

# CRS Report for Congress

Received through the CRS Web

## **Internet Privacy: Overview and Legislation in the 109<sup>th</sup> Congress, 1<sup>st</sup> Session**

**Updated January 26, 2006**

name redacted  
Specialist in Aerospace and Telecommunications Policy  
Resources, Science, and Industry Division

# Internet Privacy: Overview and Legislation in the 109<sup>th</sup> Congress, 1<sup>st</sup> Session

## Summary

Internet privacy issues encompass several 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. Another is the monitoring of electronic mail and Web usage by the government or law enforcement officials, employers, or email service providers.

The September 11, 2001 terrorist attacks intensified debate over the issue of monitoring by the government and law enforcement officials, with some advocating increased tools to help them 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 officials to monitor Internet activities. That act was 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. Some provisions of the USA PATRIOT Act, including two that relate to Internet use, would have expired on December 31, 2005. Congress passed a brief extension (to February 3, 2006) in P.L. 109-160. Debate over whether civil liberties protections need to be added if the provisions are to be made permanent is expected to continue in the second session of the 109<sup>th</sup> Congress. Revelations that President Bush directed the National Security Agency to monitor some communications, including e-mails, in the United States without warrants may affect those deliberations.

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 the only law that has been enacted (COPPA, P.L. 105-277) concerns the privacy of children under 13, not the general public. Legislation has passed regarding information practices for *federal government* websites, including 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 briefly in this report, but in more detail 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, Internet-based practices called "phishing" and "pharming" may contribute to identity theft. Identity theft is briefly discussed in this report; 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 is the final edition of this report. It provides an overview of Internet privacy issues and related laws passed in previous Congresses, and discusses legislative activity in the first session of the 109<sup>th</sup> Congress.

## Contents

Introduction .....	1
Internet: Commercial Website Practices .....	1
Children’s Online Privacy Protection Act (COPPA), P.L. 105-277 .....	2
FTC Activities and Fair Information Practices .....	3
Advocates of Self Regulation .....	3
Advocates of Legislation .....	4
Congressional Action .....	5
Internet: Federal Government Website Information Practices .....	5
Monitoring of E-mail and Web Usage .....	6
By Government and Law Enforcement Officials .....	6
The USA PATRIOT Act .....	7
The 9/11 Commission Report, and Creation of the Privacy and Civil Liberties Oversight Board .....	9
Government Access to Search Engine Data (e.g. Google) .....	10
By Employers .....	11
By E-Mail Service Providers: The “Councilman Case” .....	11
Spyware .....	13
Identity Theft (Including Phishing and Pharming) .....	14
Identity Theft Statistics .....	14
“Phishing” and “Pharming” .....	15
Existing Laws .....	16
Legislation in the 109 <sup>th</sup> Congress, 1 <sup>st</sup> Session .....	18
Summary of Internet Privacy-Related Legislation in the 109 <sup>th</sup> Congress, 1 <sup>st</sup> Session .....	19
Appendix A. Internet Privacy-Related Legislation Passed by the 108 <sup>th</sup> Congress .....	25
Appendix B. Internet Privacy-Related Legislation Passed by the 107 <sup>th</sup> Congress .....	25

## List of Tables

Table 1. Bills Introduced in the 109 <sup>th</sup> Congress, 1 <sup>st</sup> Session .....	19
--	----

# Internet Privacy: Overview and Legislation in the 109<sup>th</sup> Congress, 1<sup>st</sup> Session

## Introduction

Internet privacy issues encompass several 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. Another is the monitoring of electronic mail and Web usage by the government or law enforcement officials, employers, or e-mail service providers. 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, Internet-based practices called "phishing" and "pharming" may contribute to identity theft.

This report provides an overview of Internet privacy-related issues and related laws passed in previous Congresses, and discusses legislative activity in the first session of the 109<sup>th</sup> Congress. Background information on Internet privacy issues is available in an archived CRS Report RL30784, *Internet Privacy: An Analysis of Technology and Policy Issues*, by Marcia Smith (available from author); and CRS Report RL31289, *The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government*, by Marcia Smith, et al.

## 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 105<sup>th</sup> 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.<sup>1</sup> 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 Commission adopted a "sliding scale" for complying with the verifiable consent requirement depending on how the data would be used. That is, if the information was for internal use only, the verifiable consent could be obtained from the parent by e-mail, plus an additional step to ensure the person giving consent is, in fact, the parent. If the website operator planned to disclose the information publicly or to third parties, a higher standard was set. This sliding scale was set to expire in 2002 with the expectation that better verification technologies would become available. However, in 2002, the FTC determined that such technologies still were not available, and the sliding scale was extended to April 12, 2005. In 2005, the Commission extended it again, and is seeking public comment on how to proceed, as part of its overall review of the COPPA rule.<sup>2</sup>

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.<sup>3</sup>

As required by COPPA, on April 21, 2005, the Commission issued a request for public comment on its final rule, five years after the rule's effective date.<sup>4</sup> Comments were requested on the costs and benefits of the rule; whether it should be retained,

---

<sup>1</sup> COPPA should not be confused with COPA — the Child Online Protection Act — which addresses protecting children from unsuitable material, such as pornography, on the Internet. COPA is discussed in CRS Report RS21328, *Internet: Status of Legislative Attempts to Protect Children from Unsuitable Material on the Web*, by (name redacted).

