COMMENT

THERE OUGHTA BE A LAW: CRAFTING EFFECTIVE WEAPONS IN THE WAR AGAINST SPYWARE*

TABLE OF CONTENTS

---

* This Comment received the Vinson & Elkins, L.L.P. Award for the best paper in an emerging area of law.

The following scenario is all too familiar for most Internet users: A consumer turns on her computer, but it loads more slowly than usual. She launches her web browser and notices an unfamiliar toolbar near the top of the screen. The buttons on the toolbar link to gambling, file sharing, and pornography sites. She stares at it, wondering where it came from because she does not remember downloading it. She looks for a way to remove the toolbar, but it is not listed as a program that she can uninstall. Then an advertisement pops up, covering her screen. The consumer's machine has become infected with software she did not request; she does not know who put it there or what it might be doing, and she cannot remove it. In short, her computer has spyware,[1] and she is hardly alone. Estimates say as many as eighty percent of computers are infected with spyware.[2]

Spyware is more than a mere nuisance. It monitors the websites a consumer visits and reports that information to third parties.[3] It fills the screen with advertisements, changes the

---

1. ED TITTEL, PC MAGAZINE: FIGHTING SPYWARE, VIRUSES, AND MALWARE 9 (Chris Webb et al. eds., 2d ed. 2005) (listing the most common symptoms exhibited by computers infested with spyware, including new toolbars, increased pop-ups, and performance degradation).

2. Dan Tynan & Tom Spring, *The Hidden Money Trail*, PC WORLD, Nov. 2005, at 71, 78 (citing RICHARD STIENNON & PAUL PICCARD, STATE OF SPYWARE 12 (2d quarter ed. 2005), *available at* http://www.webroot.com/pdf/2005-q2-sos.pdf).

3. *See* TITTEL, *supra* note 1, at 6–8. "[S]pyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties." *Id.* at 7. (quoting Whatis.com, Spyware – A Definition from Whatis.com, http://searchcrm.techtarget.com/sDefinition/0,,sid11_gci214518,00 (last visited Sept. 20, 2006)). A Microsoft webpage lists a user's browsing history as one type of information gathered by spyware. *Id.* at 8. (citing Microsoft, What Is Spyware?, http://www.microsoft.com/athome/security/spyware/spywarewhat.mspx (last

default homepage, and adds its own preferred websites to the browser's list of favorites.[4] It silently downloads other programs and installs them without permission, taking up system resources and slowing down the computer.[5] It resists removal.[6] Sometimes it causes the computer to malfunction.[7] All the while, it makes Internet advertising companies very wealthy.[8]

This Comment analyzes the nature of spyware, its effect on consumers, and current efforts within the legal community to bring the problem under control. Part I provides the background to this issue by discussing the nature of spyware, why it exists, and how it arrives on consumers' machines. Parts II and III analyze, respectively, the state and federal approaches to addressing spyware. These Parts explain why the current and pending legislation do not adequately address the abuses of spyware. Part IV reviews existing causes of action that may be used against spyware by discussing several lawsuits brought by the Federal Trade Commission and individual consumers. Part V concludes that spyware demands strong federal laws and recommends provisions that could be effective. Bear in mind that this Comment provides only a snapshot of a fast-moving target. As one judge noted, the Internet is "one of the most fluid, rapidly developing, and virtually daily changing areas of commerce that the law has had to focus upon and endeavor to apply established principles to."[9]

I. BACKGROUND

A. Defining Spyware

Unfortunately, no single, comprehensive, uniform definition of spyware exists. One bill submitted to the Massachusetts House of Representatives used two pages to define what does and does

---

visited Sept. 20, 2006)).

4. *See* Tynan & Spring, *supra* note 2, at 74 (describing the ill effects of a tested spyware application).

5. TITTEL, *supra* note 1, at 9.

6. *See* Tynan & Spring, *supra* note 2, at 74 (describing CoolWebSearch, a spyware application tested by the authors, as an example of spyware that resists uninstallation).

7. *See* TITTEL, *supra* note 1, at 9 (stating, specifically, that spyware may cause the computer to crash, become unstable, or lose important system files or documents).

8. *See, e.g.*, Tynan & Spring, *supra* note 2, at 72 (estimating that adware and spyware companies earn between $200 million and $2 billion per year in revenue and lamenting the continued "bullish" investment in the companies creating the adware and spyware).

9. ImOn, Inc., v. ImaginOn, Inc., 90 F. Supp. 2d 345, 346 (S.D.N.Y. 2000).

not fall within the scope of spyware.[10] California's Consumer Protection Against Computer Spyware Act, on the other hand, does not define spyware at all.[11] The Federal Trade Commission (FTC) attempted to define spyware at a workshop in 2004,[12] but differences of opinion over issues such as notice and consent, the software's behavior, and the nature and extent of the harm it must cause thwarted the FTC's efforts.[13]

Narrowly, spyware may be defined as any software that monitors and reports a consumer's browsing habits or other personal information to another computer or person without adequate consent.[14] By this definition, software that monitors a consumer's browsing habits to deliver contextually relevant advertisements ("adware") is spyware only if the program reports the information and does not provide notice or obtain consent before installing.[15] Using a more broad definition, spyware can mean software that has some combination of undesirable characteristics other than spying, including (1) installing without the consumer's knowledge or consent; (2) modifying the consumer's settings without knowledge or consent; (3) hiding from the consumer; and (4) resisting reasonable attempts at removal.[16] Because the above characteristics constitute the types of behaviors that antispyware legislation attempts to curtail, this Comment adopts the more general definition.[17]

---

10. H.B. 3739, 184th Gen. Court (Mass. 2005).

11. *See* Consumer Protection Against Computer Spyware Act, CAL. BUS. & PROF. CODE § 22947 (West Supp. 2006). Although the word "spyware" is in the Act's title, and the Act prohibits software activities consistent with spyware, the Act declines to define the term explicitly. *See id.*

12. *See* FED. TRADE COMM'N, SPYWARE WORKSHOP: MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE 2–4 (2005), http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf.

