Order Code RL32706

CRS Report for Congress
Received through the CRS Web

Spyware: Background and Policy Issues for Congress

Updated July 17, 2006

Patricia Moloney Figliola
Specialist in Telecommunications and Internet Policy
Resources, Science, and Industry Division

Spyware: Background and Policy Issues for Congress

Summary

The term "spyware" is not well defined. Generally it is used to refer to any software that is downloaded onto a person's computer without their knowledge. Spyware may collect information about a computer user's activities and transmit that information to someone else. It may change computer settings, or cause "pop-up" advertisements to appear (in that context, it is called "adware"). Spyware may redirect a Web browser to a site different from what the user intended to visit, or change the user's home page. A type of spyware called "keylogging" software records individual keystrokes, even if the author modifies or deletes what was written, or if the characters do not appear on the monitor. Thus, passwords, credit card numbers, and other personally identifiable information may be captured and relayed to unauthorized recipients.

Some of these software programs have legitimate applications the computer user wants. They obtain the moniker "spyware" when they are installed surreptitiously, or perform additional functions of which the user is unaware. Users typically do not realize that spyware is on their computer. They may have unknowingly downloaded it from the Internet by clicking within a website, or it might have been included in an attachment to an electronic mail message (e-mail) or embedded in other software.

According to an October 2004 survey and tests conducted by America Online and the National Cyber Security Alliance, 80% of computers in the test group were infected by spyware or adware, and 89% of the users of those computers were unaware of it. The Federal Trade Commission (FTC) issued a consumer alert on spyware in October 2004. It provided a list of warning signs that might indicate that a computer is infected with spyware, and advice on what to do if it is.

Several states have passed spyware laws, but there is no specific federal law. During the first session of the 109th Congress, the House passed two different spyware bills, H.R. 29 and H.R. 744, on May 23, 2005. In the Senate, three bills were introduced: S. 687, S. 1004, and S. 1608. S. 687 and S. 1608 were ordered reported from the Senate Commerce Committee during 2005.

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 that could lead to unintended consequences. Opponents of new legislation 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, and resulting impacts on their privacy, leads others to conclude that more legislation is needed. The FTC supports S. 1608, which would enhance FTC enforcement against spyware, focusing on cross-border fraud.

Note: This report was originally written by Marcia S. Smith; the author acknowledges her contribution to CRS coverage of this issue area.

Contents

Spyware: Background and Policy Issues for Congress

Background

Congress is debating whether to enact new legislation to deal with the growing problem of "spyware." Spyware is not well defined, but generally includes software placed 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 "pop-up" advertisements to appear, or collecting information and transmitting it to another person. The lack of a firm definition of the term adds to the complexities of drafting new laws.

Opponents of new legislation argue that industry self-regulation and enforcement of existing laws are sufficient. They worry that further legislation could have unintended consequences that, for example, limit the development of new technologies that could have beneficial uses. Supporters of new legislation believe that current laws are inadequate, as evidenced by the growth in spyware incidents.

In the first session of the 109th Congress, debate resumed, and the House again passed two bills (similar to the two passed in the 108th Congress): H.R. 29 and H.R. 744.[1] In the Senate, three bills were introduced: S. 687, S. 1004, and S. 1608. S. 687 and S. 1608 were ordered reported from the Senate Commerce Committee during 2005. Legislative action during the 109th Congress on these bills is discussed later in this report.

A June 2006 report on spyware enforcement by the Center for Democracy and Technology (CDT) summarizes active and resolved spyware cases at the FTC and the Department of Justice, and in individual states.[2]

What is Spyware?

The term "spyware" is not well defined. Jerry Berman, President of CDT, explained in testimony to the Subcommittee on Communications of the Senate Commerce, Science, and Transportation Committee in March 2004 that "The term

---

[1] The 108th Congress debated spyware legislation, and two bills passed the House, but neither cleared Congress. A summary of legislative action in the 108th Congress is included at the end of this report in the Appendix.

[2] "Spyware Enforcement," CDT, June 2006, available online at [http://www.cdt.org/privacy/spyware/20060626spyware-enforcement.pdf].

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."[3] 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." More recently, in June 2006, the Anti-Spyware Coalition (ASC)[4] issued a paper that defined spyware as "technologies deployed without appropriate user consent and/or implemented in ways that impair user control over:

- Material changes that affect their user experience, privacy, or system security;
- Use of their system resources, including what programs are installed on their computers; and/or
- Collection, use, and distribution of their personal or other sensitive information."[5]

Software programs that include spyware may be sold or available for free ("freeware"). They may be on a disk or other media, downloaded from the Internet, or downloaded when opening an attachment to an electronic mail (e-mail) message. Typically, users have no knowledge that spyware is on their computers. Because the spyware is resident on the computer's hard drive, it can generate pop-up ads, for example, even when the computer is not connected to the Internet.

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, such as Web browsing habits. Some of these products may collect personally identifiable information (PII). When the computer is connected to the Internet, the software periodically relays the information back to another party, such as the software manufacturer or a marketing company. Another oft-cited example of spyware is "**adware**," which may cause advertisements to suddenly appear on the user's monitor — called "pop-up" ads. In some cases, the adware uses information that the software obtained by tracking a user's Web browsing habits to determine shopping preferences, for example. Some adware

---

[3] 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.

[4] The ASC is dedicated to building a consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies. Composed of anti-spyware software companies, academics, and consumer groups, the ASC seeks to bring together a diverse array of perspective on the problem of controlling spyware and other potentially unwanted technologies. It's members include AOL, Cyber Security Industry Alliance, McAfee, Microsoft, SurfControl, US Coalition Against Unsolicited Commercial Email, and Yahoo. A complete list of the group's members is available online at [http://www.antispywarecoalition.org/about/index.htm].

[5] Anti-Spyware Coalition Definitions Document, June 2006, available online at [http://www.antispywarecoalition.org/documents/DefinitionsJune292006.htm].

companies, however, insist that adware is not necessarily spyware, because the user may have permitted it to be downloaded onto the computer because it provides desirable benefits.

