Order Code RL32706

CRS Report for Congress
Received through the CRS Web

Spyware: Background and Policy Issues for Congress

Updated April 4, 2005

Marcia S. Smith
Specialist in Aerospace and Telecommunications 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 a 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.

Utah and California have passed spyware laws, but there is no specific federal law regarding spyware. The 109th Congress is considering H.R. 29, H.R. 744, and S. 687. The two House bills are similar to bills that passed the House in 2004. H.R. 29 was ordered reported from the House Energy and Commerce Committee on March 9, 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. 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, and resulting impacts on their privacy, leads others to conclude that legislative action is needed.

This report will be updated as warranted.

Contents

Background 1
What is Spyware? 1
Prevalence of Spyware 3
FTC Advice to Consumers 3
Other FTC Activities 4

State Laws 6
Utah 6
California 7

Issues for Congress 7
Debate Over the Need for Federal Spyware Legislation 7
FTC's Position 8
Industry Positions 9
Consumer Groups and Others 10
109th Congress Legislation 10
H.R. 29 (Bono), Spy Act 10
H.R. 774 (Goodlatte), I-SPY Act 13
S. 687 (Burns), SPY BLOCK Act 14

Appendix: Summary of Legislative Action in the 108th Congress 17
H.R. 2929 (Bono), SPY ACT 17
H.R. 4661 (Goodlatte), I-SPY Act 19
S. 2145 (Burns), SPY BLOCK Act 20

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 emplaced on a computer without the user's knowledge that takes control of the computer away from the user, such as by redirecting the computer to unintended websites, causing advertisements to appear, or collecting information and transmitting it to another person. The lack of a firm definition of the term adds to the complexities of drafting new laws.

The Federal Trade Commission (FTC) and others 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. The 108th Congress debated spyware legislation, and two bills passed the House, but neither cleared Congress. Debate has resumed in the 109th Congress. Pending legislation is discussed later in this report.

What is Spyware?

The term "spyware" is not well defined. Jerry Berman, President of the Center for Democracy and Technology (CDT), explained in testimony to the Subcommittee on Communications of the Senate Commerce, Science, and Transportation Committee in March 2004 that "The term has been applied to software ranging from 'keystroke loggers' that capture every key typed on a particular computer; to advertising applications that track users' web browsing; to programs that hijack users' system settings."[1] 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."

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

---

[1] 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.

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.

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.[2] 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.[3]

As discussed below, the lack of a precise definition for spyware is often cited by opponents of legislation as a reason not to legislate. They argue that without a 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, have legitimate uses. The question is whether the user has given consent for it to be installed.

---

[2] 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.

[3] 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.

Prevalence of Spyware

In October 2004, America Online (AOL) and the National Cyber Security Alliance (NCSA)[4] released the results of a survey of 329 dial-up and broadband computer users regarding online threats, including spyware.[5] 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.[6]

A representative of Dell Inc. told the *Washington Post* that between August 2003 and October 2004, customer support calls related to spyware rose from about 2% to 10-15%.[7]

FTC Advice to Consumers

The 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.[8] The FTC alert listed the following clues:

- a barrage of pop-up ads;

---

[4] According to its website [http://www.staysafeonline.info], 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.

[5] 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].

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

[7] Cha, Ariana Eunjung. Computer Users Face New Scourge; Hidden Adware Programs Hijack Hard Drives. Washington Post, October 10, 2004, p. A1 (via Factiva).

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

- 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.

- 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.[9]

Other FTC Activities

The FTC held a workshop on spyware on April 19, 2004.[10] The director of FTC's Bureau of Consumer Protection, Howard Beales, 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

---

[9] 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.