<sup>2</sup> "FTC Seeks Public Comment on Children's Online Privacy Rule." FTC press release, April 21, 2005. See [<http://www.ftc.gov/opa/2005/04/coppacomments.htm>]. (Hereafter cited as *FTC Seeks Public Comment on Children's Online Privacy Rule*.)

<sup>3</sup> Prepared statement of Timothy Muris, Chairman, Federal Trade Commission, p. 10, available at [<http://commerce.senate.gov/hearings/witnesslist.cfm?id=807>].

<sup>4</sup> *FTC Seeks Public Comment on Children's Online Privacy Rule*.

eliminated, or modified; and its effect on practices relating to the collection of information relating to children, children's ability to access information of their choice online, and the availability of websites directed to children.

## **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 archived CRS Report RL30784, *Internet Privacy: An Analysis of Technology and Policy Issues*, by Marcia Smith (available from author), 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 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.”<sup>5</sup> 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 20<sup>th</sup> 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 21<sup>st</sup> century [sic] problem of Internet privacy.”<sup>6</sup>

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 have been 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.

---

<sup>5</sup> Clark, Drew. “Tech, Banking Firms Criticize Limitations of Privacy Standard.” *NationalJournal.com*, November 11, 2002.

<sup>6</sup> 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 the 107<sup>th</sup> and 108<sup>th</sup> Congresses. Other than extending an existing prohibition regarding federal websites (see next section), none cleared Congress. Several bills were introduced in the first session of the 109<sup>th</sup> Congress (see table at end of report).

### 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 FY2006, it is Section 832 of the Transportation-Treasury Appropriations Act (P.L. 109-115).

Nonetheless, in December 2005, the Associated Press (AP) reported that a privacy advocate, Daniel Brandt, had discovered that the National Security Agency (NSA) was using permanent cookies on its website.<sup>7</sup> The AP quoted an NSA spokesman as saying that it resulted from a recent software upgrade and the agency was not aware that permanent cookies were being set. C|NET News.Com reported a week later that, based on its own investigation, “dozens” of agencies were setting

---

<sup>7</sup> Jesdanun, Anick. NSA Inadvertently Uses Banned Data-Tracking “Cookies” At website. Associated Press, December 28, 2005, 15:35 (via Factiva).

permanent cookies or “web bugs.”<sup>8</sup> The article identified the White House, the Air Force, and the Treasury Department as examples, and reported that some of the agencies changed their practices after being contacted, and many seemed to have no idea that their software was setting cookies.

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,

---

<sup>8</sup> McCullagh, Declan. Government Web Sites Are Keeping an Eye On You. C|NET News.com, January 5, 2006. Available on the news.com.com website at [[http://news.com.com/Government+Web+sites+are+keeping+an+eye+on+you/2100-1028\\_3-6018702.html](http://news.com.com/Government+Web+sites+are+keeping+an+eye+on+you/2100-1028_3-6018702.html)]. Web bugs are very small (i.e., not visible) graphic images placed on HTML pages or in e-mails that allow third parties to track user behavior.

leading to their concerns. Section 305 of the 21<sup>st</sup> 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.<sup>9</sup> The reports indicate that the Justice Department no longer uses Carnivore/DCS 1000, using 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:

- 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 Cyber Security Enhancement 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

---

<sup>9</sup> See [[http://www.epic.org/privacy/carnivore/2002\\_report.pdf](http://www.epic.org/privacy/carnivore/2002_report.pdf)], and [[http://www.epic.org/privacy/carnivore/2003\\_report.pdf](http://www.epic.org/privacy/carnivore/2003_report.pdf)].

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. Sections 210 and 216 are excluded from the sunset. Sections 212 and 217 are not, and therefore will expire on December 31, 2005. As discussed below, Congress is considering legislation that would amend this sunset clause, making either more or fewer sections subject to it.

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”).

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.<sup>10</sup> A Senate Judiciary Committee hearing on September 23, 2004 explored some of these concerns.

Several House and Senate committees held hearings in the first session of the 109<sup>th</sup> Congress on various provisions of the USA PATRIOT Act, and more are expected in the second session, as Congress debates whether to extend the “sunset date,” or expiration date, of several provisions of that act. Under Section 224, a number of sections would have expired on December 31, 2005, including Section 212 and 217. Section 210 and Section 216 are not subject to the sunset clause (i.e., they are permanent).

Several bills were introduced to modify the sunset clause by making temporary provisions permanent, by making permanent provisions temporary, or by modifying reporting requirements or otherwise enhancing oversight of how the provisions are implemented. As December 31, 2005 approached, the issue became very contentious. The House passed a permanent extension (i.e., it repealed the sunset clause) in H.R. 3199. The Senate, however, passed only a six-month extension (S.

---

<sup>10</sup> [[http://www.epic.org/alert/EPIC\\_Alert\\_9.23.html](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.