As Mr. Berman explained, 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.[6] In the context of the spyware debate, the concern is that such software can record credit card numbers and other personally identifiable information that consumers type when using Internet-based shopping and financial services, and transmit that information to someone else. Thus it could contribute to identity theft.[7]

Spyware remains difficult to define, however, in spite of the work done by groups such as the ASC and government agencies such as the Federal Trade Commission (FTC).[8] As discussed below, this lack of agreement is often cited by opponents of legislation as a reason not to legislate. Opponents of anti-spyware legislation argue that without a widely agreed-upon definition, legislation could have unintended consequences, banning current or future technologies and activities that, in fact, could be beneficial. Some of these software applications, including adware and keylogging software, do, in fact, have legitimate uses. The question is whether the user has given consent for it to be installed.

Prevalence of Spyware

In October 2004, America Online (AOL) and the National Cyber Security Alliance (NCSA)[9] released the results of a survey of 329 dial-up and broadband

---

[6] The existence of keylogging software was publicly highlighted in 2001 when the FBI, with a search warrant, installed such software on a suspect's computer, allowing them to obtain his password for an encryption program he used, and thereby evidence. Some privacy advocates argued that wiretapping authority should have been obtained, but the judge, after reviewing classified information about how the software works, ruled in favor of the FBI. Press reports also indicate that the FBI is developing a "Magic Lantern" program that performs a similar task, but can be installed on a subject's computer remotely by surreptitiously including it in an e-mail message, for example.

[7] For more on identity theft, see CRS Report RS22082, Identity Theft: The Internet Connection, by Marcia S. Smith; and CRS Report RL31919, Remedies Available to Victims of Identity Theft, by Angie A. Welborn.

[8] The FTC has a spyware information page on its website, [http://www.ftc.gov/spyware]. Further, a report from the FTC's April 2004 workshop on spyware is available online at [http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf]. This report contains a discussion on the difficulties of defining spyware.

[9] According to its website [http://www.staysafeonline.org], NCSA is a public-private partnership, with government sponsors including the Department of Homeland Security and the FTC. Its Board of Officers includes representatives from Cisco Systems, Symantec, RSA Security, AOL, McAfee, Microsoft, and BellSouth.

computer users regarding online threats, including spyware.[10] According to the study:

- 80% of the computers they tested were infected with spyware or adware, and 89% of the users of those computers were unaware of it;
- the average infected computer had 93 spyware/adware components on it, and the most found on a single computer was 1,059; and
- most users do not recognize the symptoms of spyware — 63% of users with a pop-up blocker said they got pop-up ads anyway, 43% of users said their home page had been changed without their permission, and 40% said their search results are being redirected or changed.

Separately, Webroot Software, a provider of privacy and protection software, released the results of a survey of 287 corporate information technology managers on October 27, 2004. That survey concluded that although more than 70% of corporations expressed increased concern about spyware, less than 10% had implemented commercially available anti-spyware software.[11]

FTC Advice to Consumers

The Federal Trade Commission (FTC) issued a consumer alert about spyware in October 2004 offering a list of warning signs that might indicate that a computer is infected with spyware.[12] The FTC alert listed the following clues:

- a barrage of pop-up ads;
- a hijacked browser — that is, a browser that takes you to sites other than those you type into the address box;
- a sudden or repeated change in your computer's Internet home page;
- new and unexpected toolbars;
- new and unexpected icons on the system tray at the bottom of your computer screen;
- keys that don't work (for example, the "Tab" key that might not work when you try to move to the next field in a Web form);
- random error messages; and
- sluggish or downright slow performance when opening programs or saving files.

The FTC alert also offered preventive actions consumers can take.

---

[10] Largest In-Home Study of Home Computer Users Shows Major Online Threats, Perception Gap. Business Wire, October 25, 2004, 08:02 (via Factiva). The study is available on NCSA's website at [http://www.staysafeonline.info/news/safety_study_v04.pdf].

[11] Spyware Infiltration Rises in Corporate Networks, but Webroot Survey Finds Companies Still Neglect Threat. PR Newswire, October 27, 2004, 06:00 (via Factiva).

[12] Available at [http://www.ftc.gov/bcp/conline/pubs/alerts/spywarealrt.htm].

- update your operating system and Web browser software;
- download free software only from sites you know and trust;
- don't install any software without knowing exactly what it is;
- minimize "drive-by" downloads by ensuring that your browser's security setting is high enough to detect unauthorized downloads;
- don't click on any links within pop-up windows;
- don't click on links in spam that claim to offer anti-spyware software; and
- install a personal firewall to stop uninvited users from accessing your computer.

Finally, the FTC alert advised consumers who think their computers are infected to get an anti-spyware program from a vendor they know and trust; set it to scan on a regular basis, at startup and at least once a week; and delete any software programs detected by the anti-spyware program that the consumer does not want.

Reviews of some of the commercially available anti-spyware programs are available in magazines such as PC World and Consumer Reports, or at [http://www.spywarewarrior.com].[13] Consumers must be cautious about choosing a spyware product, however. At a May 11, 2005 Senate Commerce, Science, and Transportation Committee hearing, the point was raised that some websites masquerade as anti-spyware sites selling spyware solutions, but instead download spyware onto an unwitting consumer's computer.

Other FTC Activities

The FTC held a workshop on spyware on April 19, 2004.[14] The director of FTC's Bureau of Consumer Protection, Howard Beale, summarized the workshop at a hearing before the Subcommittee on Telecommunications and the Internet of the House Energy and Commerce Committee 10 days later. He listed a number of ways in which spyware can harm consumers and businesses.

> .... It seems clear from the workshop's discussions spyware may harvest personally identifiable information from consumers through monitoring computer use without consent. It also may facilitate identity theft by surreptitiously planting a keystroke logger on a user's computer.
>
> Spyware may create security risks if it exposes communications channels to hackers. It also may effect [sic] the operation of personal computers, causing crashes, browser hijacking, homepage resetting and the like. These harms are problems in themselves and could lead to a loss in consumer confidence in the Internet as a medium of communication and commerce.

