Order Code RL31408

Internet Privacy: Overview and Pending Legislation

Updated October 28, 2004

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. Congress and privacy advocates are monitoring how the act is implemented. The report of the 9/11 Commission called for a full and informed debate on the act. Legislation is pending regarding whether to add, or remove, "sunset" provisions under which certain sections of the act will expire on December 31, 2005.

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). Meanwhile, controversy is rising about how to protect computer users from spyware without creating unintended consequences. Spyware is not well defined, but generally includes software emplaced on a computer without the user's knowledge that takes control of the computer away from the user, such as by redirecting the computer to unintended websites, causing advertisements to appear, or collecting information and transmitting it to another person. The House passed two spyware bills (H.R. 2929 and H.R. 4661) in October 2004; a Senate bill (S. 2145) has been ordered reported from committee.

This report provides an overview of Internet privacy, tracks Internet privacy legislation pending before the 108th Congress, and describes the laws that were enacted in the 107th Congress. For information on wireless privacy issues, see CRS Report RL31636. 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. Thus, identity theft and phishing are briefly discussed in this report. More specific information on identity theft is available in CRS Report RL31919 and CRS Report RL32121. 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 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 pending legislation. More information on Internet privacy issues is available in CRS Report RL30784, *Internet Privacy: An Analysis of Technology and Policy Issues*, and CRS Report RL31289, *The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government*.

Internet: Commercial 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 website 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, p. 10, available at [http://commerce.senate.gov/hearings/index.cfm].

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

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

Privacy advocates are particularly concerned about online profiling, where companies collect data about what 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.

107th Congress Action

Many Internet privacy bills were considered by, but did not clear, the 107th Congress. H.R. 89, H.R. 237, H.R. 347, and S. 2201 dealt specifically with commercial website practices. H.R. 4678 was a broader consumer privacy protection bill. The Bankruptcy Reform bill (H.R. 333/S. 420) would have prohibited (with exceptions) companies, including website operators, that file for bankruptcy from selling or leasing PII obtained in accordance with a policy that said such information would not be transferred to third parties, if that policy was in effect at the time of the bankruptcy filing. H.R. 2135 would have limited the disclosure of personal information (defined as PII and sensitive personal information) by information recipients in general, and S. 1055 would have limited the commercial sale and marketing of PII. In a related measure, S. 2839 sought to protect the privacy of children using elementary or secondary school or library computers that use "Internet content management services," such as filtering software to restrict access to certain websites.

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

Legislation in the 108th Congress

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

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

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

(Explanation of Acronyms at End)

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

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

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

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

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 H.R. 5025/S. 2806, the Transportation, Treasury, and General Government Appropriations Bill.

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. According to a February 2004 Federal Computer Week article, agency implementation of that provision was proceeding slowly.[3]

Monitoring of E-mail and Web Usage

By Government and Law Enforcement Officials

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

---

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

subject of an investigation and similar usage by other people. Section 305 of the 21st Century Department of Justice Appropriations Authorization Act (P.L. 107-273) required the Justice Department to report to Congress at the end of FY2002 and FY2003 on its use of Carnivore/DCS 1000 or any similar system.

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:

- 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.[4] It lowers the threshold for when ISPs may voluntarily divulge the content of communications. Now ISPs need only a "good faith" (instead of a "reasonable") belief that there is an emergency involving danger (instead of "immediate" danger) of death or serious physical injury. The contents can be disclosed to "a Federal, state, or local governmental entity" (instead of a "law enforcement agency").

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 as it considered S. 1709.

Recommendations of the 9/11 Commission. 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."

---

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

[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]

Pending Legislation Regarding the 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 are pending that would affect the sunset clause. S.1695 (Leahy) would amend the sunset provision such that all of the sections cited above would expire, including Sections 210 and 216, which currently are not subject to the sunset clause. S. 1709 (Craig) would include Sec. 216 in the sunset clause. By contrast, S. 2476 (Kyl), would repeal Sec. 224 so that none of the provisions sunset. For more on the sunset clause, see CRS Report RL32186. The Senate Judiciary Committee held a hearing on S. 1709 on September 23, 2004.

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[7] and the text of the court's ruling,[8] 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

---

[7] (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).