2167) to allow time for further consideration of concerns by some Senators that more civil liberties protections are needed. The House did not agree with the Senate action, and amended S. 2167 so that the extension was only for five weeks (through February 3, 2006) to ensure that the Congress dealt with the issue early in the second session. Debate may be influenced by revelations in December 2005 that President George W. Bush directed the National Security Agency to monitor phone calls and e-mails in the United States without warrants. (For further information on the debate over warrantless searches, see the CRS general distribution memorandum at this CRS website: [<http://www.crs.gov/products/browse/documents/WD00002.pdf>].

**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.<sup>11</sup> 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 108<sup>th</sup> Congress passed legislation implementing many of the Commission’s recommendations. Called the Intelligence Reform and Terrorism Prevention Act (S. 2845, P.L. 108-458), Section 1061 creates a Privacy and Civil Liberties Oversight Board as part of the Executive Office of the President. 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.”<sup>12</sup> 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 Senate. All must come from outside the government to help ensure their independence.

*National Journal* reported on January 13, 2006 that although the five members of the Board have been appointed, the chairman and vice chairman have not yet been

---

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

<sup>12</sup> *Congressional Record*, December 8, 2004, p. S11974.

confirmed by the Senate.<sup>13</sup> An August 2005 *Reuters* report cited critics (including a former 9/11 Commissioner, Members of the House and Senate, and others) as concluding that the panel is a “toothless, underfunded shell with inadequate support” from the President.<sup>14</sup>

H.R. 1310 (Maloney) was introduced in the first session of the 109<sup>th</sup> Congress to make a number of changes, including establishing the Board as an independent agency in the executive branch, instead of part of the Executive Office of the President; setting out certain qualifications for Board members; and requiring that all of the Board members be confirmed by the Senate, not just the chairman and vice-chairman. There was no legislative action on the bill during the first session. As with debate over the USA PATRIOT Act, this discussion may be influenced by the controversy over warrantless searches (see above).

**Government Access to Search Engine Data (e.g. Google).** In January 2006, Internet search engine company Google indicated that it was resisting a Justice Department subpoena requiring the company to provide the government with data on searches made by users.<sup>15</sup> The Justice Department reportedly is seeking the data to help it in a court case to uphold the Child Online Protection Act (COPA), which was enacted to protect children using the Internet from objectionable material such as pornography.<sup>16</sup> According to various media reports, other search engine companies, including Yahoo!, MSN, and America Online, did comply with the government’s request. Although much of the publicity focused on the extent to which the privacy of Internet users would be undermined if the government could access such data, some observers pointed out that the data are anonymous, and Google’s response might be stimulated more by business concerns (e.g., revealing proprietary information) than privacy concerns.<sup>17</sup> Nevertheless, public response suggests that some consumers now worry about what search terms they use, lest the government track their activities and draw erroneous conclusions.<sup>18</sup>

---

<sup>13</sup> Friel, Brian. Civil Liberties Board Has Yet To Get Off the Ground. *National Journal*, January 13, 2006. Available on the govexec.com website at [[http://www.govexec.com/story\\_page.cfm?articleid=33176&dcn=todaysnews](http://www.govexec.com/story_page.cfm?articleid=33176&dcn=todaysnews)]

<sup>14</sup> Drees, Caroline. “U.S. Civil Liberties Board Struggles Into Existence.” *Reuters*, August 4, 2005, 12:33 (via Factiva).

<sup>15</sup> Delaney, Kevin. Google to Buck U.S. on Data Request — Firm Resists Agency’s Efforts to Obtain Scaled-Back List of Web Sites, Search Queries. *Wall Street Journal*, January 20, 2006, p. A3 (via Factiva).

<sup>16</sup> For a discussion of COPA, see CRS Report RS21328, *Internet: Status of Legislative Attempts to Protect Children from Unsuitable Material on the Web*, by (name redacted).

<sup>17</sup> Liptak, Adam. In Case About Google’s Secrets, Yours Are Safe. *New York Times*, January 26, 2006, p. 1 (via Factiva).

<sup>18</sup> Hafner, Katie. After Subpoenas, Internet Searches Give Some Pause. *New York Times*, January 25, 2006, p. 1 (via Factiva).

## 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 2005 survey of 526 companies by the American Management Association and the ePolicy Institute found that 76% monitor Web usage, and 55% retain and review e-mail messages.<sup>19</sup> The survey found that 26% of the companies had fired employees for misusing the Internet, and 25% had fired workers for e-mail misuse. Regarding notice, the survey reported that 80% of the companies inform workers that they are monitoring content, keystrokes, and time spent at the keyboard; 82% inform workers that computer files are stored and reviewed; 86% inform workers that e-mail is monitored; and 89% inform workers that Web usage is tracked. One criticism is that top level employees may not be subject to the same monitoring as rank and file workers.<sup>20</sup>

## 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<sup>21</sup> and the text of the court’s ruling,<sup>22</sup> 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.<sup>23</sup> The court’s majority

<sup>19</sup> American Management Association. “2005 Electronic Monitoring & Surveillance Survey.” Press Release, May 18, 2005. [<http://www.amanet.org/press/amanews/ems05.htm>].

<sup>20</sup> Sandberg, Jared. “Monitoring of Workers is Boss’s Right But Why Not Include Top Brass?,” Wall Street Journal, May 18, 2005, p. B1 (via Factiva).

<sup>21</sup> (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).

<sup>22</sup> *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>].

<sup>23</sup> 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 (continued...)