---

[13] For example, see Bass, Steve. Spyware Wrap-Up. PC World, November 3, 2004. Available at [http://www.pcworld.com/howto/article/0,aid,118215,00.asp]. The September 2004 issue of Consumer Reports rates anti-spyware products.

[14] The transcript of the workshop is available at [http://www.ftc.gov/bcp/workshops/spyware/transcript.pdf].

> Second, many of the panelists discussed how spyware may cause problems for businesses, too. Companies may incur costs as they seek to block and remove spyware from computers of their employees or their customers. Employees will also be less productive if spyware causes their computers to crash or if they're distracted...by a barrage of pop-up ads. Spyware that captures the keystrokes of employees could be used to obtain trade secrets and confidential information from businesses.[15]

Mr. Beale also listed a number of ways in which the computer industry is attempting to help consumers and businesses cope with the spyware problem, for example through development of anti-spyware programs.

An FTC staff report on the results of the workshop was published in March 2005.[16] The report concluded that addressing the spyware problem will require a coordinated and sustained effort on the part of the private sector and government.

The FTC also has taken legal actions to stop spyware practices. FTC Chairwoman Deborah Platt Majoras summarized the FTC's activities at an October 5, 2005 hearing before the Subcommittee on Trade, Tourism, and Economic Development of the Senate Commerce, Science, and Transportation Committee.[17]

State Laws

In March 2004, Utah became the first state to enact spyware legislation (although a preliminary injunction prevented it from taking effect, and the Utah legislature passed a new law in 2005 amending the 2004 act).[18] In testimony to a House Energy and Commerce subcommittee in April 2004, then-FTC Commissioner Mozelle Thompson asked states to "be cautious" about passing such legislation because "a patchwork of differing and inconsistent state approaches might be confusing to industry and consumers alike."[19]

---

[15] House Energy and Commerce Committee. Hearing, April 29, 2004. Hearing transcript provided by Federal Document Clearing House (via Factiva).

[16] An FTC press release, and a link to the report, are at [http://www.ftc.gov/opa/2005/03/spywarerpt.htm].

[17] Ms. Majoras' statement is available at [http://commerce.senate.gov/pdf/majoras-spyware.pdf].

[18] WhenU, an adware company, filed suit against the Utah law on constitutional grounds. (WhenU's President and CEO, Avi Naider, testified to the Senate Commerce Committee's Subcommittee on Communications about spyware in March 2004. See **Industry Positions**, below.) The Third Judicial District Court in Salt Lake City, Utah granted a preliminary injunction on June 22, 2004, preventing the law from taking effect. See Judge Grants NY Pop-Up Company Preliminary Injunction Against Spyware Law. Associated Press, June 23, 2004, 06:06 (via Factiva).

[19] House Committee on Energy and Commerce. Hearing, April 29, 2004. Hearing transcript provided by the Federal Document Clearing House (via Factiva).

In 2006, at least 18 states have considered spyware legislation and at least three have enacted/adopted that legislation: Hawaii, Louisiana, and Tennessee. Detailed listings of spyware legislation from 2004, 2005, and 2006, are available on the National Council for State Legislature's website.[20]

Issues for Congress

The first session of the 109th Congress continued to debate the spyware issue. Two bills passed the House: H.R. 29 (Bono) and H.R. 744 (Goodlatte). Three bills were introduced in the Senate: S. 687 (Burns-Wyden), S. 1004 (Allen), and S. 1608 (Smith). S. 687 and S. 1608 were ordered reported from the Senate Commerce Committee in 2005. All the bills from the 109th Congress, 1st session, are summarized later in this report. Legislation from the 108th Congress is summarized in the Appendix.

Debate Over the Need for Federal Spyware Legislation

The main issue for Congress is whether to enact new legislation specifically addressing spyware, or to rely on industry self-regulation and enforcement actions by the FTC and the Department of Justice under existing law.

Advocates of legislation want specific laws to stop spyware. For example, they want software providers to be required to obtain the consent of an authorized user of a computer ("opt-in") before any software is downloaded onto that computer. Skeptics contend that spyware is difficult to define and consequently legislation could have unintended consequences, and that legislation is likely to be ineffective. One argument is that the "bad actors" are not likely to obey any opt-in requirement, but are difficult to locate and prosecute. Also, some are overseas and not subject to U.S. law. Other arguments are 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.

In many ways, the debate over how to cope with spyware parallels the controversy that led to unsolicited commercial electronic mail ("spam") legislation.[21] Whether to enact a new law, or rely on enforcement of existing law and industry self-regulation, were the cornerstones of that debate as well. Congress chose to pass the CAN-SPAM Act (P.L. 108-187). Questions remain about that law's effectiveness (see CRS Report RL31953). Such reports fuel the argument that spyware legislation similarly cannot stop the threat. In the case of spam, FTC officials emphasized that consumers should not expect any legislation to solve the spam problem — that

---

[20] See NCSL Electronic/Internet Privacy page ay [http://www.ncsl.org/programs/lis/privacy/techprivacy.htm].

[21] See CRS Report RL31953, "Spam": An Overview of Issues Concerning Commercial Electronic Mail, by Marcia S. Smith.

consumer education and technological advancements also are needed. The same is true for spyware.

Several subcommittee or full committee hearings on spyware were held in 2004 and 2005 at which witnesses from the government, industry, and consumer groups laid out their various points of view:[22]

- Senate Commerce, Science, and Transportation Committee, Subcommittee on Communications, March 23, 2004
- House Energy and Commerce Committee, Subcommittee on Telecommunications and the Internet, April 29, 2004
- House Energy and Commerce Committee, January 26, 2005
- Senate Commerce, Science, and Transportation Committee, May 11, 2005
- Senate Commerce, Science, and Transportation Committee, Subcommittee on Trade, Tourism, and Economic Development, October 5, 2005.

