Spyware: Background and Policy Issues for Congress

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

September 8, 2010

Congressional Research Service
7-5700
www.crs.gov
RL32706

CRS Report for Congress
Prepared for Members and Committees of Congress

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
08 SEP 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Spyware: Background and Policy Issues for Congress	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Congressional Research Service,The Library of Congress,101 Independence Avenue SE,Washington,DC,20540-7500**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**10**	

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. Additionally, the FTC has consumer information on spyware that includes a link to file a complaint with the commission through its "OnGuard Online" website.

Several states have passed spyware laws, but there is no specific federal law and no legislation has been introduced thus far in the 111th Congress.

Contents

Appendixes

Contacts

Background

The Anti-Spyware Coalition (ASC)[1] defines spyware as "technologies deployed without appropriate user consent and/or implemented in ways that impair user control over (1) material changes that affect their user experience, privacy, or system security; (2) use of their system resources, including what programs are installed on their computers; and/or (3) collection, use, and distribution of their personal or other sensitive information.[2]

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

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.[3] 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. 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.

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

[1] 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 perspectives on the problem of controlling spyware and other potentially unwanted technologies. Its 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.

[2] For examples of different types of spyware, see http://www.antispywarecoalition.org/documents/DefinitionsJune292006.htm.

[3] See CRS Report RL31953, *"Spam": An Overview of Issues Concerning Commercial Electronic Mail*, by Patricia Moloney Figliola.

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.

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.[4] 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.[5]

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).[6] 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.

A report on spyware law enforcement by the Center for Democracy and Technology (CDT) summarizes active and resolved spyware cases at the federal and state levels.[7] Additionally, the FTC maintains its own list of cases.[8]

---

[4] 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.

[5] For more on identity theft, see CRS Report RS22082, *Identity Theft: The Internet Connection*, by Marcia S. Smith; and CRS Report RL31919, *Federal Laws Related to Identity Theft*, by Gina Stevens.

[6] 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.

[7] The full report is available online at http://www.cdt.org/privacy/spyware/20071015SpywareEnforcement.pdf.

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.[9] The FTC has also issued a consumer alert about spyware that lists warning signs that might indicate a computer is infected with spyware.[10] 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.

(...continued)

[8] Available online at http://www.ftc.gov/bcp/edu/microsites/spyware/law_enfor.htm.

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

[10] Available online 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.[11] According to the National Conference of State Legislatures, by January 2009, at least 15 states had enacted spyware legislation: Alaska, Arizona, Arkansas, California, Georgia, Illinois, Indiana, Iowa, Louisiana, Nevada, New Hampshire, Rhode Island, Texas, Utah, and Washington.[12]

Legislative Action—111th Congress

No legislative action on spyware has taken place at this time.

Legislative Action—110th Congress

During the 110th Congress, two bills were introduced in the House of Representatives and one bill was introduced in the Senate; the House 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.[13] 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. 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,[14] and referred to the Senate Committee on Commerce, Science, and Transportation on June 7, 2007. No further action was taken.

[11] A preliminary injunction prevented it from taking effect, and the Utah legislature passed a new law in 2005 amending the 2004 act. Originally, 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).

[12] This information is online at http://www.ncsl.org/programs/lis/privacy/spywarelaws.htm.

[13] 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.

[14] H.Rept. 110-169.

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.[15] 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[16] 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[17] 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,[18] and then referred to the Senate Committee on the Judiciary on May 23, 2007. No further action was taken.

S. 1625—Counter Spy Act

The Counter Spy Act was introduced by Senator Pryor on June14, 2007. This bill would prohibit unauthorized installation on a protected[19] 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, and a hearing was held on June 11, 2008. No further action was taken.

[15] 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.

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

[17] 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.

[18] H.Rept. 110-169.

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

Additional Reading

Federal Trade Commission "Microsite" on Spyware [Web page]. Available online at http://www.ftc.gov/bcp/edu/microsites/spyware/index.html.

Anti-Spyware Coalition [Web page]. Available online at http://www.antispywarecoalition.org.

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.

Author Contact Information

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy
pfigliola@crs.loc.gov, 7-2508

Acknowledgments

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