty, since the success of one helps protect the other. The choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend."

The 108th Congress passed legislation implementing many of the Commission's recommendations. Called the Intelligence Reform and Terrorism Prevention Act (S. 2845, P.L. 108-458), Sec. 1061 creates a Privacy and Civil Liberties Oversight Board. According to the bill's sponsor, Senator Collins, the Board's purpose is to "ensure that privacy and civil liberties concerns are appropriately considered in the implementation of all laws, regulations, and policies that are related to efforts to protect the Nation against terrorism."[7] It must report to Congress annually on an unclassified basis to the greatest extent possible. It will be composed of five members, two of which (the chairman and vice-chairman) must be confirmed by the

---

[5] [http://www.epic.org/alert/EPIC_Alert_9.23.html]. See entry under "[3] Homeland Security Bill Limits Open Government, and click on hyperlink to EPIC's February 26, 2002 letter to the House Judiciary Committee.

[6] National Commission on Terrorist Attacks Upon the United States. The 9/11 Commission Report. 585 p. [http://www.9-11commission.gov/report/911Report.pdf]

[7] Congressional Record, December 8, 2004, p. S11974.

Senate. All must come from outside the government to help ensure their independence.

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 websites 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.

By E-Mail Service Providers: The "Councilman Case"

In what is widely-regarded as a landmark ruling concerning Internet privacy, the U.S. Court of Appeals for the First Circuit in Massachusetts ruled (2-1) on June 29, 2004 that an e-mail service provider did not violate federal wiretapping statutes when it intercepted and read subscribers' e-mails to obtain a competitive business advantage. The ruling upheld the decision of a lower court to dismiss the case.

The case involved an e-mail service provider, Interloc, Inc., that sold out-of-print books. According to press accounts[8] and the text of the court's ruling,[9] Interloc used software code to intercept and copy e-mail messages sent to its subscribers (who were dealers looking for buyers of rare and out-of-print books) by competitor Amazon.com. The e-mail was intercepted and copied prior to its delivery to the recipient so that Interloc officials could read the e-mails and obtain a competitive advantage over Amazon.com. Interloc Vice President Bradford Councilman was charged with violating the Wiretap Act.[10] The court's majority opinion noted that the parties stipulated that, at all times that the Interloc software was performing operations on the e-mails, they existed in the random access memory or in hard drives within Interloc's computer system.

---

[8] (1) Jewell, Mark. Interception of E-Mail Raises Questions. Associated Press, June 30, 2004, 9:14 pm. (2) Zetter, Kim. E-Mail Snooping Ruled Permissible. Wired News, June 30, 2004, 08:40. (3) Krim, Jonathan. Court Limits Privacy of E-Mail Messages; Providers Free to Monitor Communications. Washington Post, July 1, 2004, E1 (via Factiva).

[9] U.S. v Bradford C. Councilman. U.S. Court of Appeals for the First Circuit. No. 03-1383. [http://www.ca1.uscourts.gov/pdf.opinions/03-1383-01A.pdf].

[10] The Wiretap Act,18 U.S.C. §§ 2510-2522, is Title I of the Electronic Communications Privacy Act (ECPA), P.L. 99-508. According to Jewell, op. cit., two other defendants — Alibris, which bought Interloc in 1998, and Interloc's systems administrator — pleaded guilty.

The case turned on the distinction between the e-mail being in transit, or in storage (and therefore governed by a different law[11]). The government argued that the e-mails were copied contemporaneously with their transmission, and therefore were intercepted under the meaning of the Wiretap Act. Judges Torruella and Cyr concluded, however, that they were in temporary storage in Interloc's computer system, and therefore were not subject to the provisions of the Wiretap Act. They further stated that "We believe that the language of the statute makes clear that Congress meant to give lesser protection to electronic communications than wire and oral communication. Moreover, at this juncture, much of the protection may have been eviscerated by the realities of modern technology.... However, it is not the province of this court to graft meaning onto the statute where Congress has spoken plainly." (p. 14-15). In his dissent, Judge Lipez stated, conversely, that he did not believe Congress intended for e-mail that is temporarily stored as part of the transmission process to have less privacy than messages as they are in transit. He agreed with the government's contention that an "intercept" occurs between the time the author hits the "send" button and the message arrives in the recipient's in-box. He concluded that "Councilman's approach to the Wiretap Act would undo decades of practice and precedent ... and would essentially render the act irrelevant .... Since I find it inconceivable that Congress could have intended such a result merely by omitting the term 'electronic storage' from its definition of 'electronic communication,' I respectfully dissent."[12]

