Washington Journal of Law, Technology & Arts

Volume 2 | Issue 1 Article 1

8-12-2005

# Defining Spyware: Necessary or Dangerous

Andrew T. Braff

**Corporate & Commercial**
Cite as: Andrew T. Braff, *Defining Spyware: Necessary or Dangerous*, 2 Shidler J. L. Com. & Tech. 1 (Aug. 12, 2005), *at* <http://www.lctjournal.washington.edu/Vol2/a001Braff.html>

# DEFINING SPYWARE: NECESSARY OR DANGEROUS

By Andrew T. Braff[1]


## Abstract

State legislation attempting to define and proscribe *spyware* has been criticized for either being under-inclusive or over-inclusive. This article provides an overview of the technology that is commonly considered spyware and examines the potential effects of attempting to legislatively define and curtail spyware as a specific technology. It concludes that a more appropriate method to regulate spyware would focus on prohibiting conduct associated with placing monitoring software on a computer and enforcing existing law regarding such conduct.

## Table of Contents



## INTRODUCTION

<1> Studies show that as many as 90 percent of Internet-enabled U.S. home computers are infected with an average of 26 spyware programs.[2] Most users are unaware of the presence of such monitoring programs[3] until the computer begins malfunctioning or a 'dialer' program hijacks their modem, resulting in exorbitant phone bills.[4] Other victims of 'keystroke loggers'— software monitoring information entered onto a personal computer—learn their privacy has been compromised after the damage is done.[5]

<2> A solution to the spyware epidemic that does not prohibit beneficial technologies or turn the Internet into a maze of disclaimers, notices, and end user license agreements (EULAs) has proven elusive. Aside from bills in two states, [6] attempts to legislate a solution to spyware in 2004 temporarily stalled as states

awaited Congressional action, which did not occur in the waning days of the 108th Congress.[7] Although there is agreement on the harmful effects of this malicious software, a lack of action is largely attributable to intense disagreement over the precise definition of spyware—or whether to define it at all. For some, certain *technology* should be defined as spyware and then prohibited. Others emphasize that the *conduct* associated with the surreptitious or questionable installation of monitoring software on a user's computer should be prohibited. Many question whether a legislative solution is needed at all, claiming that enforcement mechanisms already exist to punish those disseminating such monitoring technology.

## OVERVIEW OF TECHNOLOGY

<3> Websites contain programming that defines the web page, causes a user's browser to display text and images, and instructs the browser to perform more complex functions (e.g. Java script or ActiveX controls). The latter is known as *active content*. Browsers, such as Microsoft's Internet Explorer (IE), Netscape Navigator, and Mozilla Firefox, interface with web servers hosting web pages, retrieve and display the requested pages, and run any active content associated with the site. Browsers also contain security features designed to protect the user from harmful content; therefore, they act as the gateway and first line of defense between a computer and the Internet.

<4> Spyware can appear on a computer in many ways. For instance, vulnerabilities in system software can be exploited. This was the case in *FTC v. Seismic*, in which the defendants exploited vulnerabilities in Microsoft's IE to circumvent default security settings designed to warn users when content was being downloaded.[8] Once a user visited a 'seed' web page, a series of processes occurred almost instantaneously. Active content was used to change the user's default web page to the seed web page, which contained script to restart this process each time the user opened IE. The seed page instructed the browser to retrieve additional pages advertising anti-spyware software that could not be closed. Other windows were opened containing script that altered the Windows registry and downloaded harmful active content without consent. These included *Trojan horse* programs, which periodically contact the Internet hosts and allow additional programs to be downloaded.[9]

<5> Another common method of distributing spyware is through *bundling*—the practice of combining a number of related or unrelated programs into a single installation. Bundling has increased as a way to disseminate software in mass quantities, to achieve exposure, and to reduce costs for the consumer. Peer-to-Peer (P2P) file sharing software has created fertile ground for those distributing spyware via bundling due to the volume of P2P software being

downloaded.[10] P2P developers receive significant revenue from those having their software bundled—including monitoring software. Bundling monitoring software poses complications for defining particular software as spyware because the user provides *consent* when downloading the programs. This consent, however, is questionably meaningful because of the growing length of EULAs and the corresponding likelihood that the user does not know exactly what is being downloaded.[11]