FTC's Position. At the October 5, 2005 Senate Commerce subcommittee hearing, FTC Chairwoman Deborah Platt Majoras offered the FTC's formal position on the need for new spyware legislation for the first time.[23] Ms. Majoras called spyware a "serious and growing problem" and reviewed FTC actions to protect consumers from it.[24] She said that in the past year the FTC had initiated five law enforcement actions, and has ongoing investigations. She said that the FTC supports legislation that would enhance its ability to investigate and prosecute spyware distributors that are located abroad or who use foreign intermediaries. She specifically endorsed S. 1608, which was introduced by the subcommittee's chairman, Senator Smith. She also said the FTC could support legislation giving it authority to seek civil penalties against spyware distributors. Further, she said that the FTC would continue to coordinate with federal and state partners in bringing law enforcement actions under existing law, and to educate consumers about the risks of spyware and anti-spyware tools. She also noted, however, that technological solutions are needed.

Absent a formal FTC position, two commissioners, Orson Swindle and Mozelle Thompson, previously had offered personal views on the spyware issue. Both have since left the Commission. Neither supported new legislation at the time of their statements. Mr. Swindle told a March 4, 2005 technology forum sponsored by Citizens Against Government Waste that the government should "walk slowly" on such issues, noting that participants in the spyware debate cannot even agree on a

---

[22] Witness testimony and hearing transcripts, when available, are online at [http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Home] (Senate) and [http://energycommerce.house.gov/108/action.htm] (House).

[23] Ms. Majoras offered similar statements in a February 9, 2006, speech at the Anti-Spyware Coalition public meeting, available online at [http://www.ftc.gov/speeches/majoras/060209cdtspyware.pdf].

[24] FTC Chairwoman Majoras' statement is available at the Senate Commerce Committee's website at [http://commerce.senate.gov/pdf/majoras-spyware.pdf].

definition of the term.[25] He reportedly called for Congress to focus on expanding enforcement of existing laws against bad actors, rather than further regulation of software makers. At a November 5, 2004 luncheon sponsored by the Cato Institute,[26] Mr. Swindle expressed similar views, and also called on industry to develop effective approaches to counteract spyware — through self-regulation, adopting standards, consumer education, business education, assisting the government in finding the people doing the harm, and monitoring their own advertising (and whom they hire to do advertising on their behalf). He added that if industry did not solve the problem, by necessity the government would need to act.

At the April 2004 House Energy and Commerce subcommittee hearing, Commissioner Mozelle Thompson argued that industry should be given an opportunity to solve the problem and the government should step in only if necessary. Mr. Thompson reviewed challenges he had given to industry at the FTC's spyware workshop: to develop a set of "best practices ... including meaningful notice and choice so that consumers can make informed decisions about whether or not they wish to deal with an online business that uses monitoring software or partners with companies that do"; to develop a campaign to educate consumers and businesses about spyware and how to cope with it; and to establish a mechanism to allow businesses and consumers to have a dialog "on how government can take action against those who do wrong and undermine consumer confidence through the misuse of spyware."[27]

Industry Positions. At the March 2004 Senate Commerce subcommittee hearing, industry witnesses discussed the difficulties in legislating in an area where definitions are unclear, and that the pace of technology might quickly render any such definitions obsolete. Robert Holleyman, representing the Business Software Alliance, testified that the focus of legislation should be regulating bad behavior, not technology. He expressed reservations about legislation which then was pending in the Senate, and called on Congress not to preclude the evolution of tools and marketplace solutions to the problem.

While there is concern generally about any software product installed without the user's knowledge or consent, adware is a particular area of controversy. Many users object to pop-up ads as vigorously as they do to spam. The extent to which pop-up ads are, or should be, included in a definition of spyware was discussed at the March 2004 Senate Commerce subcommittee hearing. 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

---

[25] As reported in: "Walk Slowly" on Privacy Legislation, FTC Comr. Says. Warren's Washington Internet Daily, March 7, 2005 (via Factiva).

[26] A video of the presentation is available at [http://www.cato.org/event.php?eventid=1725]. See also: FTC's Swindle: Leave Spyware Solution to Industry. Warren's Washington Internet Daily, November 8, 2004 (via Factiva).

[27] House Energy and Commerce Committee. Hearing, April 29, 2004. Hearing transcript provided by Federal Document Clearing House (via Factiva).

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 above, WhenU has filed suit against a Utah law regulating spyware.

At the April 2004 House Energy and Commerce subcommittee hearing, David Baker, representing Earthlink, described his company's efforts to combat spyware, and supported legislation to protect consumers. Jeffrey Friedberg, from Microsoft, said that his company supports a "holistic" solution, and that if existing law is inadequate, then additional legislation would be appropriate.

At the January 2005 House Energy and Commerce Committee hearing, representatives of Microsoft and Earthlink generally supported H.R. 29, with some minor alterations. Modifications were made to that bill during subcommittee and full committee markup, reportedly in response to industry and Senate concerns.[28]

At the May 2005 Senate Commerce Committee hearing, the Network Advertising Initiative (NAI) called for federal legislation that preempts state laws, and that focuses on fraudulent and deceptive behaviors. NAI's Executive Director, J. Trevor Hughes, stated that NAI supports Section 2 of H.R. 29, which deals with deceptive practices, but not other provisions of that bill that would set standards for online advertising. He argued that "Online advertising is the primary economic force that creates the enormous amount of free content we enjoy online today. Proscribing online advertising will compromise that economic model, and may threaten the available of free resources online."[29] He added that "Spyware is not caused by technology. Indeed, in many cases the technology is irrelevant to the practice involved. If legislation were to limit a certain technology, the purveyors of spyware would simply move to, or develop, other technologies to continue their activities. Prohibiting or proscribing technologies is not good public policy."[30] He argued that industry self regulation and technology solutions are needed in addition to narrowly-based legislation, and cautioned that spyware should not be confused with privacy, and the two should be treated separately. Conversely, at the same hearing, Webroot Software CEO C. David Moll, specifically linked spyware and online privacy, saying that "spyware is the cyber-age equivalent of someone trespassing into your home."[31]

---

[28] Juliana Gruenwald. House Panel Backs Bill to Crack Down on Spyware. Technology Daily, available at [http://nationaljournal.com/members/markups/2005/02/200504702.htm].

[29] Testimony of J. Trevor Hughes, Network Advertising Initiative, to the Senate Commerce, Science, and Transportation Committee May 11, 2005. Available on the committee's website [http://commerce.senate.gov]. The NAI [http://www.networkadvertising.org] is a cooperative group of network advertisers that established self-regulatory privacy principles for online advertising.