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<sup>24</sup>). 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."<sup>25</sup>

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."<sup>26</sup> 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.<sup>27</sup> The U.S. Department of Justice appealed the court's decision; and several civil liberties filed a "friend of the court" brief in support of the government's appeal. In August 2005, the First Circuit Court of Appeals overturned the lower court's decision 5-2.<sup>28</sup>

---

<sup>23</sup> (...continued)

guilty.

<sup>24</sup> Stored communications are covered by the Stored Communications Act, which is Title II of ECPA, 18 U.S.C. §§ 2701-2711.

<sup>25</sup> *U.S. v. Bradford C. Councilman*, p. 53.

<sup>26</sup> Online Privacy "Eviscerated" by First Circuit Decision. June 29, 2004. [[http://www.eff.org/news/archives/2004\\_06.php#001658](http://www.eff.org/news/archives/2004_06.php#001658)].

<sup>27</sup> Krim, op. cit.

<sup>28</sup> McCullagh, Declan. "E-mail Wiretap Case Can Proceed, Court Says." c|net News.com, (continued...)

Two bills were introduced in the 108<sup>th</sup> Congress that would have affected this debate by amending either the Wiretap Act or the Stored Communications Act. There was no action on either bill.

In the first session of the 109<sup>th</sup> Congress, H.R. 3503/S. 936 were introduced to amend the Wiretap Act to clarify that it applies “contemporaneous with transit, or on an ongoing basis during transit, through the use of any electronic, mechanical, or other device or process, notwithstanding that the communication may simultaneously be in electronic storage.” There was no action on the bills in 2005.

## Spyware

Spyware is discussed in more detail in CRS Report RL32706, *Spyware: Background and Policy Issues for Congress*, by Marcia Smith. 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 software 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,” and one aspect of the spyware debate is whether adware should be included in the definition of spyware. 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 108<sup>th</sup> 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.

Two bills passed the House in the first session of the 109<sup>th</sup> Congress : H.R. 29 (Bono) and H.R. 744 (Goodlatte). Two bills specific to spyware were introduced in the Senate: S. 687 (Burns-Wyden), and S. 1004 (Allen). A Senate Commerce

---

<sup>28</sup> (...continued)

August 11, 2005, 14:30:00 PDT.

Committee hearing on S. 687 was held on May 11, 2005. On November 17, 2005, the committee ordered reported S. 687, and defeated S. 1004, with committee Chairman Stevens reportedly saying that he hoped a compromise could be reached before the issue was debated on the floor.<sup>29</sup> Meanwhile, the FTC endorsed a different bill, S. 1608, at a hearing before a Senate Commerce subcommittee on October 5, 2005. That bill deals not only with spyware, but with other Internet-related fraud, including spam. Its focus is enhancing the FTC's ability to investigate and prosecute perpetrators who are located abroad or who use foreign intermediaries. For more information, see CRS Report RL32706, *Spyware: Background and Policy Issues for Congress*, by Marcia Smith.

## Identity Theft (Including Phishing and Pharming)

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.<sup>30</sup>

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. 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 early 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: The Internet Connection*, by Marcia Smith.

## 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

---

<sup>29</sup> Stables, Eleanor. Panel Approves Slew of Transportation, Spyware and Other Bills in Markup. CQ.com, November 17, 2005.

<sup>30</sup> 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*, both by Angie Welborn.

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).<sup>31</sup>

Another survey, conducted by the Council of Better Business Bureaus and Javelin Strategy & Research, was released in January 2005.<sup>32</sup> 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.

On January 25, 2006, the FTC released its most recent data about the top ten consumer fraud complaints.<sup>33</sup> Identity theft represented 37% of the 686,683 complaints filed with the FTC in 2005. Although the total number of ID theft complaints was higher than in the two previous years (255,565 in 2005 compared with 246,847 in 2004 and 215,177 in 2003), as a percentage of complaints filed with the FTC, the 2005 figure was less (37% in 2005 compared with 38% in 2004 and 40% in 2003). Credit card fraud was identified as the most common form of identity theft (26%), compared with phone or utilities fraud (18%), bank fraud (17%), employment fraud (12%), government documents/benefits fraud (9%), and loan fraud (5%).

## “Phishing” and “Pharming”

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 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

---

<sup>31</sup> Synovate. “Federal Trade Commission — Identity Theft Survey Report.” September 2003. pp. 30-31. [<http://www.ftc.gov/opa/2003/09/idtheft.htm>]

<sup>32</sup> 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.

<sup>33</sup> FTC. Consumer Fraud and Identity Theft Complaint Data: January - December 2005. [<http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf>].

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.<sup>34</sup> An “Anti-Phishing Working Group” industry association has been established to collectively work on solutions to phishing [<http://www.antiphishing.org/>].

A version of phishing, dubbed “pharming,” involves fraudulent use of domain names.<sup>35</sup> In pharming, hackers hijack a legitimate website’s domain name, and redirect traffic intended for that website to their own. The computer user sees the intended website’s address in the browser’s address line, but instead, he or she is connected to the hacker’s site and may unknowingly provide PII to the hacker.<sup>36</sup>

## 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.<sup>37</sup> 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, *Remedies Available to Victims of Identity Theft*, by Angie Welborn. 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*, by Angie Welborn. Among its identity theft-related provisions, the law:

---

<sup>34</sup> FTC. “How Not to Get Hooked by a ‘Phishing’ Scam.” June 2004. [<http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.pdf>].