[8] 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].

charged with violating the Wiretap Act.[9,10] 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.

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

---

[9] The Wiretap Act,18 U.S.C. §§ 2510-2522, is Title I of the Electronic Communications Privacy Act (ECPA), P.L. 99-508.

[10] According to Jewell, op. cit., two other defendants — Alibris, which bought Interloc in 1998, and Interloc's systems administrator — pleaded guilty.

[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.

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. H.R. 4977 (Nadler) would amend the definition of prohibited activities in the Wiretap Act to include "any temporary, intermediate storage of that communication incidental to the electronic transmission thereof."

Spyware

What is Spyware?

The term "spyware" is not well defined. Jerry Berman, President of the Center for Democracy and Technology (CDT), explained in testimony to the Senate Commerce Committee in March 2004 that "The term has been applied to software ranging from 'keystroke loggers' that capture every key typed on a particular computer; to advertising applications that track users' web browsing; to programs that hijack users' system settings."[16] He noted that what these various types of software programs "have in common is a lack of transparency and an absence of respect for users' ability to control their own computers and Internet connections." The FTC held a workshop on spyware on April 19, 2004.

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

As noted, spyware also can refer to "keylogging" software that records 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 key logging software has been available for some time, but its existence was highlighted in 2001 when the FBI, with a search warrant, installed the software on a suspect's computer, allowing them to obtain his password for an encryption program he used, and thereby evidence. Some privacy advocates argue wiretapping authority should have been obtained, but the judge, after reviewing classified information about how the software works, ruled in favor of the FBI. Press reports also indicate that the FBI is

---

[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]

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

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.

108th Congress Spyware Legislation

The House has passed two spyware bills — H.R. 2929 and H.R. 4661. The Senate Commerce Committee ordered reported S. 2145 (Burns) on September 22.

H.R. 2929 (Bono), SPY ACT. The Securely Protect Yourself Against Cyber Trespass Act passed the House (399-1), amended, on October 5, 2004. Different sections have various effective dates, but the legislation overall would expire on December 31, 2009. The version passed by the House reflected changes to the committee-reported version made by a manager's amendment. In the following description, ***text shown in bold italics was added or deleted by the manager's amendment***.

- Section 2 prohibits deceptive acts or practices relating to spyware. It would be unlawful for anyone who is not the owner or authorized user (hereafter, the user) of a protected computer to —

  - → take control of the computer by: utilizing the computer to send unsolicited information or material from the computer to others; diverting the computer's browser away from the site the user intended to view ***without authorization of the owner or authorized user of the computer, or otherwise authorized***; accessing or using the computer's Internet connection and thereby damaging the computer or causing the user to incur unauthorized financial charges; using the computer as part of an activity performed by a group of computers that causes damage to another computer; or delivering advertisements that a user cannot close without turning off the computer or closing all sessions of the Internet browser;
  - → modify settings related to use of the computer or the computer's access to the Internet by altering the Web page that appears when the browser is launched; the default provider used to access or search the Internet; the list of bookmarks; or security or other settings that protect information about the user ***for the purposes of causing damage or harm to the computer or its owner or user***;
  - → collect personally identifiable information through keylogging (***the phrase "or similar function" was deleted***);
  - → induce the user to install software, or prevent reasonable efforts to block the installation or execution of, or to disable, software, by presenting the user with an option to decline installation but the installation nevertheless proceeds, or causing software that has been properly removed or disabled to automatically reinstall or reactivate;
  - → misrepresent that certain actions or information is needed to open, view, or play a particular type of content;
  - → misrepresent the identity or authority of a person or entity providing software in order to induce the user to install or execute the software;

- → misrepresent the identity (***the words "or authority" were deleted***) of a person seeking information in order to induce the user to provide personally identifiable ***password or account*** information***, or without the authority of the intended recipient of the information***;
- → remove, disable, or render inoperative security, anti-spyware, or anti-virus technology installed on the computer;
- → install or execute on the computer one or more additional software components with the intent of causing a person to use such component in a way that violates any other provision of this section.

Effective on the date of enactment, the FTC is directed to provide guidance regarding compliance or violation of this section, while the effective date of the section is 6 months after enactment (in the committee-reported bill, this section would have become effective on the date of enactment).