[30] Hughes, May 11, 2005 Senate Commerce Committee testimony, Ibid.

[31] Testimony of C. David Moll, Webroot Software, to the Senate Commerce, Science, and (continued...)

The Information Technology Association of America (ITAA) reportedly supports H.R. 744.[32]

Meanwhile, in January 2006, an industry coalition launched a website — [http://www.stopbadware.org] — to gather data from consumers about their experiences with spyware and other "badware" programs. The website describes itself as a "neighborhood watch" type of organization, and a clearinghouse for research on "badware and the bad actors who spread it." The industry coalition includes technology companies Google, Lenovo, and Sun Microsystems.

Consumer Groups and Others. At the March 2004 Senate Commerce subcommittee hearing, John L. Levine, author of *The Internet for Dummies* and similar books, concluded that legislation should ban spyware 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.

At the same 2004 hearing, CDT's Jerry Berman noted that three existing laws can be used to address spyware concerns: the Federal Trade Commission Act (the FTC Act), the Electronic Communications Privacy Act (ECPA), and the Computer Fraud and Abuse Act (CFAA). He added 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. Another CDT representative, Ari Schwartz, made similar arguments at three other hearings.

More recently, CDT issued a report on spyware enforcement that summarizes active and resolved spyware cases at the FTC and the Department of Justice, and in individual states.[33]

Legislation in the 109th Congress, 1st Session

Two bills passed the House on May 23, 2005 — H.R. 29 (Bono) and H.R. 744 (Goodlatte) — both of which are very similar to legislation that passed the House in 2004 (H.R. 2929 and H.R. 4661, respectively). Three bills were introduced in the Senate — S. 687 (Burns), which is similar to legislation that was considered in 2004, but did not reach the floor (S. 2145); S. 1004 (Allen); and S. 1608 (Smith). S. 687

---

[31] (...continued)
Transportation Committee, May 11, 2005. Available on the committee's website [http://commerce.senate.gov].

[32] Sharma, Amol. House Committee Approves Bono's Anti-Spyware Bill. CQ Today, March 9, 2005, 12:19 pm.

[33] "Spyware Enforcement," CDT, June 2006, available online at [http://www.cdt.org/privacy/spyware/20060626spyware-enforcement.pdf].

and S. 1608 were ordered reported from the Senate Commerce Committee in 2005.[34] At the markup that favorably reported S. 687, the committee rejected Senator Allen's attempt to substitute the language of his bill (S. 1004) for the text of S. 687.[35] S. 687 was placed on the Senate Legislative Calendar under general Orders, Calendar no. 467, on June 12, 2006. S. 1608 was referred to the House Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection, on April 19, 2006.

H.R. 29 (Bono), Spy Act. H.R. 29, the Securely Protect Yourself Against Cyber Trespass Act (Spy Act), passed the House on May 23, 2005. It is a revised version of H.R. 2929, which passed the House in 2004 (see Appendix). The only change made to the bill's language when it was reintroduced was changing the date when the act would sunset to 2010 (instead of 2009) so that it still would have a five-year lifetime. The House Energy and Commerce Committee held a hearing on H.R. 29 on January 26, 2005. Some modifications (including changing SPY ACT to Spy Act) were made during subcommittee markup on February 4, 2005, and full committee markup on March 9, 2005. The bill was reported from committee on April 12, 2005 (H. Rept. 109-32). Additional changes were made before the bill was brought to the House floor.

The provisions of H.R. 29 as passed by the House are summarized in general below. *Changes made after the bill was reported from committee, prior to House passage, are shown in italics.* Different sections have various effective dates, but the legislation overall would become effective 12 months after enactment, and expire on December 31, 2011 (*as reported from committee, it would have expired in 2010*).

- Section 2 prohibits *unfair or* 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, hijacking, or using the computer's Internet connection and thereby damaging the computer or causing the owner, user, or third party defrauded by such conduct, to incur unauthorized financial charges or other costs; 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 undue effort or knowledge by the user or* without turning off the computer or closing all sessions of the Internet browser;

---

[34] The bill reports are available online at [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_reports&docid=f:sr262.109.pdf] (S. 687) and [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_reports&docid=f:sr219.109.pdf] (S. 1608).

[35] Tessler, Joelle. Consumer Protections Against 'Spyware' Advanced by Senate Committee. CQ Weekly, November 21, 2005, p. 3146.

- → 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;
- → induce the owner or user of a computer to disclose PII by means of a Web page that is substantially similar to a Web page established or provided by another person, or mislead the owner or user that such Web page is provided by such other person;
- → 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 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.

- 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 was provided as required in this bill, and the program included 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 was executed.

"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, except if the only information collected regarding Web pages is information regarding Web pages within a particular website and such information is not sent to anyone other than the provider of that website or a party authorized to facilitate the display or functionality of Web pages within that website, and the only advertising delivered to or displayed using such information is advertising on Web

pages within that particular website. The bill specifies certain requirements for notice (differentiating among various types of software at issue) and 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, executed 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 type, or for a purpose, materially different from and outside the scope of what was 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 accesses a Web page or online location other than that of the program's provider, the program must include a function that identifies itself, except for the embedded display of advertising on a Web page that contemporaneously displays other information. Telecommunications carriers, information service or interactive computer service providers, cable operators, or providers of transmission capability are not liable under the act.

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

Violations are to be treated as an unfair or deceptive act or practice under the section 18 of 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. Civil penalties may not be granted by the FTC or a court, however, unless it is established that the action was 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. In determining the amount of any penalty, the court shall take into account the degree of culpability, any history of prior such conduct, ability to pay, affect on ability to continue to do business, and such other matters as justice may require.