<6> The performance of a computer containing spyware may be dramatically reduced. A computer may function more slowly, there may be an inability to access the Internet, extra icons may appear, and the number of programs running simultaneously may result in system freezes and crashes.[12]

## DEFINING SPYWARE TO PROHIBIT THE TECHNOLOGY

<7> Passed in 2004, Utah's Spyware Control Act provides a definition of spyware and prohibits software meeting this definition; however, it does not necessarily punish the questionable conduct that places such technology on computers.

<8> Generally, the Utah Act defines *spyware* as software residing on a computer that possesses all of the following components:

- **Monitoring:** monitors the computer's usage; AND
- **Data Transmission and Display of Ads:** sends information about the computer's usage to a remote computer or server, OR displays an advertisement neglecting to identify its purveyor and uses a triggering mechanism to display the advertisement according to the Internet websites accessed by a user; AND
- **Consent and Notice Components:** does not obtain a user's consent via a fully disclosed, *plain language* license agreement providing notice of the information to be transmitted following installation, an example of advertisements that may be delivered, ad frequency, and a method describing how one purveyor's advertisements can be distinguished from another; AND
- **Removal:** does not provide a quick and easy method for removing the software without affecting non-affiliated parts of the user's computer.[13]

<9> Using this definition, the Act prohibits the installation of such software on another user's computer and the use of a "context based triggering mechanism to display an advertisement that partially or wholly covers … or interferes with a user's ability to view the Internet website."[14] Automatically minimizing or hiding a pop-

up advertisement behind the user's active browser window is not a defense.[15]

<10> The Utah Act exemplifies the problems associated with defining spyware as a technology in order to prohibit it. First, the Act considers *adware* to be a subset of spyware. Adware is software that serves banner ads or pop-up ads to a user while online, often in exchange for free Internet access. Some agree with this assessment, especially when sophisticated software monitors and collects personal information and activity to serve targeted ads.[16] Others disagree with classifying adware as spyware because adware endows the user with certain benefits and is characterized by some form of notice and consent.[17] Ultimately, the Act's prohibition of context-based advertising—despite the user consenting to such software—has proven fatal to its constitutionality under the Commerce Clause, and the Act remains enjoined.[18] However, Utah recently passed new spyware legislation in an attempt to remedy these defects.[19]

<11> Second, the definition encompasses beneficial software such as Net Nanny, Internet communications such as instant messaging, and pop-ups notifying users about legitimate needs such as software updates.[20] If these pop-ups partially cover or interfere with the user's ability to view another website, this statute would be violated.

<12> Third, the consent requirements are also broad, which may lead to cumbersome license agreements. Long license agreements tend to dilute meaningful consent since length can be used to mask questionable features of the program, given that the average user will accept the terms without reading the EULA. Additionally, requiring separate notice each time new information is transmitted could degrade a consumer's online experience—the very problem created by spyware itself.

<13> Finally, by relying on bright-line definitions, certain software may be excluded for good or ill. For instance, the Utah Act exempts *cookies*, which fit the definition outlined in the Act.[21] Cookies are bits of information sent by a web server and stored on a user's computer, enabling the visited website to customize material and recall preferences if visited in the future. On a more sensitive issue, they enable servers to track websites visited by a user and can be exploited by targeted marketers.

