Order Code RL32706

CRS Report for Congress

Spyware: Background and Policy Issues for Congress

Updated September 26, 2007

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

Prepared for Members and Committees of Congress

Spyware: Background and Policy Issues for Congress

Summary

The term "spyware" generally refers to any software that is downloaded onto a computer without the owner's or user's 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.

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. Thus far, two bills have been introduced in the House of Representatives (H.R. 964 and H.R. 1525) and one has been introduced in the Senate (S. 1625). Both of the House bills have been reported and referred to the Senate. The Senate bill was referred to committee and no further action has been taken.

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.

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.[1]

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.

---

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

In many ways, the debate over how to cope with spyware parallels the controversy that led to unsolicited commercial electronic mail ("spam") legislation.[2] 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 consumer education and technological advancements also are needed. The same is true for spyware.

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 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]

---

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

[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].

(continued...)

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 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

---

[5] (...continued)

[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.

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 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]

---

[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.

[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 online 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).

FTC Advice to Consumers

The FTC has consumer information on spyware that includes a link to file a complaint with the commission through its "OnGuard Online website.[12] The FTC has also issued a consumer alert about spyware that lists warning signs that might indicate a computer is infected with spyware.[13] 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
- 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
- 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 [http://www.pcworld.com/howto/article/0,aid,118215,00.asp] or at Spyware Warrior [http://www.spywarewarrior.com].

---

[12] Available at [http://onguardonline.gov/spyware.html].

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

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).[14] 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."[15]

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.[16]

Legislative Action – 110th Congress

During the 110th Congress, two bills have been introduced in the House of Representatives and one bill has been introduced in the Senate; the House has held two hearings.

H.R. 964 – Securely Protect Yourself Against Cyber Trespass Act

The "SPY ACT" was introduced by Representative Towns on February 8, 2007, and a hearing on it was held by the Committee on Energy and Commerce Subcommittee on Commerce, Trade and Consumer Protection on March 15, 2007.[17] This bill would make it unlawful to engage in unfair or deceptive acts or practices to take unsolicited control of computer, modify computer settings, collect personally identifiable information, induce the owner or authorized user of the computer to disclose personally identifiable information, induce the unsolicited installation of computer software, and/or remove or disable a security, anti-spyware, or anti-virus technology. This bill would also require the FTC to submit two reports to Congress.

---

[14] 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. 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).

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

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

[17] Information on this hearing, including a list of witnesses, witness testimony, and a link to the hearing broadcast archive are available online at [http://energycommerce.house.gov/cmte_mtgs/110-ctcp_hrg.031507.HR_964_spyact.shtml].

The first report would be on the use of cookies in the delivery or display of advertising; the second would be on the extent to which information collection programs were installed and in use at the time of enactment.

H.R. 964 was reported by the House Committee on Energy and Commerce on May 24, 2007,[18] and referred to the Senate Committee on Commerce, Science, and Transportation on June 7, 2007. No further action has been taken.

H.R. 1525 – Internet Spyware Prevention Act

The "I-SPY" Act was introduced by Representative Lofgren on March 14, 2007, and a hearing on it was held by the Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security on May 1, 2007.[19] . This bill would amend the federal criminal code to impose a fine and/or prison term of up to five years for intentionally accessing a protected computer[20] without appropriate authorization by causing a computer program or code to be copied onto the protected computer and intentionally using that program or code in furtherance of another federal criminal offense. The bill would impose a fine and/or prison term of up to two years if the unauthorized access was for the purpose of —

- intentionally obtaining or transmitting personal information[21] with intent to defraud or injure a person or cause damage to a protected computer
- intentionally impairing the security protection of a protected computer with the intent to defraud or injure a person or damage such computer.

H.R. 1525 was reported by House Committee on the Judiciary, where it was reported on May 21, 2007,[22] and then referred to the Senate Committee on the Judiciary on May 23, 2007. No further action has been taken.

---

[18] H. Rep. 110-169. Available online at [http://www.congress.gov/cgi-lis/cpquery/R?cp110:FLD010:@1(hr169)].

[19] Information on this hearing, including a list of witnesses, witness testimony, and a link to the hearing webcast are available online at [http://judiciary.house.gov/Hearings.aspx?ID=170].

[20] A protected computer is defined in this bill as "a computer exclusively for the use of a financial institution or the U.S. government

[21] For example, a Social Security number or other government-issued identification number, a bank or credit card number, or an associated password or access code.

[22] H. Rep. 110-169. Available online at [http://www.congress.gov/cgi-lis/cpquery/R?cp110:FLD010:@1(hr169)].

S. 1625 – Counter Spy Act

The Counter Spy Act was introduced by Senator Pryor on June14, 2007. This bill would prohibits unauthorized installation on a protected[23] computer of "software that takes control of the computer, modifies the computer's settings, or prevents the user's efforts to block installation of, disable, or uninstall software." It also would prohibit the installation of "software that collects sensitive personal information without first providing clear and conspicuous disclosure. . . and obtaining the user's consent. Additionally, S. 1625 would prohibit installation of software that "causes advertising windows to appear (popularly known as adware) unless: (1) the source is clear and instructions are provided for uninstalling the software; or (2) the advertisements are displayed only when the user uses the software author's or publisher's website or online service." This bill was referred to the Senate Committee on Commerce, Science, and Transportation on June 14, 2007. No further action has been taken.

[23] A protected computer is defined in this bill as " a computer used in interstate or foreign commerce or communication."

Appendix: Bills in the 108th and 109th Congresses

109th Congress

Two bills passed the House on May 23, 2005 — H.R. 29 (Bono) and H.R. 744 (Goodlatte) — both of which were very similar to legislation that passed the House in the 108th Congress.

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 and S. 1608 were ordered reported from the Senate Commerce Committee in 2005. 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. 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.

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.