- 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 *unfair or* 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. No person other than a state Attorney General is allowed to 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 does 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 a second report. The second report is to be on the use of "cookies, including tracking cookies" to deliver or display advertisements, the methods by which cookies and the websites that place them on websites function separately and together, and comparing the use of cookies with the use of information collection programs to determine the extent to which such uses are similar or different. The report may include recommendations including treatment of cookies under this act or other laws. [*The definition of tracking cookie was modified in the version of the bill that passed the House.]*
- → *Requirements for the FTC to submit a report on the extent to which information collection programs that were installed prior to the effective date of the act would have been subject to the act's protections under section 3, including recommendations regarding requiring a one-time notice and consent by the owner or authorized user of a computer to the continued collection of information by such program.* (The effective date of the act is 12 months after enactment, and section 3 does not apply to information collection programs installed before that date.)

In general, the FTC is required to issue regulations required by the act no later than six months after enactment, and shall determine that the regulations are consistent with the public interest and the purposes of the act.

H.R. 744 (Goodlatte), I-SPY Act. H.R. 744, the Internet Spyware Prevention (I-SPY Act), also passed the House on May 23, 2005. The bill was introduced on February 10, 2005, and referred to the House Judiciary Committee. It was reported on May 23, 2005 (H.Rept. 109-93) and passed the House that day. As introduced, the bill was identical to H.R. 4661 as it passed the House in 2004, except that the four years for which funding was authorized shifted from FY2005-2008 to FY2006-2009. As reported and passed, slight modifications were made.

In general, the bill imposes fines or imprisonment for certain acts associated with spyware. As passed, H.R. 744 would impose fines and/or imprisonment of up to five years for anyone who accesses a computer without authorization, or exceeds authorized access, by causing a computer program or code to be copied onto a protected computer and intentionally uses it in furtherance of another federal crime. Anyone who intentionally accesses a computer without authorization, or exceeds authorized access, by causing a computer program or code to be copied onto a computer and uses it to intentionally obtain, or transmit to someone else, personal information, with the intent to defraud or injure a person or cause damage to the computer, or to intentionally impair the security protections of the computer, would be fined and subject to up to two years in prison.

No person may bring a civil action under state law if the action is premised in whole or in part upon a violation of this bill. Language is included clarifying that the bill does not prohibit lawfully authorized investigative, protective, or intelligence activities.

The bill authorizes $10 million for each of four fiscal years (FY2006-FY2009) to the Department of Justice for prosecutions needed to discourage spyware, "phishing" or "pharming."[36] It includes a sense of Congress provision that the Department of Justice should use this act to vigorously prosecute those who use spyware to commit crimes and those that conduct phishing or pharming scams.

S. 687 (Burns-Wyden), SPY BLOCK Act. S. 687, the Software Principles Yielding Better Levels of Consumer Knowledge (SPY BLOCK)Act, was introduced by Senators Burns and Wyden on March 20, 2005. It was ordered reported from the Senate Commerce, Science, and Transportation Committee, amended, on November 17, 2005, and placed on the Senate Legislative Calendar on June 12, 2006 (Calendar no. 467).

As introduced, it was similar, but not identical, to S. 2145 from the 108th Congress (see Appendix). The text of the version that was ordered reported from committee is not yet publicly available, although the committee issued a press release describing the bill as amended.[37] The summary of the bill below is based on the version that was introduced, except that changes specifically noted in the press releases are shown in italics.

As introduced, the bill would make it unlawful for a person who is not an authorized user of a computer —

- to cause the installation of software on that computer in a manner that conceals from the user the fact that the software was being installed, or prevents the user from having an opportunity to knowingly grant or withhold consent to the installation. This does not apply to (1) the installation of software falling within the scope of a previous grant of authorization, (2) installation of an upgrade to software already installed with the user's authorization, (3) software installed before the first retail sale and delivery of the computer, or (4) installation of software that ceases to operate when the user of the computer exits the software or service through which the user accesses the Internet, if the software so installed does not begin to operate again when the user accesses the Internet in the future.

- to induce a person to consent to the installation of software by means of a materially false or misleading representation concerning — the identity of the operator of an Internet website or online service

---

[36] "Phishing" 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). 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.

[37] Senate Commerce, Science, and Transportation Committee. Senate Commerce Committee Approves SPY BLOCK Act. Undated press release available at the committee's website: [http://commerce.senate.gov/newsroom/printable.cfm?id=249026]

where the software is made available for download from the Internet; the identity of the author, publisher, or authorized distributor of the software, the nature or function of the software; or the consequences of not installing the software. The software must be able to be easily uninstalled or disabled, with exceptions (for example, a parent, employee, or system administrator may install software that another user would find difficult to uninstall or disable).

- to cause the installation of software that includes a surreptitious information collection feature (as defined in the legislation), or to use such software to collect information about a user of the computer or how the computer is used. This does not, however, prohibit a person from causing the installation of software that collects and transmits only information that is reasonably needed to determine whether or not the user of a computer is licensed or authorized to use the software.

- to cause the installation of "adware" that does not have a label or other reasonable means of identifying which software caused the advertisement to be displayed. This would not apply if the advertisement is displayed only when a user is accessing an Internet website or online service operated by the publisher of the software, or that operator has provided express consent to the display of such advertisements to users of the website or service. It also would not apply if the advertisement is displayed only in a manner, or at a time, such that a reasonable user would understand which software caused the delivery of the advertisement.

- to engage in an unfair and deceptive act or practice that involves utilizing the computer to send unsolicited information or material to other computers; to divert an authorized user's Internet browser away from the site the user intended to view; to display an advertisement or other content through windows in an Internet browser in such a manner that the computer's user cannot end the display without turning off the computer or terminating the browser; modify computer settings related to use of the computer or Internet access, such as altering the default website that initially appears when a user opens an Internet browser; or remove, disable, or render inoperative a security or privacy protection technology installed on the computer.

According to the committee's press release, the amended version of the bill prohibits personal information collection when the collection is not "clearly and conspicuously disclosed" or advertised as part of the software's purpose. If sensitive personal information, such as social security numbers or account numbers, is being collected, then a notice and consent regime is required. In addition, users must be able to uninstall any software that collects personal information.