<14> The definitional approach to prohibiting technology is of great concern to industry because automatic downloads, surveillance, and resistance to uninstallation provide consumer benefits if done with notice and consent. For instance, an "across-the-board technical ability to uninstall on the part of the consumer could, in fact, leave them in worse situations."[22] Additionally, new technologies termed *supportware* could be considered spyware under the definitional approach taken by the Utah Act (2004). These are "software

technologies that update, renew, and monitor programs residing on the computer user's system to provide a better service to them and to enhance overall computer user satisfaction."[23]

## PROHIBITING CONDUCT

<15> The Federal Trade Commission (FTC) tentatively defined spyware as "[s]oftware that aids in gathering information about a person or an organization without their knowledge, and that may send such information to another entity without the consumer's consent, or that asserts control over computers without the consumer's knowledge."[24] This definition was largely accepted at the FTC's workshop *Monitoring Software on Your PC: Spyware, Adware, and Other Software* in order to talk about the issue; however, panelists were virtually unanimous in their reluctance to submit such a definition to legislation.[25]

<16> Instead of defining spyware, panelists preferred an approach taken by the Center for Democracy and Technology's (CDT) Working Group, whereby deceptive and devious behavior would be banned, rather than a defined technology.[26] These practices would include hijacking, surreptitious surveillance, and inhibiting termination or de-installation—all without *meaningful* notice or consent of the user.[27] Panelists expressed the common concern that defining and creating an "illegal category of product is very dangerous and has significant consequences."[28]

<17> Other legislation enacted or seriously considered following this conference has reflected this concern. Instead of defining and proscribing a particular type of software, authors of California's Consumer Protection Against Computer Spyware Act[29] chose to regulate conduct. This is also true of the federal legislation considered in the 108th Congress,[30] and related bills in the 109th Congress such as the SPY ACT (H.R. 29)[31] and the Internet Spyware Prevention Act (H.R. 744).[32] For instance, H.R. 29—the successor to H.R. 2929 in the 109th Congress—makes it unlawful to "engage in deceptive acts or practices" that involve nine general methods of conduct.[33] These methods include: 1) taking control of the computer; 2) modifying settings; 3) collecting personally identifiable information via keystroke logging programs; 4) inducing the owner to install software or preventing efforts to block installation; 5) misrepresenting the necessity of installing additional software components; 6) inducing software downloads by misrepresenting the source of the software; 7) inducing the owner to provide password or account information via misrepresentation; 8) interfering with a computer's defenses by removing or disabling security, anti-spyware, or anti-virus software; and 9) installing software components with the intent of causing a person to use such software in a manner that violates any of the above provisions.

Additionally, any information collection program may only be installed after the owner *opts-in* after clear, conspicuous notice is given in plain language and meets a litany of additional criteria.[34] H.R. 744, the successor to H.R. 4661 in the 108th Congress, creates additional crimes relating to unauthorized access of a computer and transmission of personal information with intent to defraud or impair the security protections of a computer. Both bills passed in the House of Representatives on May 23, 2005.[35]

<18> Prohibiting certain conduct is much easier for industry to accept, and many originally opposed to H.R. 2929 subsequently endorsed it and its successor, H.R. 29.[36] Still, there are several deficiencies. For instance, H.R. 29 fails to address the issue involving cookies, leaving this work to the FTC.[37] Ultimately, however, focusing on conduct rather than eliminating potentially beneficial technology is a legislative approach with fewer pitfalls—both legally and politically.

## LEGISLATIVE RESTRAINT IN FAVOR OF EXISTING LAW

<19> Short of guidelines codifying *acceptable notice*, the conduct discussed above is largely illegal under existing law. For instance, taking advantage of security holes and downloading software without consent (known as *drive-by downloading*) are already illegal under the Computer Fraud and Abuse Act (CFAA), provided certain damage thresholds are met.[38] This raises the question of whether federal legislation is really needed, other than to pre-empt differing state attempts to eliminate spyware.

<20> The FTC opposes legislative attempts to deal with spyware in favor of relying on existing legal tools and technological evolution. FTC commissioner Orson Swindle continues to assert that "[current] law is adequate…. Most, if not all, spyware is executed under a deceptive cloud. If people are deceived, it's a deceptive practice."[39] The problem with enforcement is not the absence of law, but rather the difficulty in finding purveyors of spyware.