<sup>35</sup> For more on domain names, and the DNS, see CRS Report 97-868, *Internet Domain Names: Background and Policy Issues*, by (name redacted).

<sup>36</sup> For more on pharming, see, for example, Delio, Michelle. “Pharming Out-Scams Phishing.” March 14, 2005 [<http://www.wired.com/news/infrastructure/0,1377,66853,00.html>].

<sup>37</sup> Available at [[http://banking.senate.gov/\\_files/majoras.pdf](http://banking.senate.gov/_files/majoras.pdf)].

- 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;<sup>38</sup>
- 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;
- 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 — two additional years beyond the penalty for the underlying crime, or five additional years for those who steal identities in conjunction with a terrorist act.<sup>39</sup>

---

<sup>38</sup> 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>].

<sup>39</sup> "Senate Clears Tougher Penalties for Identity Theft in Conjunction with Felony." *CQ Weekly*, June 26, 2004, p. 1561.

At the March 10, 2005 Senate Banking Committee hearing,<sup>40</sup> 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.

## Legislation in the 109<sup>th</sup> Congress, 1<sup>st</sup> Session

Congress continues to consider ways to reduce the incidence of identity theft. Legislative approaches include strengthening penalties for identity theft or for the misuse of SSNs;<sup>41</sup> 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.

Despite the widespread attention to these issues, and the introduction of many bills, no legislation to further address identity theft or to regulate data brokers passed during the first session of the 109<sup>th</sup> Congress. Four bills were acted upon in committee or subcommittee, however (H.R. 4127, S. 1326, S. 1408, and S. 1789). According to the *Wall Street Journal*, legislative action stalled because of differing views among the various stakeholders in the debate.

Consumer groups are pushing for credit protections that financial institutions oppose. Small banks are arguing with larger ones about who picks up the ‘reissuing costs’ when credit or debit cards must be replaced. And everyone with a stake in the issue is debating the ‘notification trigger,’ specifying what breaches require altering customers.<sup>42</sup>

The markup of H.R. 4127 (Stearns) by the House Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection was spirited, and the vote split on party lines.<sup>43</sup> The Senate Judiciary Committee reported S. 1326 (Sessions) without amendment and without written report on October 20, 2005. By contrast, the markup of S. 1789 (Specter) by the same committee on October 27,

---

<sup>40</sup> The hearing can be viewed on the committee’s website at [<http://banking.senate.gov/index.cfm?Fuseaction=Hearings.Detail&HearingID=142>].

<sup>41</sup> For more on Social Security numbers, see CRS Report RL30318, *The Social Security Number: Legal Developments Affecting Its Collection, Disclosure, and Confidentiality*, by (name redacted).

<sup>42</sup> Conkey, Christopher. Identity-Theft Bills Stall in Congress. *Wall Street Journal*, November 26, 2005, p. A4 (via Factiva).

<sup>43</sup> Krim, Jonathan. Parties Split on Data-Protection Bill. *Washington Post*, November 4, 2005, p. D 4 (via Factiva).

2005 involved considerable debate.<sup>44</sup> The Senate Commerce, Science, and Transportation Committee reported S. 1408 (Smith), amended, on December 8, 2005. See Table 1 for brief descriptions of the bills and associated report numbers.

For more on legislative action, see CRS Report RL31919, *Remedies Available to Victims of Identity Theft*, by Angie Welborn.

## Summary of Internet Privacy-Related Legislation in the 109<sup>th</sup> Congress, 1<sup>st</sup> Session

The following table provides summary information on Internet privacy-related legislation introduced in the first session of the 109<sup>th</sup> Congress. 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). Some concern “data,” while others concern “electronic data.” Definitions may vary, or, in some cases, the FTC is directed to determine a definition.

**Table 1. Bills Introduced in the 109<sup>th</sup> Congress, 1<sup>st</sup> Session**

Bill (Sponsor)	Summary, Committee(s) of Referral, and Status as of January 26, 2006
<b>Internet Privacy General</b>	
<b>H.R. 84</b> (Frelinghuysen)	<b>Online Privacy Protection Act.</b> Requires the FTC to prescribe regulations to protect the privacy of personal information collected from and about individuals not covered by COPPA. (Energy & Commerce)
<b>H.R. 1263</b> (Stearns)	<b>Consumer Privacy Protection Act.</b> 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)
<b>H.R. 1310</b> (Maloney)	<b>Protection of Civil Liberties Act.</b> <i>Inter alia</i> , makes the Privacy and Civil Liberties Oversight Board an independent agency, instead of part of the Executive Office of the President, and specifies certain qualifications for Board members and requires they be confirmed by the Senate. (Government Reform, Judiciary, Homeland Security, Intelligence)
<b>H.R. 1526</b> (Otter)	<b>Security and Freedom Ensured Act (SAFE Act).</b> <i>Inter alia</i> , makes Section 216 of the USA PATRIOT Act subject to the sunset date. (Judiciary, Intelligence)

<sup>44</sup> Ibid.