- Section 3 prohibits the collection of certain information without notice and consent. It contains an opt-in requirement, whereby it would be unlawful —

  - → to transmit any information collection program without obtaining consent from the user ***unless notice is provided as required in this bill, and the program includes certain functions required in the bill***; or
  - → to execute any information collection functions installed on a computer, without obtaining consent from the user before the information collection program is executed (***the committee-reported bill stated that it was before "first" execution of the program, but "first" was deleted***).

"Information collection program" is defined as software that collects personally identifiable information and sends it to a person other than the user, or uses such information to deliver or display advertising; or collects information regarding Web pages accessed using the computer and uses such information to deliver or display advertising. The bill specifies certain requirements for notice (differentiating among various types of software at issue) and consent. ***The House-passed bill adds language about notice providing for the user to abandon or cancel the transmission or execution without granting or denying consent.***

Only one ***clear and conspicuous*** notice ***in plain language*** is required if multiple collection programs ***provided together or as a suite of functionally-related software*** execute (***instead of "first execute"***) any of the information collection functions. The user must be notified and consent obtained before the program is used to collect or send information of a (***instead of "any"***) type or for a (***instead of "any"***) purpose materially different from and outside the scope of what is stated in an initial or previous notice. ***No subsequent notification is otherwise required.*** Users must be able to disable or remove the information collection program without undue effort or knowledge. If an information collection program uses the collected information to display advertisements ***when the owner or user is accessing a Web page or online location other than that of the program's provider***, the program must include a function that identifies itself. (***The bill as passed includes more specific language about the methods by which that identification can be made***). Telecommunications carriers, information service or interactive computer service providers, cable operators, or providers of transmission capability are not liable under the act.

Section 3 would become effective one year after the law is enacted, and would not apply to information collection programs installed on a computer prior to that date.

- Section 4 directs the FTC to enforce the act, and the FTC is either directed or permitted to promulgate rules for various sections.

Civil penalties are set for various violations of the law or related regulations. Violations ***committed with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive or violates this Act*** shall be treated as an unfair or deceptive act or practice under the FTC Act. The FTC may seek a civil penalty (maximum of $3 million per violation) if a person engages in a pattern or practice of violations. Any single action or conduct that affects multiple computers is to be treated as a single violation, but a single action or conduct that violates multiple sections of the act is to be treated as multiple violations. This section becomes effective either on the date of enactment, or one year after enactment, depending on the section of the bill that is violated.

- Other sections include —

  → Exceptions for a variety of law enforcement/national security-related activities, and for network providers that use monitoring software to protect network security and prevent fraud.
  → ***Liability protection for manufacturers or retailers of computer equipment if they are providing third party-branded software that is installed on the equipment being manufactured or sold***.
  → Provisions under which the act supersedes state laws that expressly regulate deceptive conduct similar to that described in the act, or the transmission or execution of a computer program similar to that described in the act, or ***computer software that displays advertising content based on Web pages accessed using a computer*** (the last phrase replaces committee-passed wording that would have preempted state laws concerning the use of context-based triggering mechanisms or similar means to display advertisements). ***No person other than a state Attorney General may bring a civil action under any state law if that action is premised, in whole or in part, on violations of this bill, except that this bill does not limit the enforcement of any state consumer protection law.*** The bill would not preempt other state trespass, contract, or tort laws, or other state laws to the extent they relate to fraud. And,
  → Requirements for the FTC to submit an annual report about its actions based on the bill, and, separately***, a report on the use of "tracking cookies" to display advertisements and the extent to which they are covered by this bill***.

H.R. 4661 (Goodlatte), I-SPY Act. The Internet Spyware Prevention Act passed by the House on October 7, 2004 (415-0). The bill makes it illegal to access a computer without authorization to obtain sensitive personal information, or cause damage to the computer, and imposes fines and sentences up to 2 years in prison. If the unauthorized access is to further another federal crime, a sentence of up to 5 years is allowed. No person may bring a civil action under state law is such action is

premised in whole or in part upon a violation of this bill. The bill authorizes $10 million for each of four fiscal years (FY2005-FY2008) to the Department of Justice for prosecutions needed to discourage spyware and "phishing" (see Identity Theft section below for more on phishing). The version that passed the House added a provision that clarifies that the bill does not prohibit any lawfully authorized investigative, protective, or intelligence activities.