The bill also provides liability limitations. For example, a person would not violate the law solely by providing an Internet connection through which spyware was installed. Network or online service providers to which an authorized user subscribes would not violate the section on collection of information, for example, if they do so to protect the security of the network, service or computer. Computer manufacturers and retailers would not be liable for third-party branded software unless they use a surreptitious information collection feature included in the software to collect information about a user of the computer or the use of the computer or knows that the software will cause advertisements for the manufacturer or retailer to be displayed. Furthermore, nothing in the act prohibits any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency.

The FTC is allowed to issue rules that are necessary to implement or clarify the provisions of the act, including regulations establishing safe harbors, such as notifications or labels that are sufficient to avoid violations. The FTC may establish additional liability limitations beyond those provided in the act.

Generally, the FTC is to enforce the law as if a violation was an unfair or deceptive practice. However, other agencies were identified for enforcing the law for certain businesses (e.g., the Comptroller of the Currency would enforce it for national banks and federal branches and federal agencies of foreign banks).

State Attorneys General may bring actions on behalf of residents of that state, but must notify the FTC, and the FTC may intervene. The act supersedes state laws or laws of political subdivisions of that state if the law expressly limits or restricts the installation or use of software to collect information about the user or the user's activities, or causes advertisements to be delivered to the user, except to the extent that any such statute, regulation, or rule prohibits deception in connection with the installation or use of such software. It supersedes any statute, regulation, or rule of a state or political subdivision thereof that prescribes specific methods for providing notification before the installation of software on a computer. It does not preempt the applicability of state criminal, trespass, contract, tort, or anti-fraud law. Criminal penalties (fines and/or imprisonment of up to five years) are set for violation of the law. The law would become effective 180 days after enactment.

S. 1004 (Allen), Enhanced Consumer Protection Against Spyware Act. S. 1004 was introduced by Senator Allen on May 11, 2005, and referred to the Senate Commerce, Science, and Transportation Committee. During markup of S. 687, Senator Allen offered the text of his bill as a substitute amendment for the text of S. 687, but was defeated 9-13.[38]

S. 1004 would increase civil and criminal penalties for spyware distributors and creators, allow the government to seize profits from spyware purveyors, and give the FTC authority to share information with foreign law enforcement officials.[39]

---

[38] Tessler, Joelle. Consumer Protections Against 'Spyware' Advanced by Senate Committee. CQ Weekly, November 21, 2005, p. 3146.

[39] (1) Larkin, Erik. Lawmakers Set Their Sights on Spyware. PCWorld online, May 11, (continued...)

The bill would reaffirm the FTC's authority to combat deceptive acts or practices related to spyware, and allow the FTC to triple fines under the FTC Act for spyware violations. For persons who engage in a pattern or practice of such violations, the FTC could seek a civil penalty of up to $3 million for each violation, and have the authority to "disgorge and seize any ill-gotten gains."

The bill would preempt state and local laws relating to or affecting the installation of software through deceptive acts or practices, or the use of computer software installed by means of the Internet; and does not allow private right of action, including a class action. State Attorneys General could bring action on behalf of residents of that state in a federal district court, but must notify the FTC and the U.S. Attorney General, and the U.S. Attorney General may intervene. If the U.S. Attorney General or the FTC instituted an action under this bill, state officials could not. A number of exceptions are provided for law enforcement authorities, Internet or other transmission or routing providers, certain types of websites, manufacturers and retailers of computer equipment, etc.

It would amend the FTC Act such that unfair and deceptive acts and practices include those involving foreign commerce that cause or are likely to cause reasonable foreseeable injury within the United States or involve material conduct occurring within the United States.

Persons who intentionally access a computer without authorization, or exceed authorized access, by causing a computer program or code to be copied onto the protected computer and intentionally use that program or code in furtherance of another federal crime shall be fined or imprisoned for up to five years or both. Persons who intentionally access a computer without authorization, or exceed authorized access, by causing a computer program or code to be copied onto a computer and intentionally impair the security protection of the computer shall be fined or imprisoned for up to two years, or both. Various exceptions are allowed.

The bill would authorize not more than $10 million a year, beginning with FY2006, for the FTC to enforce violations associated with computer and Internet related crimes.

S. 1608 (Smith), US SAFE WEB Act. S. 1608, the Undertaking Spam, Spyware, and Fraud Enforcement With Enforcers beyond Borders (US SAFE WEB) Act, was ordered reported, without amendment, from the Senate Commerce Committee on December 15, 2005, and referred to the House Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection, on April 19, 2006. It is not a spyware bill in the same sense as the other bills summarized in this report. Instead, it would enhance FTC enforcement against spyware and other Internet-related fraud (including spam), focusing on cross-border fraud and deception. The bill would amend the FTC Act to include within the term

---

[39] (...continued)
2005 [http://www.pcworld.com/resource/article/0,aid,120814,pg,1,RSS,RSS,00.asp]; (2) Mark, Roy. New Bill Targets Spyware Profits. Internetnews.com, May 12, 2005 [http://www.internetnews.com/bus-news/article.php/3504631]

"unfair or deceptive acts or practices" those acts or practices involving foreign commerce that (1) cause or are likely to cause reasonably foreseeable injury within the United States; or (2) involve material conduct occurring within the United States. It also would authorize the FTC to disclose certain privileged or confidential information to foreign law enforcement agencies and to grant investigative assistance to them, and would shield from liability voluntary providers of information, including certain financial institutions.

FTC Chairwoman Majoras endorsed this bill at the October 5, 2005 hearing on spyware before a Senate Commerce subcommittee that is chaired by the bill's sponsor, Senator Smith. In introducing the measure earlier in the year, Senator Smith noted that a similar bill passed the Senate unanimously in the 108th Congress, but did not clear Congress.[40]

[40] *Congressional Record*, July 29, 2005, p. S9533.

Appendix: Summary of Legislative Action in the 108th Congress

The House passed two spyware bills in the 108th Congress — H.R. 2929 and H.R. 4661. The Senate Commerce Committee reported S. 2145 (Burns), amended, December 9, 2004 (S.Rept. 108-424). None of these bills cleared that Congress.

The Senate Commerce, Science, and Transportation Committee's Subcommittee on Communications held a hearing on spyware on March 23, 2004. The House Energy and Commerce's Subcommittee on Telecommunications and the Internet held a hearing on April 29, 2004. The House passed two spyware bills (H.R. 2929 and H.R. 4661) and the Senate Commerce Committee reported S. 2145, but there was no further action.