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

> 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.
>
> 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.[11]

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.[12] 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 action to stop spyware practices. The Commission filed its first spyware case in October 2004 in response to a complaint filed by the Center for Democracy and Technology (CDT). In an October 12, 2004 press release,[13] the FTC explained that it was charging Sanford Wallace and two companies with which he is associated, Smartbot.Net and Seismic Entertainment Productions. Inc., with unfair and deceptive practices for using a variety of techniques to direct consumers to their websites where spyware was downloaded onto their computer without notice or consent. The FTC asserts that the spyware created serious problems on those computers, and the defendants thereupon offered to sell the consumers software for $30 to fix the problems. The FTC asked the U.S. District Court, District of New Hampshire, "to issue an order preventing the defendants from disseminating spyware and giving up their ill-gotten gains."[14] Mr. Wallace denied

---

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

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

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

[14] FTC press release, Ibid.

wrongdoing.[15] U.S. District Judge Joseph DiClerico issued a temporary restraining order against the defendants on October 21, 2004.[16]

State Laws

In March 2004, Utah became the first state to pass spyware legislation. California followed in September. In testimony to the House Energy and Commerce Committee's Subcommittee on Telecommunications and the Internet in April 2004, FTC Commissioner Mozelle Thompson not only called on Congress to give industry an opportunity to self-regulate, but also 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."[17]

Utah

On March 23, 2004, the Governor of Utah, Olene Walker, signed the first state anti-spyware law, which became effective on May 3, 2004.[18] The definition of spyware in that law includes certain pop-up ads. It prohibits, for example, some pop-up ads that partially or wholly cover or obscure paid advertising or other content on a website in a way that interferes with a user's ability to view the website. A media report stated that passage of the law was "driven by a Utah company in a legal fight with a pop-up company."[19] The Utah law also defines spyware, inter alia, as software installed on a computer without the user's consent and that cannot be easily disabled and removed. Several high-tech companies reportedly argued that the law could have unintended consequences, for example, prohibiting parents from installing software to block access by their children to certain Websites because the software monitors Web activities, may have been installed without the child's consent, and the child may not be able to uninstall it easily.[20]

WhenU, an adware company, filed suit against the Utah law on constitutional grounds.[21] (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

---

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

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

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

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

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

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

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

City, Utah granted a preliminary injunction on June 22, 2004, preventing the law from taking effect.[22]

California

California Governor Arnold Schwarzenegger signed a spyware bill into law on September 28, 2004,[23] which went into effect on January 1, 2005. Inter alia, the law prohibits a person or entity other than the authorized used of a computer — with actual knowledge, conscious avoidance of actual knowledge, or willfully — to cause software to be downloaded onto a computer and using it to take control of the computer, as specified; modify certain settings; collect PII; prevent reasonable efforts to block the installation of or disable the software; intentionally misrepresent that the software will not be installed or will be disabled; or through intentionally deceptive means, remove, disable, or render inoperative certain other software programs on the computer (security, antispyware, or antivirus). Critics argue that the law does not address many spyware-type practices, such as adware.[24]

Issues for Congress

The 109th Congress has resumed debate on the spyware issue. Two bills are pending in the House: H.R. 29 (Bono) and H.R. 744 (Goodlatte). One has been introduced in the Senate : S. 687 (Burns). Those bills are summarized later in this report. In the 108th Congress, the House passed two spyware bills, and a bill was reported from committee in the Senate. They are 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

---

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

[23] California Business and Professions Code. Section 22947-22947.6. Available at: [http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=6431619090+0+0+0&WAISaction=retrieve]

[24] California Goes After Spyware. Reuters, October 2, 2004., 07:17 am, available at : [http://www.wired.com/news/politics/0,1283,65203,00.html]/

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.[25] 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. MX Logic, a provider of "email defense solutions,"reported that, in November 2004, the percentage of unsolicited commercial e-mails that were compliant with the law was only 6% (up from 4% the previous month).[26] The report that the vast majority of commercial e-mails are not complying with the law fuels 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 consumer education and technological advancements also are needed. The same likely is true for spyware, too.

FTC's Position. The FTC has not taken a formal position on the spyware issue, but two commissioners have stated that they do not support new legislation at this time. Commissioner Orson Swindle reportedly 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 definition of the term.[27] 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,[28] 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 a hearing before the House Energy and Commerce Committee's Telecommunications and the Internet subcommittee on April 29, 2004, 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

---

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

[26] MX Logic Reports Compliance with Anti-Spam Law Increased 6 Percent in November; Highest Monthly Compliance to Date. Press release, December 13, 2004. [http://www.mxlogic.com/news_events/12_13_04.html]

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

[28] 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).