S. 2145 (Burns), SPY BLOCK Act. The Software Principles Yielding Better Levels of Consumer Knowledge Act, as introduced, requires notice to and consent of a user before anyone installs software on a user's computer (not including pre-installed software, and certain other exceptions). It also requires the user's affirmative consent to each information collection feature, advertising feature, distributed computing feature, and setting modification feature in the software. The software also must be able to be easily uninstalled. The bill was ordered reported, amended, from the Senate Commerce Committee on September 22, 2004. The amended version is not yet publicly available, but according to *CQ Weekly*, a Burns substitute amendment was adopted that "steered clear of setting technical requirements for software companies."[17] *CQ Weekly* added that an Allen amendment also was adopted that sets criminal penalties for spyware providers.

Arguments For and Against Legislation

The Senate Commerce Committee's Communications Subcommittee held a hearing on S. 2145 on March 23, 2004. Witnesses discussed the difficulties in legislating in an area where definitions are unclear, and the pace of technology might quickly render any such definitions obsolete. Mr. Robert Holleyman, representing the Business Software Alliance, testified that the focus of legislation should be regulating bad behavior, not technology. He expressed reservations about S. 2145, and called on Congress not to preclude the evolution of tools and marketplace solutions to the problem. Mr. John L. Levine, author of *The Internet for Dummies* and similar books, concluded that the legislation should ban spyware banned entirely, or consumers should be able to give a one-time permanent notice (akin to the telemarketing Do Not Call list) that they do not want spyware on their computers. He also said that the legislation should allow consumers to sue violators, rather than relying only on the FTC and state Attorneys General to enforce the law. Mr. Berman of CDT noted that three existing laws (including the FTC Act) can be used to address spyware concerns, and that technology measures, self-regulation and user education also are important to dealing with spyware. He concluded that CDT believes that new legislation specifically targeted at spyware would be useful, but that Congress also should pass broad Internet privacy legislation that could address the privacy aspects of the spyware debate.

While there is concern generally about any software product installed without the user's knowledge or consent, one particular area of controversy is programs that cause pop-up ads to appear. Many users object to pop-up ads as vigorously as they do to unsolicited commercial e-mail ("spam" — see CRS Report RL31953). The extent to which pop-up ads are, or should be, included in a definition of spyware was

---

[17] Senate Panel Approves 'Spyware' Bill. CQ Weekly, September 25, 2004, p. 2273.

discussed at the Senate Commerce Committee hearing. Mr Avi Naider, President and CEO of WhenU.com, argued that although his company's WhenU software does create pop-up ads, it is not spyware because users are notified that the program is about to be installed, must affirmatively consent to a license agreement, and may decline it. Mr. Naider explained that his program often is "bundled" with software that users obtain for free (called "free-ware"), or a software developer may offer users a choice between paying for the software or obtaining it for free if they agree to receive ads from WhenU. While agreeing that spyware is a serious concern, and that Congress and the FTC should regulate in this area, Mr. Naider urged that legislation be written carefully to exclude products like his that offer notice and choice and therefore should not be considered spyware. As noted below, WhenU has filed suit against a Utah law regulating spyware.

The House Energy and Commerce's Subcommittee on Telecommunications and the Internet held a hearing on April 29, 2004. At the hearing, FTC representatives argued that many of the actions under the rubric of "spyware" already are illegal, and additional legislation is not needed and could have unintended consequences because of the difficulty in defining spyware. A CDT witness again argued in favor of broad privacy legislation rather than focusing only on spyware. A representative from Earthlink supported legislation. A witness from Microsoft said that his company supports a "holistic" solution, but did not clearly state whether he supported new legislation or not.

Media sources reported prior to the House votes that the two House bills would be combined into a single package, but they were not. *Congressional Quarterly* explained that the two bills represent different philosophies about how to deal with the spyware issue: "Some want to crack down on the so-called bad actors who use spyware for nefarious purposes. Others propose requiring anybody installing the software to get a computer user's advance permission."[18] The first approach is that taken in H.R. 4661; the second is in H.R. 2929.