Bill (Sponsor)	Summary, Committee(s) of Referral, and Status as of January 26, 2006
<b>H.R. 3058</b> (Knollenberg)  <b>P.L. 109-115</b>	<b>FY2006 Transportation-Treasury Appropriations.</b> Continues language in previous appropriations bills prohibiting federal websites from collecting data about visitors to those websites. Section 933 in House version (passed House June 30, 2005); Section 831 in Senate version (passed Senate October 20, 2005). Sec. 832 in final version, <b>signed into law on November 30, 2005.</b>
<b>H.R. 3199</b> (Sensenbrenner)  <b>S. 1389</b> (Specter)	<b>USA Patriot and Terrorism Prevention Reauthorization Act.</b> <i>Inter alia</i> , House version repeals the sunset provision of USA PATRIOT Act, meaning that none of the sections would expire. Senate version, <i>inter alia</i> , enhances reporting requirements for Section 216. Reported from House Judiciary and Intelligence Committees (H.Rept. 109-174, Pt. I and Pt. II) 7/18/2005; passed House, amended, July 21, 2005. Passed Senate July 29 after substituting the language of S. 1389 as reported from Senate Judiciary Committee (no written report) and further amended. Conference report (H.Rept. 109-333) adopted House position re sunset clause. Passed House December 14, 2005. Senate did not pass conference report in the first session of the 109 <sup>th</sup> Congress. Instead, it passed S. 2167, extending the sunset date by six months, but the House modified that to five weeks (to February 3, 2006). See S. 2167.
<b>H.R. 3503</b> (Cannon)  <b>S. 936</b> (Leahy-Sununu)	<b>E-Mail Privacy Act.</b> Amends the Wiretap Act to clarify that it covers e-mail that is temporarily stored in transit (in response to the Councilman case). (House Judiciary; Senate Judiciary)
<b>S. 737</b> (Craig)	<b>Security and Freedom Ensured Act (SAFE Act).</b> <i>Inter alia</i> , sets additional requirements regarding use of authorities under Section 216 of the USA PATRIOT Act. (Judiciary)
<b>S. 2082</b> (Sununu)	To extend the sunset provisions of the USA PATRIOT Act and other purposes. Would extend the sunset provisions to March 31, 2006. (Judiciary)
<b>S. 2167</b> (Sununu)  <b>P.L. 109-160</b>	Extends the sunset date for certain provisions of the USA PATRIOT Act. <i>See also H.R. 3199.</i> The Senate passed S. 2167 on Dec. 21, 2005, extending the sunset date for six months. The House amended S. 2167 to extend the sunset date only for five weeks, to February 3, 2006, to ensure Congress would resume debate early in the second session. The Senate agreed with the House amendment on Dec. 22, 2005. <b>Signed into law December 30, 2005.</b>
<b>Spyware</b>	
<b>H.R. 29</b> (Bono)	<b>Spy Act.</b> 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. <b>Reported from House Energy and Commerce Committee (H.Rept. 109-32); passed House May 23, 2005.</b>

Bill (Sponsor)	Summary, Committee(s) of Referral, and Status as of January 26, 2006
<b>H.R. 744</b> (Goodlatte)	<b>Internet Spyware (I-SPY) Prevention Act.</b> Sets criminal penalties for certain spyware practices. <b>Reported from House Judiciary Committee (H.Rept. 109-93); passed House May 23, 2005.</b>
<b>S. 687</b> (Burns-Wyden)	<b>SPY BLOCK Act.</b> Broad anti-spyware bill. <b>Ordered reported from Senate Commerce Committee, November 17, 2005.</b>
<b>S. 1004</b> (Allen)	<b>Enhanced Consumer Protection Against Spyware Act.</b> To provide the FTC with the resources necessary to protect Internet users from spyware. (Commerce)
<b>S. 1608</b> (Smith)	<b>Undertaking Spam, Spyware, and Fraud Enforcement With Enforcers Beyond Borders (U.S. SAFE WEB) Act.</b> To enhance FTC enforcement against spyware and other Internet-related fraud (including spam), focusing on cross-border fraud and deception. <b>Ordered reported from Senate Commerce Committee December 15, 2005.</b>
<b>Identity theft/protecting SSNs and other PII</b>	
<b>H.R. 82</b> (Frelinghuysen)	<b>Social Security On-line Privacy Protection Act.</b> Regulates the use by interactive computer services of SSNs and related PII. (Energy and Commerce)
<b>H.R. 92</b> (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)
<b>H.R. 220</b> (Paul)	<b>Identity Theft Prevention Act.</b> 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)
<b>H.R. 1069</b> (Bean)	<b>Notification of Risk to Personal Data Act.*</b> Requires federal agencies, and persons engaged in interstate commerce, in possession of electronic data containing personal information, to disclose any unauthorized acquisition of such information; requires financial institutions to disclose to customers and consumer reporting agencies any unauthorized access to personal information; and requires consumer reporting agencies to implement fraud alerts under certain circumstances. (Energy & Commerce, Government Reform, Financial Services)
<b>H.R. 1078</b> (Markey)	<b>Social Security Number Protection Act.</b> Regulates the sale and purchase of SSNs. (Energy & Commerce, Ways & Means)
<b>H.R. 1080</b> (Markey)	<b>Information Protection and Security Act.</b> Regulates the conduct of information brokers and the protection of PII held by them. (Energy & Commerce)
<b>H.R. 1099</b> (Hooley)	<b>Anti-Phishing Act.</b> Criminalizes phishing. (Judiciary)