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."[29]

Industry Positions. At a hearing before the Senate Commerce, Science, and Transportation Committee's Communications Subcommittee on March 23, 2004, 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 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 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 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.

The House Energy and Commerce Committee held another hearing on January 26, 2005. At the 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

---

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

industry and Senate concerns.[30] Not all industry representatives support the bill, however. The Information Technology Association of America (ITAA), for example, reportedly is backing H.R. 744 instead[31] (that bill is summarized below).

Consumer Groups and Others. At the 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 the April 2004 and January 2005 House Energy and Commerce hearings.

109th Congress Legislation

Two bills are pending in the House — 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). One bill is pending in the Senate — S. 687 (Burns), which is similar to legislation that was considered in 2004, but did not reach the floor (S. 2145). Action in the 108th Congress is summarized in the Appendix.

The House Energy and Commerce Committee held a hearing on H.R. 29 on January 26, 2005. H.R. 774 was referred to the House Judiciary Committee; no hearing has been held on that bill. S. 687 was referred to the Senate Commerce, Science, and Transportation Committee; no hearing has been held.

H.R. 29 (Bono), Spy Act. H.R. 29, the Securely Protect Yourself Against Cyber Trespass Act (Spy Act), 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. Other modifications (including changing SPY ACT to Spy Act) were made during subcommittee markup

---

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

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

on February 4, 2005, and full committee markup on March 9, 2005, when the bill was ordered reported.

The provisions of H.R. 29 as ordered reported are summarized in general below. *Significant additions or deletions that occurred during the two markups are shown in italics*. Different sections have various effective dates, but the legislation overall would expire on December 31, 2010.

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

  - → take control of the computer by: utilizing the computer to send unsolicited information or material from the computer to others; diverting the computer's browser away from the site the user intended to view without authorization of the owner or authorized user of the computer, or otherwise authorized; accessing, *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 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 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 Web site and such information is not sent to anyone other than the provider of that Web site or a party authorized to facilitate the display or functionality of Web pages within that Web site, and the only advertising delivered to or displayed using such information is advertising on Web pages within that particular Web site.* 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.* [The bill as introduced said that violations that were committed with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, would be treated as unfair or deceptive acts or practices violating a rule promulgated under section 18 of the FTC Act, rather than saying that penalties may only be granted if those conditions are met]. *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 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. [*Regarding the second report, the original bill said the report was to be on "tracking cookies," not on cookies generically, and on the extent to which tracking cookies were covered by this act, without a comparison of cookies and information collection programs.*]

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. 774 (Goodlatte), I-SPY Act. The Internet Spyware Prevention (I-SPY Act) was introduced on February 10, 2005, and referred to the House Judiciary

Committee. The bill is identical to H.R. 4661 as it passed the House in 2004, except that the four years for which funding is authorized is shifted from FY2005-2008, to FY2006-2009. H.R. 774 would make it illegal to access a computer without authorization to obtain sensitive personal information or cause damage to the computer, and imposes fines and sentences up to two years in prison. If the unauthorized access is to further another federal crime, a sentence of up to five years is allowed. 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. The bill authorizes $10 million for each of four fiscal years (FY2006-FY2009) to the Department of Justice for prosecutions needed to discourage spyware and "phishing."[32] Language is included clarifying that the bill does not prohibit any lawfully authorized investigative, protective, or intelligence activities.

S. 687 (Burns), SPY BLOCK Act . The Software Principles Yielding Better Levels of Consumer Knowledge Act, was introduced by Senator Burns on March 20, 2005. It is similar, but not identical, to S. 2145 from the 108th Congress (see Appendix).

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 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).

---

[32] "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).

- 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.

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.

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."[33] 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

---

[33] 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."[34] 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."[35] 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

---

[34] "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).

[35] 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