Skeptics contend that legislation is likely to be ineffective. One argument is that the "bad actors" are not likely to obey the opt-in requirement, but are difficult to locate and prosecute. Also, some are overseas and not subject to U.S. law. Another argument is that one member of a household (a child, for example) might unwittingly opt-in to spyware that others in the family would know to decline, or that users might not read through a lengthy licensing agreement to ascertain precisely what they are accepting.[19]

FTC Action

As noted, some argue that new legislation is unnecessary because existing law is adequate to prosecute spyware cases. In that vein, the FTC filed its first spyware case in October 2004, prior to enactment of new legislation. The action was taken in response to a complaint filed by the Center for Democracy and Technology (CDT).

---

[18] Sharma, Amol. Congressional "Spyware" Fix Likely to Prove Elusive. CQ Weekly, October 9, 2004, p. 2377.

[19] Ibid.

In an October 12, 2004 press release, the FTC explained that it was charging Sanford Wallace and two companies with which he is associated, Smartbot.Net and Seismic Entertainment Productions. Inc., with unfair and deceptive practices for using a variety of techniques to direct consumers to their Web sites where spyware was downloaded onto their computer without notice or consent. The FTC asserts that the spyware created serious problems on those computers, and the defendants thereupon offered to sell the consumers software for $30 to fix the problems. The FTC asked the U.S. District Court, District of New Hampshire, "to issue an order preventing the defendants from disseminating spyware and giving up their ill-gotten gains."[20] Mr. Wallace denies wrongdoing.[21] U.S. District Judge Joseph DiClerico issued a temporary restraining order against the defendants on October 21, 2004.[22]

Spyware Laws in Utah and California

On March 23, 2004, the Governor of Utah signed the first state anti-spyware law, which became effective on May 3, 2004.[23] The definition of spyware in that law includes certain pop-up ads. It prohibits, for example, some pop-up ads that partially or wholly cover or obscure paid advertising or other content on a website in a way that interferes with a user's ability to view the website. A media report stated that passage of the law was "driven by a Utah company in a legal fight with a pop-up company."[24] The Utah law also defines spyware, inter alia, as software installed on a computer without the user's consent and that cannot be easily disabled and removed. Several high-tech companies reportedly argued that the law could have unintended consequences, for example, prohibiting parents from installing software to block access by their children to certain Websites because the software monitors Web activities, may have been installed without the child's consent, and the child may not be able to uninstall it easily.[25]

WhenU filed suit against the Utah law on constitutional grounds, and Utah legislators reportedly are considering modifications to the law.[26] The Third Judicial

---

[20] FTC Cracks Down on Spyware Operation. FTC press release, October 12, 2004. [http://www.ftc.gov/opa/2004/10/spyware.htm].

[21] Wang, Beverly. New Hampshire Man Denies Wrongdoing in Federal Anti-Spam Case. Associated Press, October 8, 2004, 20:52 (via Factiva).

[22] Federal Judge Orders Immediate Halt to Spyware. Associated Press, October 23, 2004, 14:40 (via Factiva).

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

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

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

[26] Wallace, Brice. Deseret Morning News, April 22, 2004, E01 (via Factiva).

District Court in Salt Lake City, Utah granted a preliminary injunction on June 22, 2004, preventing the law from taking effect.[27]

California governor Schwarzenegger signed a spyware bill into law on September 28, 2004.[28] Inter alia, the bill prohibits a person or entity other than the authorized used of a computer — with actual knowledge, conscious avoidance of actual knowledge, or wilfully — to cause software to be downloaded onto a computer and using it to take control on the computer, as specified; modify certain settings; collect PII; prevent reasonable efforts to block the installation of or disable the software; intentionally misrepresent that the software will not be installed or will be disabled; or through intentionally deceptive means, remove, disable, or render inoperative certain other software programs on the computer (security, antispyware, or antivirus). A critic of the new law, Ben Edelman, a Harvard graduate student specializing in the spyware issue, called it "the most superfluous of all legislation."[29] On his Web site,[30] he comments that most of the actions prohibited by the California law already are illegal, and it does not address other issues — such as the length and presentation of software license agreements that may lead potential users to "accept" it without fully comprehending what the software will do.