<21> Commissioner Swindle's theory is currently being tested. After receiving a tongue lashing from Congress[40] and over 300 complaints from school districts, libraries, businesses, and individual computer users, the FTC commenced its first spyware prosecution[41] on October 12, 2004, citing violation of several sections of the Federal Trade Commission Act. The Act prohibits unlawful acts related to "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce," as well as false advertising "likely to induce, directly or indirectly, the purchase of … devices, [or] services."[42] These are broad statutes, and how federal legislation in the 109th Congress may change legal regimes regarding the victimization of private citizens

on the Internet will be addressed in a forthcoming publication.



## CONCLUSION

<22> The Internet has created a lexicon for the 21st Century, but generating an acceptable legislative definition of spyware has proven unattainable. On the state front, Utah's 2004 law evidences the dangers of a definitional approach. It is too early to determine the impact of other state laws enacted in California, Virginia, and Washington, the latter of which will not enter force until the end of July. Although federal legislation stalled in the lame duck session, the debate remains at the forefront given its resurrection and passage early in the 109th Congress. Despite some uncertainty on the legislative front, the potential outcomes legislative action could bring, coupled with the toll that spyware has taken on their own balance sheets, has provided industry with a reason to pursue self regulation.[43] Should the FTC prove that adequate enforcement mechanisms are available, the legal and technological efforts currently underway may render legislation and a definition of spyware superfluous.

<< Top

## FOOTNOTES

1. Andrew T. Braff, University of Washington School of Law, Class of 2006, abraff@u.washington.edu.

2. *Fast and Present Danger: In-home Study on Broad Band Security Among American Consumers*, National Cyber Security Alliance, June 2003, *available at* http://www.staysafeonline.info/press/060403.pdf; John Borland, *Dell backs spyware education drive*, CNET News.com, 10/15/04, http://news.com.com/2100-1032_3-5410568.html (last visited Jan. 2, 2005); *Earthlink finds spyware running amok*, CNET News.com, 10/05/04, http://news.com.com/2100-1032_3-5397333.html (last visited Jan. 2, 2005).

3. Rob Cheng and Dave Methvin, *Lack of Consent: A Survey of Gain Users*, PCPitstop.com 1 (2004), *at* http://www.ftc.gov/os/comments/spyware/040315pcpitstop.pdf (last visited Jan. 2, 2005); Dave Methvin, *Eighty-Seven Percent of WhenU Users Are Unaware They Are Using It*, PCPitstop.com (2004), *at* http://www.ftc.gov/os/comments/spyware/040413pcpitstop.pdf (last visited Jan. 2, 2005).

4. See *Monitoring Software on Your PC: Spyware, Adware, and Other Software*, FTC Public Workshop, 74 (Apr. 19, 2004), *available at*

http://www.ftc.gov/bcp/workshops/spyware/ (last visited Jan. 2, 2005).

5. Ray Everett-Church, Remarks, *Monitoring Software on Your PC, supra* note 4 at 122.

6. Anti-spyware legislation has been has passed in Utah and California in 2004, and Virginia and Washington in 2005. Spyware Control Act, 2004 Utah Laws ch. 363 (2004) (codified at Utah Code Ann. § 13-40-101 (2004)); Consumer Protection Against Computer Spyware Act, 2004 Cal. Legis. Serv. ch. 843 (codified at 8 Bus. & Prof. §§ 22947-22947.6 (2004)); Act Relating to Computer Crimes, Virginia Laws ch. 812 (2005); Act Regulating Computer Spyware, ch. 500 (2005) (to be codified at Wash. Rev. Code Tit. 19). As of May 2005, other states with spyware legislation pending include Alabama, Alaska, Arizona, Arkansas, California, Florida, Georgia, Illinois, Indiana, Kansas, Maryland, Massachusetts, Michigan, Missouri, Nebraska, New Hampshire, New York, Oregon, Pennsylvania, Rhode Island, Tennessee, Texas, West Virginia. For more information, see *2005 State Legislation Relating to Internet Spyware or Adware*, National Conference of State Legislatures, *at* http://www.ncsl.org/programs/lis/spyware05.htm (last visited May 26, 2005).