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."[41] The first approach is that taken in H.R. 4661; the second is in H.R. 2929.

H.R. 2929 (Bono), SPY ACT. H.R. 2929 has been reintroduced in the 109th Congress as H.R. 29, which is discussed above.

In the 108th Congress, the Securely Protect Yourself Against Cyber Trespass Act (SPY ACT) passed the House (399-1) on October 5, 2004. As passed, H.R. 2929 included the following provisions. Different sections had various effective dates, but the legislation overall would have expired on December 31, 2009. The version passed by the House reflected changes to the committee-reported version made by a manager's amendment.

- Section 2 would have prohibited deceptive acts or practices relating to spyware. It would have been unlawful for anyone who was 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

---

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

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;
- → 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 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.

- Section 3 would have prohibited the collection of certain information without notice and consent. It contained an opt-in requirement, whereby it would have been unlawful —

  - → to transmit any information collection program without obtaining consent from the user unless notice was provided as required in this bill, and the program included 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 was executed.

"Information collection program" was 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 specified certain requirements for notice (differentiating among various types of software at issue) and consent.

Only one clear and conspicuous notice, in plain language, was required if multiple collection programs, provided together or as a suite of functionally-related software, executed any of the information collection functions. The user had to be notified, and consent obtained, before the program was used to collect or send

information of a type, or for a purpose, materially different from and outside the scope of what was stated in an initial or previous notice. No subsequent notification was otherwise required. Users had to be able to disable or remove the information collection program without undue effort or knowledge. If an information collection program used the collected information to display advertisements when the owner or user accessed a Web page or online location other than that of the program's provider, the program had to include a function that identified itself. Telecommunications carriers, information service or interactive computer service providers, cable operators, or providers of transmission capability were not liable under the act.

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

Civil penalties were 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 was unfair or deceptive, or violated this act, were to be treated as an unfair or deceptive act or practice under the FTC Act. The FTC could have sought a civil penalty (maximum of $3 million per violation) if a person engaged in a pattern or practice of violations. Any single action, or conduct that affected multiple computers, was to be treated as a single violation. But a single action or conduct that violated multiple sections of the act was to be treated as multiple violations.

- Other sections included —

  - → 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. No person other than a state Attorney General would have been allowed to bring a civil action under any state law if that action was premised, in whole or in part, on violations of this bill, except that this bill did not limit the enforcement of any state consumer protection law. The bill would not have preempted 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 the House on October 7, 2004 (415-0). The bill would have made it illegal

to access a computer without authorization to obtain sensitive personal information or cause damage to the computer, and imposed fines and sentences up to two years in prison. If the unauthorized access was to further another federal crime, a sentence of up to five years was allowed. No person could have brought a civil action under state law if the action was premised in whole or in part upon a violation of this bill. The bill authorized $10 million for each of four fiscal years (FY2005-FY2008) to the Department of Justice for prosecutions needed to discourage spyware and "phishing."[42] Language was included clarifying that the bill did 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, was ordered reported from the Senate Commerce Committee on September 22, 2004, after adopting a Burns substitute amendment that "steered clear of setting technical requirements for software companies."[43] Another amendment, offered by Senator Allen, was adopted that sets criminal penalties for spyware providers. The bill was reported, without a written report, on November 19, 2004, and with a written report (S.Rept. 108-424) on December 7. There was no floor action.

The bill, as reported, would have made it unlawful for a person who is not an authorized user of a computer —

- to cause the installation of software on a computer in a manner designed to conceal from the user the fact that the software was being installed, or prevent the user from having an opportunity to knowingly grant or withhold consent to the installation. This would not have applied to software falling within the scope of a previous grant of authorization, installation of an upgrade to software already installed with the user's authorization, or software installed before the first retail sale of the computer.

- to induce a person to consent to the installation of software by means of a materially false or misleading representation concerning — the identity of the operator of an Internet Website or online service where the software is made available for download from the Internet; the identity of the author or publisher of the software, the nature or function of the software; or the consequences of not installing the software. The software had to be able to be easily uninstalled or disabled, with exceptions (for example, a parent or system administrator may install software that another user would find difficult to uninstall or disable).

- to authorize or cause the installation of software that collects information about the user of the computer or the user's activities

---

[42] "Phishing" 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).

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

and transmits that information to any other person on an automatic basis or at the direction of someone other than the authorized user, with exceptions.

- to authorize or cause the installation of "adware."

- to knowingly and without authorization use the computer to send unsolicited information or material to other computers; to divert an authorized user's Internet browser away from the site the user intended to view; to display an advertisement or other content through windows in an Internet browser in such a manner that the computer's user cannot end the display without turning off the computer or terminating the browser; covertly modify computer settings related to use of the computer or Internet access, such as altering the default website that initially appears when a user opens an Internet browser; use software installed in violation of an earlier section of the bill regarding collection of information; or remove, disable, or render inoperative a security or privacy protection technology installed on the computer.

The bill also would have provided liability limitations for certain persons. For example, a person would not have violated the law solely by providing an Internet connection through which spyware was installed. Network or online service providers to which an authorized user subscribes would not have been deemed to have violated the section on collection of information, for example, if they did so to protect the security of the network, service or computer.

Generally, the FTC would have enforced the law as an unfair or deceptive practice. However, other agencies were identified for enforcing the law for certain businesses (e.g., the Comptroller of the Currency would enforce it for national banks and federal branches and federal agencies of foreign banks).

State Attorneys General could have brought actions on behalf of residents of that state, but would have been required to notify the FTC, and the FTC could intervene. The law would have superseded state laws or laws of political subdivisions of that state if the law expressly limited or restricted the installation or use of software to collect information about the user or the user's activities, or cause advertisements to be delivered to the user, except to the extent that any such statute, regulation, or rule prohibited deception in connection with the installation or use of such software. It would not have preempted the applicability of state trespass, contract, tort, or anti-fraud law. Criminal penalties (fines and/or imprisonment of up to five years) were set for violations of the law.