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 rates of identity theft, where one individual assumes the identity of another using personal information such as credit card and Social Security numbers (SSNs). The FTC has a toll free number (877-ID-THEFT) to help victims.[31]

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 personally identifiable information, and by credit issuers that grant credit without proper checks. In a 2003 survey for the FTC, Synovate found that 51% of victims did not know how their personal information was obtained by the thief; 14% said their information was obtained from lost or stolen wallets, checkbooks, or credit cards;

---

[27] Judge Grants NY Pop-Up Company Preliminary Injunction Against Spyware Law. Associated Press, June 23, 2004, 06:06 (via Factiva).

[28] The enrolled version of the bill, California SB 1436, is available at: [http://www.leginfo.ca.gov/pub/bill/sen/sb_1401-1450/sb_1436_bill_20040826_enrolled.html]. This description of the bill is based on a summary provided on that Web site.

[29] Schwarzenegger Signs California Anti-Spyware Bill. Reuters, September 28, 2004, 21:59 (via Factiva).

[30] [http://www.benedelman.org/]

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

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).[32]

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

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

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

- allows consumers one free copy of their consumer report each year from nationwide consumer reporting agencies as long as the consumer requests it through a centralized source under rules to be established by the FTC;[33]

- allows consumers one free copy of their consumer report each year from nationwide specialty consumer reporting agencies (medical records or payments, residential or tenant history, check writing history, employment history, and insurance claims) upon request pursuant to regulations to be established by the FTC; [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 consumer reporting agencies to block the reporting of information in a consumer's file that resulted from identity theft and to notify the furnisher of the information in question that it may be the result of identity theft;

---

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

[33] 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].

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

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

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

Congress passed another identity theft bill, the Identity Theft Penalty Enhancement Act (H.R. 1731), in June 2004. President Bush signed it into law July 15, 2004 (P.L. 108-275). It 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.[34]

One 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 personally identifiable information (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 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.[35] An "Anti-Phishing Working Group" industry association has been established to collectively work on solutions to phishing. According to its website [http://www.antiphishing.org/], more than 407 companies are members. Congress also is addressing the issue. S. 2636 (Leahy), the Anti-Phishing Act, would make it a crime to create a website or domain name in order to misrepresent oneself as a legitimate online business without approval or authority of the registered owner of the actual website or domain name, and to induce, request, ask, or solicit anyone to provide any means of identification. In addition, H.R. 2929 (discussed above under **Spyware**) makes it a crime to misrepresent the identity of a person seeking information in order to induce the user to provide certain PII.

A number of other bills are pending in the 108th Congress regarding identity theft and protection of Social Security Numbers. They are summarized in Table 2.

---

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

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

Summary of Pending 108th Congress Legislation

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

Table 2: Pending Internet Privacy-Related Legislation

INTERNET PRIVACY (GENERAL)	
Bill/Status	**Summary/Committee(s) of Referral**
H.R. 69 Frelinghuysen	**Online Privacy Protection Act**. Requires the FTC to prescribe regulations to protect the privacy of personal information collected from and about individuals not covered by COPPA. (Energy & Commerce)
H.R. 1636 Stearns	**Consumer Privacy Protection Act.** See Table 1 for summary of provisions. (Energy & Commerce)
H.R. 4977 Nadler	**E-Mail Privacy Act.** Amends Wiretap Act to include in prohibited activities the temporary, intermediate storage of a communication incidental to the electronic transmission thereof. (Judiciary)
H.R. 5025 Istook **S. 2806** Shelby **Passed House; report from committee in Senate**	**FY2005 Transportation, Treasury and General Government Appropriations Bill.** Continues provision prohibiting use of funds to collect personal information about visitors to federal Web sites. **H.R. 5025 passed House Sept. 22, 2004; S. 2806 reported from Senate Appropriations Committee Sept. 15 (S.Rept. 108-342).**
S. 745 Feinstein	**Privacy Act.** Title I requires commercial entities to provide notice and choice (opt-out) to individuals regarding the collection and disclosure or sale of their PII, with exceptions. (Judiciary)
S. 1350 Feinstein	**Notification of Risk to Personal Data.** Requires federal agencies and persons engaged in interstate commerce, who possess electronic data containing personal information, to disclose any unauthorized acquisition of that data. (Judiciary)
S. 1695 Leahy	**PATRIOT Oversight Restoration Act.** *Inter alia*, would sunset Sections 210 and 216 of the USA PATRIOT Act on Dec. 31, 2005 (those sections are not subject to the sunset provisions now included in the act). (Judiciary)
S. 1709 Craig	**Security and Freedom Ensured (SAFE) Act**. *Inter alia* would sunset Section 216 of the USA PATRIOT Act on December 31, 2005. (Judiciary)
S. 2476 Kyl	[no title]. Would repeal section 224 of the USA PATRIOT Act, which sunsets certain provisions of that law. (Judiciary)