Privacy advocates expressed deep concern about the ruling. Electronic Frontier Foundation (EFF) attorney Kevin Bankston stated that the court had "effectively given Internet communications providers free rein to invade the privacy of their users for any reason and at any time."[13] The five major ISPs (AOL, Earthlink, Microsoft, Comcast, and Yahoo) all reportedly have policies governing their terms of service that state that they do not read subscribers' e-mail or disclose personal information unless required to do so by law enforcement agencies.[14] The U.S. Department of Justice is appealing the court's decision, and several civil liberties filed a "friend of the court" brief in support of the government's appeal.[15] The U.S. Court of Appeals for the First Circuit agreed to rehear the case. Two bills were introduced in the 108th Congress that would have affected this debate by amending either the Wiretap Act (H.R. 4977) or the Stored Communications Act (H.R. 5059). There was no action on either bill.

---

[11] Stored communications are covered by the Stored Communications Act, which is Title II of ECPA, 18 U.S.C. §§ 2701-2711.

[12] U.S. v Bradford C. Councilman, p. 53.

[13] Online Privacy "Eviscerated" by First Circuit Decision. June 29, 2004. [http://www.eff.org/news/archives/2004_06.php#001658].

[14] Krim, op. cit.

[15] Singel, Ryan. Strange Bedfellows in E-Mail Case. Wired News, September 3, 2004, 02:00 PM. [http://www.wired.com/news/privacy/0,1848,64847,00.html]

Spyware

Spyware is discussed in more detail in CRS Report RL32706. The term "spyware" is not well defined. 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. Such software is called "adware." 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.

A central point of the debate is whether new laws are needed, or if industry self-regulation, coupled with enforcement actions under existing laws such as the Federal Trade Commission Act, is sufficient. The lack of a precise definition for spyware is cited as a fundamental problem in attempting to write new laws. FTC representatives and others caution that new legislation could have unintended consequences, barring current or future technologies that might, in fact, have beneficial uses. They further insist that, if legal action is necessary, existing laws provide sufficient authority. Consumer concern about control of their computers being taken over by spyware leads others to conclude that legislative action is needed.

Utah and California have passed spyware laws, but there is no specific federal law regarding spyware. In the 108th Congress, the House passed two bills (H.R. 2929 and H.R. 4661) and the Senate Commerce Committee reported S. 2145. There was no further action. In the 109th Congress, H.R. 29 (Bono) is very similar to H.R. 2929 as it passed the House in 2004. H.R. 29 was ordered reported from the House Energy and Commerce Committee on March 9, 2005.

Identity Theft (Including Phishing)

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 rate of identity theft over the past several years, 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.[16]

The extent to which the Internet is responsible for the increase in cases is debatable. Some attribute the rise instead to carelessness by businesses in handling

---

[16] See also CRS Report RL31919, *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*.

personally identifiable information, and by credit issuers that grant credit without proper checks. More traditional methods of acquiring someone's personal information — from lost or stolen wallets, or "dumpster diving" — also are used by identity thieves. Three high profile incidents that became public in 2005, where the security of consumer PII was compromised, reinforced existing fears about identity theft. The companies involved are ChoicePoint, Bank of America, and LexisNexis. These incidents are described in CRS Report RS22082.

Identity Theft Statistics

In a 2003 survey for the FTC, Synovate found that 51% of victims knew 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).[17]

Another survey, conducted by the Council of Better Business Bureaus and Javelin Strategy & Research, was released in January 2005.[18] The *2005 Identity Fraud Survey* is based on data collected in 2004 by Synovate using questions that closely mirrored those used in the 2003 FTC survey, plus several new questions. The survey found that computer crime accounted for 11.6% of identity theft cases in 2004, compared with 68% from paper sources. It further found that the average loss for online identity theft was $551 compared to $4,543 from paper sources. In cases where the perpetrator could be identified, family members were responsible for 32% of cases; complete strangers outside the workplace for 24%; friends, neighbors, and in-home employees for 18%; someone at a company with access to personal information for 13%; someone at the victim's workplace for 4%; or "someone else" for 8%. The study concluded that, contrary to popular perception, identity theft is *not* getting worse. For example, it reported that the number of victims declined from 10.1 million in 2003 to 9.3 million in 2004, and the annual dollar volume, adjusted for inflation, is "highly similar" ($52.6 billion) in the 2003 survey and this survey.