7. Securely Protect Yourself Against Cyber Trespass Act ("SPY ACT"), H.R. 2929, 108th Cong. (2004). H.R. 2929 passed the House of Representatives on October 5, 2004 by a vote of 399-1. 150 Cong. Rec. H8130 (Oct. 5, 2004); Internet Spyware (I-SPY) Prevention Act of 2004, H.R. 4661, 108th Cong. (2004). H.R. 4661 passed the House of Representatives on October 7, 2004 by a vote of 415-0 (Roll No. 503). 150 Cong. Rec. H8649 (Oct. 7, 2004). No further action was taken on this legislation in the Senate.

8. See *FTC v. Seismic Entm't Prod., Inc., Smartbot.net, Inc., and Sanford Wallace,* Civ. No. 04-377-JD "Temporary Injunction Order" at *3-4 (D.N.H. 2004), *available at* http://www.cdt.org/privacy/spyware/spywiper/20041021seismicorder.pdf (last visited Jan. 2, 2005). For the court's rationale ("Order"), see http://www.cdt.org/privacy/spyware/spywiper/20041021seismicruling.pdf (last visited Jan. 2, 2005). The FTC's "Complaint" and "Memorandum in Support of Plaintiff's Motion for a Temporary Restraining Order" are *available at* http://www.ftc.gov/os/caselist/0423142/0423142.htm (last visited Jan. 2, 2005).

9. Declaration of Steven D. Gribble, *FTC v. Seismic Entm't Prod., Inc., Smartbot.net, Inc., and Sanford Wallace*, Civ. No. 04-377-JD (D.N.H. 2004). For other examples, see generally Stefan Saroiu, Steven D. Gribble, and Henry M. Levy, *Measurement and Analysis of Spyware in a University Environment*, Paper, Networked Systems Design and Implementation Symposium (Mar. 2004), *available at* http://www.cs.washington.edu/homes/gribble/papers/spyware.pdf (last visited Jan. 2, 2005).

10. See Center for Democracy and Technology, Comment, *Peer-to-Peer File-Sharing*, FTC Public Workshop 4 (Dec. 15-16, 2004), *available at* http://www.cdt.org/copyright/20041115cdt.pdf (last visited Jan. 2, 2005). Workshop transcript *available at* http://www.ftc.gov/bcp/workshops/filesharing/ (last visited Jan. 2, 2005).

11. Ari Schwartz, Remarks, *Monitoring Software on Your PC*, *supra* note 4 at 45. See Benjamin Edelman, *WhenU License Agreement is Forty Five Pages Long*, Apr. 2004, http://www.benedelman.org/spyware/whenu-license/ (last visited Jan. 2, 2005); Benjamin Edelman, *Claria License Agreement is Fifty Six Pages Long*, June 2004, http://www.benedelman.org/spyware/claria-license/ (last visited Jan. 2, 2005).

12. Maureen Cushman, Remarks, *Monitoring Software on Your PC*, *supra* note 4 at 70-71. See also Benjamin Edelman, *Methods and Effects of Spyware*: *Response to FTC Call for Comments*, Mar. 19, 2004, http://www.benedelman.org/spyware/ftc-031904.pdf (last visited Jan. 2, 2005).

13. Utah Code Ann. 1953 § 13-40-101 (West 2004).

14. *Id.* at § 13-40-201(1).

15. *Id.* at § 13-40-201(2).

16. See Edelman, *Methods and Effects of Spyware*, *supra* note 12 at 3.

17. See Avi Naider, Remarks, *Monitoring Software on Your PC*, *supra* note 4 at 32-34.

18. *WhenU.com v. Utah*, Case No. 040907578 (Utah Dist. Ct. 2004), *available at* http://www.benedelman.org/spyware/whenu-utah/pi-ruling-transcript.pdf (last visited Jan. 2, 2005).

19. Spyware Control Act, 2005 Utah Laws ch. 168 (2005), *available at*

http://www.le.state.ut.us/%7E2005/htmdoc/hbillhtm/HB0104S02.htm (last visited May 26, 2005).