Bill (Sponsor)	Summary, Committee(s) of Referral, and Status as of January 26, 2006
<p><b>H.R. 1653</b> (Markey)</p> <p><b>S. 810</b> (Clinton)</p>	<p><b>Safeguarding Americans from Exporting Identification Data (SAFE-ID) Act.</b> Allows U.S. business entities to transmit PII of U.S. citizens to foreign affiliates or subcontractors in another country if that country has adequate privacy protections and the citizen has been given prior notice and not opted-out; and prohibits them from transmitting PII to foreign affiliates or subcontractors in a country without adequate privacy protections unless the U.S. citizen has opted-in. (House Energy &amp; Commerce; Senate Judiciary)</p>
<p><b>H.R. 1745</b> (Shaw)</p>	<p><b>Social Security Number and Identity Theft Prevention Act.</b> To enhance SSN protections, prevent fraudulent misuse of SSNs, and otherwise enhance protection against identity theft. (Ways &amp; Means)</p>
<p><b>H.R. 3140</b> (Bean)</p>	<p><b>Consumer Data Security and Notification Act.</b> To regulate information brokers, enhance information security requirements for consumer reporting agencies and information brokers, and require consumer reporting agencies, financial institutions, and other entities to notify consumers of data security breaches involving sensitive consumer information. (Financial Services)</p>
<p><b>H.R. 3374</b> (LaTourette)</p>	<p><b>Consumer Notification and Financial Data Protection Act.</b> To provide for the uniform and timely notification of consumers whose sensitive financial personal information has been placed at risk by a breach of data security, to enhance data security safeguards, and to provide appropriate consumer mitigation services. (Financial Services)</p>
<p><b>H.R. 3375</b> (Pryce)</p>	<p><b>Financial Data Security Act.</b> To amend the Fair Credit Reporting Act to provide for secure financial data. (Financial Services)</p>
<p><b>H.R. 3501</b> (Carson)</p>	<p><b>Consumer Access Rights Defense Act.</b> To require financial institutions and financial service providers to notify customers of the unauthorized use of personal financial information. (Energy &amp; Commerce, Government Reform, Financial Services)</p>
<p><b>H.R. 3804</b> (McCarthy)</p>	<p><b>Identity Theft Relief Act.</b> To allow a 100% deduction for expenses related to a “qualified identity theft” (as defined in the act) on federal tax returns. (Ways and Means)</p>
<p><b>H.R. 3997</b> (LaTourette)</p>	<p><b>Financial Data Protection Act.</b> To amend the Fair Credit Reporting Act to provide for secure financial data. (Financial Services)</p>
<p><b>H.R. 4127</b> (Stearns)</p>	<p><b>Data Accountability and Trust Act (DATA).</b> Requires reasonable security policies and procedures to protect computerized data containing personal information and provide for nationwide notice of security breaches. (Energy and Commerce) <b>Subcommittee markup November 3, 2005.</b></p>

Bill (Sponsor)	Summary, Committee(s) of Referral, and Status as of January 26, 2006
<b>H.R. 4244</b> (Hooley)	<b>Regional ID Theft Task Force Act.</b> Provides grants for regional task forces to more effectively investigate and prosecute identity theft and other economic crimes. (Judiciary)
<b>S. 29</b> (Feinstein)	<b>Social Security Misuse Prevention Act.</b> Limits the misuse of SSNs and establishes criminal penalties for such misuse. (Judiciary)
<b>S. 115</b> (Feinstein)	<b>Notification of Risk to Personal Data Act.*</b> Requires federal agencies, and persons engaged in interstate commerce, in possession of electronic data containing personal information, to disclose any unauthorized acquisition of such information. (Judiciary)
<b>S. 116</b> (Feinstein)	<b>Privacy Act of 2005.</b> Requires the consent of an individual prior to the sale and marketing of the individual's PII. (Judiciary)
<b>S. 472</b> (Leahy)	<b>Anti-Phishing Act.</b> Criminalizes phishing. (Judiciary)
<b>S. 500</b> (Bill Nelson)	<b>Information Protection and Security Act.</b> Regulates information brokers and protects individual rights to PII. (Commerce)
<b>S. 751</b> (Feinstein)	<b>Notification of Risk to Personal Data Act.*</b> Requires federal agencies, and persons engaged in interstate commerce, in possession of data containing personal information to disclose any unauthorized acquisition of such information. (Commerce)
<b>S. 768</b> (Schumer)	<b>Comprehensive Identity Theft Prevention Act.</b> Broad identity theft prevention bill, including protecting SSNs, assistance to victims, coordinating international action against identity theft, notification of information breaches, and establishing an Office of Identity Theft at the FTC. (Commerce)
<b>S. 1326</b> (Sessions)	<b>Notification of Risk to Personal Data Act.</b> Requires federal agencies and persons in possession of computerized data containing sensitive personal information to disclose security breaches if it poses a significant risk of identity theft. <b>Reported from Senate Judiciary Committee without amendment and without written report October 20, 2005.</b>
<b>S. 1332</b> (Specter)	<b>Personal Data Privacy and Security Act.</b> To prevent and mitigate identity theft, to ensure privacy, and to enhance criminal penalties and other protections against security breaches, fraudulent access and misuse of PII. <b>Read the second time and placed on the legislative calendar July 1.</b>
<b>S. 1336</b> (Pryor)	<b>Consumer Identity Protection and Security Act.</b> To establish procedures for the protection of consumers from misuse or unauthorized access to sensitive personal information contained in private information files maintained by commercial entities engaged in or affecting interstate commerce and provide for their enforcement by the FTC. (Commerce)