"Phishing"

One online method used to obtain PII is called "phishing." It refers to an Internet-based practice in which someone misrepresents their identity or authority in order to induce another person to provide PII. Some common phishing scams involve e-mails that purport to be from financial institutions or ISPs claiming that a person's record has been lost. The e-mail directs the person to a website that mimics

---

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

[18] An abbreviated "complimentary" version of the report is available at [http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html]. A Better Business Bureau press release is at [http://www.bbb.org/alerts/article.asp?ID=565]. The survey was sponsored Checkfree, Visa, and Wells Fargo & Company, but the report emphasizes that although those companies were invited to comment on the content of the questionnaire, they were not involved in the tabulation, analysis, or reporting of final results.

the legitimate business' website and asks the person to enter a credit card number and other PII so the record can be restored. In fact, the e-mail or website is controlled by a third party who is attempting to extract information that will be used in identity theft or other crimes. The FTC issued a consumer alert on phishing in June 2004.[19] An "Anti-Phishing Working Group" industry association has been established to collectively work on solutions to phishing [http://www.antiphishing.org/].

Existing Laws

The FTC enforces three federal laws that restrict disclosure of consumer information and require companies to ensure the security and integrity of the data in certain contexts — Section 5 of the Federal Trade Commission Act, the Fair Credit Reporting Act (FCRA), and Title V of the Gramm-Leach-Bliley Act. FTC Chairwoman Deborah Platt Majoras summarized these laws as they pertain to identity theft at a March 10, 2005 hearing before the Senate Committee on Banking, Housing, and Urban Affairs. [20] She identified two other laws that are not enforced by the FTC, but which also restrict the disclosure of certain types of information: the Driver's Privacy Protection Act, and the Health Insurance Portability and Accountability Act.

Congress also has passed laws specifically regarding identity theft: the 1998 Identity Theft and Assumption Deterrence Act; the 2003 Fair and Accurate Credit Transactions (FACT) Act; and the 2004 Identity Theft Penalty Enhancement Act. Those laws are summarized in CRS Report RL31919. Briefly, the Identity Theft and Assumption Deterrence Act (P.L.105-318) directed the FTC to establish a central repository for identity theft complaints, and provide victim assistance and consumer education.

The FACT Act (P.L. 108-159) contains perhaps the most comprehensive identity theft provisions in federal law. Implementation of that Act is discussed in CRS Report RL32535, *Implementation of the Fair and Accurate Credit Transactions (FACT) Act*. Among its identity theft-related provisions, the law —

- requires consumer reporting agencies (CRAs) 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 CRAs as long as the consumer requests it through a centralized source under rules to be established by the FTC;[21]

---

[19] FTC. How Not to Get Hooked by a 'Phishing" Scam. June 2004. [http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.pdf]

[20] Available at [http://banking.senate.gov/_files/majoras.pdf].

[21] The FTC rules on free credit reports were issued on June 4, 2004 and are available at [http://www.ftc.gov/opa/2004/06/freeannual.htm].

- allows consumers one free copy of their consumer report each year from nationwide specialty CRAs (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; [14]

- 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 CRAs 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; and

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

The Identity Theft Penalty Enhancement Act (P.L. 108-275) makes aggravated identity theft in conjunction with felonies a crime, and establishes mandatory sentences — 2 additional years beyond the penalty for the underlying crime, or 5 additional years for those who steal identities in conjunction with a terrorist act.[22]

At the March 10, 2005 Senate Banking Committee hearing,[23] FTC Chairwoman Majoras discussed the"complicated maze" of laws that governs consumer data, noting whether particular legal provisions apply depends on the type of company or institution involved, the type of data collected or sold, and the purpose for which it will be used. She conceded that it is not clear if data brokers like ChoicePoint come under the FTC's jurisdiction, and concluded that additional legislation may be necessary, particularly regarding notice and security. A witness from the Secret Service also testified about his agency's jurisdiction over identity theft crimes.

---

[22] Senate Clears Tougher Penalties for Identity Theft in Conjunction with Felony. CQ Weekly, June 26, 2004, p. 1561.

[23] The hearing can be viewed on the committee's Web site at: [http://banking.senate.gov/index.cfm?Fuseaction=Hearings.Detail&HearingID=142].

Congressional Action

Congress continues to consider ways to reduce the incidence of identity theft. Many bills are pending (see next section). Legislative approaches include strengthening penalties for identity theft or for the misuse of SSNs[24]; increasing regulation of data brokers, such as by requiring them to notify individuals whose PII has been breached, or to obtain a consumer's consent before selling PII; limiting the use of SSNs or allowing individuals to choose an identifier other than their SSN for Medicare purposes, for example; or making phishing unlawful.

The Senate Banking, Housing, and Urban Affairs Committee held hearings on identity theft on March 10 and March 15, 2005. The House Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection held a hearing on March 15, 2005.

Summary of 109th Congress Internet Privacy-Related Legislation

The following table provides summary information on pending Internet-related legislation . It should be noted that although some bills have similar titles or intents, the details may vary. For example, some bills seek to protect "personal information," while others protect "personally identifiable information" (PII). Definitions may vary, or, in some cases, the FTC is directed to determine the definition.