Bill/Status	Summary/Committee(s) of Referral
SPYWARE	
H.R. 2929 Bono **Passed House**	**Safeguard Against Privacy Invasions Act.** Requires the FTC to establish regulations prohibiting the transmission of spyware programs via the Internet to computers without the user's consent, and notification to the user that the program will be used to collect personally identifiable information (PII). **Reported from Energy & Commerce Committee July 20, 2004 (H.Rept. 108-619). Passed House October 5, 2004.**
H.R. 4255 Inslee	**Computer Software Privacy and Control Act.** To prevent deceptive software transmission practices. (Energy & Commerce; Judiciary)
H.R. 4661 Goodlatte **Passed House**	**I-SPY Prevention Act**. Sets criminal penalties for certain spyware practices. **Reported from House Judiciary Committee September 23 2004 (H.Rept. 108-698); passed House October 7. 2004.**
S. 2145 Burns	**SPY BLOCK** (Software Principles Yielding Better Levels of Consumer Knowledge). To regulate the authorized installation of computer software, and to require clear disclosure to computer users of certain computer software features that may pose a threat to user privacy. (Commerce) **Ordered reported September 22, 2004.**
IDENTITY THEFT/SOCIAL SECURITY NUMBER PROTECTION	
H.R. 70 Frelinghuysen	**Social Security On-Line Privacy Protection Act.** Regulates the use by interactive computer services of Social Security numbers (SSNs) and related personally identifiable information (PII). (Energy & Commerce)
H.R. 220 Paul	**Identity Theft Protection Act.** Protects the integrity and confidentiality of SSNs, prohibits establishment of a uniform national identifying number by federal government, and prohibits federal agencies from imposing standards for identification of individuals on other agencies or persons. (Ways & Means; Government Reform)
H.R. 637 Sweeney **S. 228** Feinstein	**Social Security Misuse Prevention Act**. Limits the display, sale, or purchase of SSNs. H.R. 637 referred to House Ways & Means Committee. S. 228 placed on Senate calendar. [The Senate bill was reintroduced from the 107th Congress, where it was reported from the Senate Judiciary Committee on May 16, 2002 — no written report. The bill number in that Congress was S. 848.]
H.R. 818 Kleczka	**Identity Theft Consumers Notification Act**. Requires financial institutions to notify consumers whose personal information has been compromised. (Financial Services)
H.R. 858 Tanner	**Identity Theft Penalty Enhancement Act**. Increases penalties for aggravated identity theft. (Judiciary)
H.R. 1729 Carson	**Negative Credit Information Act**. Requires consumer reporting agencies to notify consumers if information adverse to their interests is added to their files. (Financial Services)