Bill (Sponsor)	Summary, Committee(s) of Referral, and Status as of January 26, 2006
<b>S. 1408</b> (Smith)	<b>Identity Theft Protection Act.</b> Strengthens data protection and safeguards, requires notification of data breaches, and further prevents identity theft. <b>Reported from Senate Commerce Committee December 8, 2005 (S.Rept. 109-203).</b>
<b>S. 1461</b> (Shelby)	<b>Consumer Identity Protection and Security Act.</b> To protect consumers from misuse of, and unauthorized access to, sensitive personal information contained in private information files maintained by commercial entities engaged in, or affecting, interstate commerce, and provide for enforcement of those procedures by the FTC. (Banking)
<b>S. 1594</b> (Corzine)	<b>Financial Privacy Protection Act.</b> To require financial services providers to maintain customer information security systems and to notify customers of unauthorized access to personal information. (Banking)
<b>S. 1789</b> (Specter)	<b>Personal Data Privacy and Security Act.</b> To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of PII. <b>Reported from Senate Judiciary Committee without written report November 17, 2005.</b>

**Source:** Prepared by CRS.

**Note:** PII = Personally Identifiable Information; SSN = Social Security Number.

\* Although H.R. 1069, S. 115, and S. 751 have the same title, each is different.

## Appendix A. Internet Privacy-Related Legislation Passed by the 108<sup>th</sup> Congress

<p><b>H.R. 2622</b> (Bachus)</p> <p><b>P.L. 108-159</b></p>	<p><b>Fair and Accurate Credit Transactions Act.</b> 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.</p>
<p><b>H.R. 1731</b> (Carter)</p> <p><b>P.L. 108-275</b></p>	<p><b>Identity Theft Penalty Enhancement Act.</b> Makes aggravated identity theft in conjunction with felonies a crime, and establishes mandatory sentences.</p>
<p><b>H.R. 4818</b> (Kolbe)</p> <p><b>P.L. 108-447</b></p>	<p><b>FY2005 Transportation, Treasury and General Government Appropriations Bill</b> (incorporated into the FY2005 Consolidated Appropriations Act). Section 633 continues prohibition on use of appropriated funds to collect personal information about visitors to federal websites.</p>
<p><b>S. 2845</b> (Collins)</p> <p><b>P.L. 108-458</b></p>	<p><b>Intelligence Reform and Terrorism Protection Act.</b> Creates Privacy and Civil Liberties Oversight Board.</p>

## Appendix B. Internet Privacy-Related Legislation Passed by the 107<sup>th</sup> Congress

<p><b>H.R. 2458</b> (Turner)/ <b>S. 803</b> (Lieberman)</p> <p><b>P.L. 107-347</b></p>	<p><b>E-Government Act.</b> <i>Inter alia</i>, 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.</p>
<p><b>H.R. 5505</b> (Armey)</p> <p><b>P.L. 107-296</b></p>	<p><b>Homeland Security Act.</b> Incorporates <b>H.R. 3482, Cyber Security Enhancement Act</b>, as Section 225. Loosens restrictions on ISPs, set in the USA PATRIOT Act, as to when, and to whom, they can voluntarily release information about subscribers.</p>
<p><b>H.R. 2215</b> (Sensenbrenner)</p> <p><b>P.L. 107-273</b></p>	<p><b>21<sup>st</sup> Century Department of Justice Authorization Act.</b> Requires the Justice Department to notify Congress about its use of Carnivore (DCS 1000) or similar Internet monitoring systems.</p>
<p><b>H.R. 3162</b> (Sensenbrenner)</p> <p><b>P.L. 107-56</b></p>	<p><b>USA PATRIOT Act.</b> 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).</p>

# EveryCRSReport.com

The Congressional Research Service (CRS) is a federal legislative branch agency, housed inside the Library of Congress, charged with providing the United States Congress non-partisan advice on issues that may come before Congress.

EveryCRSReport.com republishes CRS reports that are available to all Congressional staff. The reports are not classified, and Members of Congress routinely make individual reports available to the public.

Prior to our republication, we redacted names, phone numbers and email addresses of analysts who produced the reports. We also added this page to the report. We have not intentionally made any other changes to any report published on EveryCRSReport.com.

CRS reports, as a work of the United States government, are not subject to copyright protection in the United States. Any CRS report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS report may include copyrighted images or material from a third party, you may need to obtain permission of the copyright holder if you wish to copy or otherwise use copyrighted material.

Information in a CRS report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to members of Congress in connection with CRS' institutional role.

EveryCRSReport.com is not a government website and is not affiliated with CRS. We do not claim copyright on any CRS report we have republished.