Table 1: Pending Legislation in the 109th Congress

Bill (Sponsor)	Summary, Committee(s) of Referral, and Status
INTERNET PRIVACY GENERAL	
H.R. 84 (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. 1263 (Stearns)	**Consumer Privacy Protection Act**. Broad consumer privacy bill including provisions related to identity theft, regulation of "data collection organizations," and a study of the impact on U.S. interstate and foreign commerce of privacy laws, etc., adopted by other countries. (Energy & Commerce, International Relations)

[24] For more on Social Security numbers, see CRS Report RL30318, The Social Security Number: Legal Developments Affecting Its Collection, Disclosure, and Confidentiality, by Kathleen S. Swendiman.

Bill (Sponsor)	Summary, Committee(s) of Referral, and Status
SPYWARE	
H.R. 29 (Bono)	**Spy Act**. Requires the FTC to prescribe 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; makes phishing unlawful. **Ordered reported from House Energy and Commerce Committee March 9, 2005**.
H.R. 744 (Goodlatte)	**Internet Spyware (I-SPY) Prevention Act**. Sets criminal penalties for certain spyware practices.(Judiciary)
IDENTITY THEFT/ PROTECTING SSNs AND OTHER PII	
H.R. 82 (Frelinghuysen)	**Social Security On-line Privacy Protection Act**. Regulates the use by interactive computer services of SSNs and related PII. (Energy and Commerce)
H.R. 92 (Frelinghuysen)	Permits Medicare beneficiaries to use an identification number other than their SSN in order to deter identity theft. (Ways and Means, Energy and Commerce)
H.R. 220 (Paul)	**Identity Theft Prevention Act**. Protects the integrity and confidentiality of SSNs, prohibits the establishment of a uniform national identifying number, and prohibits federal agencies from imposing standards of identification for individuals on other agencies or persons. (Ways & Means, Government Reform)
H.R. 1069 (Bean)	**Notification of Risk to Personal Data Act.** Requires federal agencies and others to disclose unauthorized acquisition of personal information in their possession, and requires consumer reporting agencies to implement fraud alerts under certain circumstances. (Energy & Commerce, Government Reform, Financial Services)
H.R. 1078 (Markey)	**Social Security Number Protection Act**. Regulates the sale and purchase of SSNs. (Energy & Commerce, Ways & Means)
H.R. 1080 (Markey)	**Information Protection and Security Act**. Regulates the conduct of information brokers and the protection of PII held by them. (Energy & Commerce)
H.R. 1099 (Hooley)	**Anti-Phishing Act**. Criminalizes phishing. (Judiciary)
S. 29 (Feinstein)	**Social Security Misuse Prevention Act**. Limits the misuse of SSNs and establishes criminal penalties for such misuse. Judiciary
S. 115 (Feinstein)	**Notification of Risk to Personal Data Act**. Requires federal agencies and persons engaged in interstate commerce to disclose any unauthorized access to electronic data containing personal information in their possession. (Judiciary)

Bill (Sponsor)	Summary, Committee(s) of Referral, and Status
S. 116 (Feinstein)	**Privacy Act of 2005.** Requires the consent of an individual prior to the sale and marketing of the individual's PII. (Judiciary)
S. 472 (Leahy)	**Anti-Phishing Act**. Criminalizes phishing. (Judiciary)
S. 500 (Bill Nelson)	**Information Protection and Security Act**. Regulates information brokers and protects individual rights to PII. (Commerce)

Prepared by CRS.
PII = Personally Identifiable Information
SSN = Social Security Number

Appendix A. Internet Privacy-Related Legislation Passed by the 108th Congress

H.R. 2622 (Bachus) **P.L. 108-159**	**Fair and Accurate Credit Transactions Act**. Includes several provisions related to identity theft, such as setting requirements on consumer reporting agencies and credit card issuers, requiring truncation of credit card numbers on electronically printed receipts, and extending the statute of limitations for when identity theft cases can be brought.
H.R. 1731 (Carter) **P.L. 108-275**	**Identity Theft Penalty Enhancement Act**. Makes aggravated identity theft in conjunction with felonies a crime, and establishes mandatory sentences.
H.R. 4818 (Kolbe) **P.L. 108-447**	**FY2005 Transportation, Treasury and General Government Appropriations Bill** (incorporated into the FY2005 Consolidated Appropriations Act). Sec. 633 continues prohibition on use of appropriated funds to collect personal information about visitors to federal websites.
S. 2845 (Collins) **P.L. 108-458**	**Intelligence Reform and Terrorism Protection Act**. Creates Privacy and Civil Liberties Oversight Board.

Appendix B. 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 websites.
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).