Bill/Status	Summary/Committee(s) of Referral
H.R. 1931 Kleczka	**Personal Information Privacy Act.** Protects SSNs and other personal information through amendments to the Fair Credit Reporting Act. (Ways & Means, Financial Services)
H.R. 2035 Hooley	**Identity Theft and Financial Privacy Protection Act**. Requires credit card issuers to confirm change of address requests if received within 30 days of request for additional card; requires consumer reporting agencies to include a fraud alert in a consumer's file if the consumer has been, or suspects he or she is about to become, a victim of identity theft; requires truncation of credit and debit card numbers on receipts; requires FTC to set rules on complaint referral, investigations, and inquiries. (Financial Services)
H.R. 2617 Shadegg	**Consumer Identity and Information Security Act**. Prohibits the display of SSNs, with exceptions, and restricts the use of SSNs; prohibits the denial of products or services because an individual will not disclose his or her SSN; requires truncation of credit and debit card numbers on receipts; requires card issuers to verify a consumer's identity if a request for an additional credit card is made, or for a debit card or any codes or other means of access associated with it; requires FTC to set up a centralized reporting system for consumers to report suspected violations. (Financial Services, Ways & Means, Energy & Commerce)
H.R. 2633 Emmanuel	**Identity Theft Protection and Information Blackout Act**. Restricts the sale of SSNs and prohibits the display of SSNs by governmental agencies; prohibits the display, sale or purchase of SSNs in the private sector, with exceptions; and makes refusal to do business with anyone who will not provide an SSN an unfair or deceptive act or practice under the FTC Act, with exceptions. (Ways & Means, Energy & Commerce, Judiciary, Financial Services)
H.R. 2971 Shaw **S. 2801** Feinstein **Reported from House Ways & Means Committee**	**Social Security Number Privacy and Identity Theft Protection Act**. Restricts the sale of SSNs and prohibits the display of SSNs by governmental agencies; prohibits the display, sale or purchase of SSNs in the private sector, with exceptions; makes refusal to do business with anyone who will not provide an SSN an unfair or deceptive act or practice under the FTC Act; and requires certain methods of verification of identity when issuing or replacing SSNs and cards. S. 2801 referred to Senate Finance Committee. **H.R. 2971 reported from House Ways & Means Sept. 14, 2004 (H.Rept. 106-685, Part 1). Also referred to House committees on Financial Services, Energy & Commerce, and Judiciary.**
H.R. 3233 Gutierrez	**Identity Theft Notification and Credit Restoration Act.** Requires financial institutions and financial services providers to notify customers of the authorized use of personal information, amends the Fair Credit Reporting Act to require fraud alerts to be included in consumer credit files, and provides consumers with enhanced access to credit reports in such cases. (Financial Services)

Bill/Status	Summary/Committee(s) of Referral
H.R. 3693 Scott	**Identity Theft Investigation and Prosecution Act.** Provides additional resources to the Department of Justice for investigating and prosecuting identity theft and related credit card and other fraud. (Judiciary)
S. 153 Feinstein **Passed Senate**	**Identity Theft Penalty Enhancement Act**. Increases penalties for identity theft. (Judiciary) [This bill was reintroduced from the 107th Congress where it was reported by the Senate Judiciary Committee on November 14, 2002 — no written report. The bill number in that Congress was S. 2541.] **Passed Senate without amendment March 19, 2003.**
S. 223 Feinstein	**Identity Theft Prevention Act**. Requires credit card numbers to be truncated on receipts; imposes fines on credit issuers who issue new credit to identity thieves despite the presence of a fraud alert on the consumer's credit file; entitles each consumer to one free credit report per year from the national credit bureaus; and requires credit card companies to notify consumers when an additional credit card is requested on an existing credit account within 30 days of an address change request. (Banking)
S. 745 Feinstein	**Privacy Act.** Title II is the Social Security Misuse Prevention Act (S. 228, see above H.R. 637/S. 228 above).
S. 1533 Cantwell	**Identity Theft Victims Assistance Act**. Requires business entities with knowledge of an identity theft to share information with the victim or law enforcement agencies and requires consumer reporting agencies to block dissemination of information resulting from an identity theft, with exceptions. This bill is reintroduced from the 107th Congress where it was S 1742. (Judiciary)
S. 1581 Cantwell	**Identity Theft Victims Assistance Act.** Similar to S. 1533, but *inter alia* expressly states that the bill does not provide for private right of action, establishes an affirmative defense, and excludes consumer reporting agencies that are reselling information from some of the act's provisions under specified conditions. (Judiciary)
S. 1633 Corzine	**Identity Theft and Credit Restoration Act.** Requires financial institutions and financial service providers to notify customers of the unauthorized use of personal information, requires fraud alerts to be included in consumer credit files in such cases, and provides customers with enhanced access to credit reports in such cases. (Banking)
S. 1749 Specter	**Prevent Identity Theft From Affecting Lives and Livelihoods (PITFALL) Act**. Amends the Consumer Protection Act to provide relief for victims of identity theft. (Banking)
S. 2636 Leahy	**Anti-Phishing Act.** Makes phishing a crime. (Judiciary)

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. (See text for more details.)
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.

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).