20. Mark Bohannon, Remarks, *Monitoring Software on Your PC*, *supra* note 4 at 23-5.

21. Utah Code Ann. 1953 § 13-39-102(5).

22. Mark Bohannon, *supra* note 20 at 58-9.

23. Letter from Harris N. Miller, Information Technology Association of America, to Chairman Joe Barton and Ranking Member John Dingell, House Comm. on Energy and Commerce (June 23, 2004), http://www.itaa.org/news/gendoc.cfm?DocID=419 (last visited Jan. 2, 2005).

24. 69 Fed. Reg. 8538-01 (Feb. 24, 2004), *available at* 2004 WL 329224.

25. Mark Bohannon, *supra* note 20.

26. Center for Democracy & Technology, Consumer Software Working Group, white paper (2004), *available at* http://www.cdt.org/privacy/spyware/20040419cswg.pdf (last visited Jan. 2, 2005).

27. *Id.* at 2-3.

28. Edward Black and Ron Plesser, Remarks, *Monitoring Software on Your PC*, *supra*, note 4 at 18-19, 124-5.

29. 2004 Cal. Legis. Serv. Ch. 843 (codified at 8 Bus. & Prof. §§ 22947-22947.6).

30. See H.R. 2929 and H.R. 4661, *supra* n. 7.

31. Securely Protect Yourself Against Cyber Trespass Act ("SPY ACT"), H.R. 29, 109th Cong. (2005) [hereinafter "SPY ACT"]. For Congressional testimony relating to the reintroduced bill, see *Combating Spyware: H.R. 29, the Spy Act: Hearings Before the House Comm. on Energy and Commerce*,109th Cong. (Jan. 26, 2005) (statements of Mr. David N. Baker, Mr. Howard A. Schmidt, Mr. Ari Schwartz, Mr. Ira Rubinstein) *available at* 2005 WL 65901263, 65901264, 65901271, 65901272.

32. Internet Spyware (I-SPY) Prevention Act of 2005, H.R. 744, 109th Cong. (2005).

33. SPY ACT (2005), at Sec. 2(a).

34. *Id.* at Sec. 3.

35. H.R. 29 passed by a vote of 393-4 (Roll No. 201). 151 Cong. Rec. H3705-3708 (May 23, 2005), and H.R. 744 passed by a vote of 395-1 (Roll No. 200). 151 Cong.

Rec. H3703 (May 23, 2005). Legislation is also pending in the Senate. See also SPY BLOCK Act, S. 687, 109th Cong. (2005).

36. See Letter from the Software Information Industry Association to Chairman Joe Barton and Ranking Member John Dingell, House Comm. on Energy and Commerce (June 23, 2004), *reprinted at* 150 Cong.Rec. H8086-H8088 (Oct. 5, 2004), *available at* http://www.siia.net/govt/docs/pub/CSWGletter%2023%20June%202004. (last visited Jan. 2, 2005).

37. SPY ACT (2005), at Sec. 8.

38. 18 U.S.C. § 1030(a)(2), (a)(5)(B)(i), (g) (2004).

39. Roy Mark, *FTC to Congress: Lose the Anti-Spyware Plans*, Internetnews.com (Nov. 5, 2004), http://www.internetnews.com/xSP/article.php/3432111 (last visited Jan. 2, 2005), quoting FTC Commissioner Orson Swindle to Capitol Hill staffers at a Nov. 5, 2004, Cato Institute seminar.

40. *Hearing on Spyware Before the House Comm. on Energy and Commerce: Subcomm. on Commerce, Trade, and Consumer Protection*, 108th Cong. 23-25 (2004), *available at* 2004 WL 939323; Declan McCullagh, *FTC officials blast spyware measures*, CNET News.com, 04/29/04, http://news.com.com/2100-1023_3-5202016.html.

41. See *Seismic Entertainment*, *supra* note 8.

42. 15 U.S.C. §§ 45(a)(1), 52.

43. Jack M. Germain, *Dell Spyware Decision Spurs New Trend*, E-Commerce Times (11/01/04), *at* http://www.ecommercetimes.com/story/37668.html (last visited Jan. 2, 2005).

<< Top