13. *Id.* at 3. For purposes of the workshop, the committee formed a working definition of spyware as "'software [. . .] that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.'" *Id.* at 4 (quoting FED. TRADE COMM'N, PUBLIC WORKSHOP: MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE, 69 Fed. Reg. 8538 (Feb. 24, 2004), *available at* http://www.ftc.gov/os/2004/02/040217spywareworkshopfrn.pdf).

14. *See* AARON HACKWORTH, US-CERT, SPYWARE 2 (2005), http://www.us-cert.gov/reading_room/spyware.pdf ("For a program to qualify as spyware it must collect data without the data owner's knowledge or consent and must deliver or make it available in some way to an unauthorized party.").

15. *See id.*; *see also* Tynan & Spring, *supra* note 2, at 72 (discussing whether adware is spyware and concluding it depends on whom is asked).

16. *See, e.g.*, Consumer Protection Against Computer Spyware Act, CAL. BUS. & PROF. CODE § 22947.2 (West Supp. 2006) (prohibiting unauthorized users from installing software with these behaviors).

17. Not all software with these behaviors spies on a consumer, so a more general

Even using this broad definition, however, some software eludes easy classification. Consider a program that offers the ability to prevent others from cheating during multiplayer games on the Internet in exchange for an agreement that the sponsoring company may monitor any data it pleases on that computer. Could such a program be classified as spyware for looking at data beyond what is necessary to prevent cheating? What about software that prevents illegal copying of a music CD but hides itself so that the consumer would not be able to see it? The following sections examine two examples of controversial software, illustrating the challenges in defining the boundaries of spyware.

1. PunkBuster. PunkBuster is software that purports to help stop cheating in certain online, multiplayer games.[18] According to its website, PunkBuster prevents cheating by scanning a player's computer for known exploits,[19] but the program's End User License Agreement (EULA) states it can do much, much more:

> Licensee understands that PunkBuster software inspects and reports information about the computer on which it is installed to other connected computers and Licensee agrees to allow PunkBuster software to inspect and report such information about the computer on which Licensee installs PunkBuster software. Licensee understands and agrees that the information that may be inspected and reported by PunkBuster software includes, but is not limited to, devices and any files residing on the hard-drive and in the memory of the computer on which PunkBuster software is installed. Further, Licensee consents to allow PunkBuster software to transfer actual screenshots taken of Licensee's computer during the operation of PunkBuster software for possible publication.[20]

---

term such as "unsolicited software" might be more appropriate than "spyware." However, legislators generally designate statutes that prohibit unsolicited software as antispyware statutes. *See, e.g., id.* (bearing the title "Consumer Protection Against Computer Spyware Act" although some of the practices prohibited are not in the nature of spying).

18. *See* PunkBuster Online Countermeasures, http://www.punkbuster.com/index.php?page=info.php (last visited Sept. 20, 2006) (explaining that the software is designed to stop cheating in games played over the Internet against other players).

19. *Id.* An "exploit" refers to instances in which a programmer takes advantage of a vulnerability in a program's code in order to cheat or gain access beyond what the authors of the program intended. *See* TITTEL, *supra* note 1, at 31–32 (defining the term "exploit" as "a documented case in which a vulnerability has been used (or exploited, if you will) to make an attack successful").

20. Maztopia, PunkBuster Anticheat a Rootkit, http://www.maztopia.org/2006/04/29/punkbuster-anticheat-privacy-invasion (last visited Sept. 20, 2006) (emphasis omitted).

Based on the above text, PunkBuster may share financial records, family photos, online chat sessions, and any other information stored on the computer with anyone on the Internet.[21] Instinctively, many consumers would label such a program as spyware, if for no other reason than the overly broad scope.[22] However, the program's creators argue that it is not spyware because "[t]he activities performed by PunkBuster are generally described on our website and we have also developed and published a Privacy Policy Statement."[23] Indeed, the United States Computer Emergency Readiness Team (US-CERT), a division of the Department of Homeland Security, published an article that expressly excludes from its definition of spyware any program that provides the user notice of the software's data collection activities through a clear privacy policy.[24] Thus, as outrageously invasive as PunkBuster may be, organizations like US-CERT would not consider it spyware.

2. The Sony BMG Rootkit. Music industry giant Sony BMG recently created a furor by installing a rootkit on consumers' computers.[25] Rootkits are utilities that can be used to hide malicious programs from consumers in an attempt to prevent detection and removal.[26] News of this rootkit initially broke after Mark Russinovich, a noted authority on Microsoft Windows

---

The End User License Agreement (EULA) is not published on the PunkBuster website, http://www.punkbuster.com, but has been posted to various forums by alert and incredulous users. *See, e.g.*, *id.*; Posting of LionsPhil to http://ars.userfriendly.org/cartoons/read.cgi?id=20050930&tid=1809885 (Sept. 30, 2005, 16:37). Even Balance, Inc., the maker of PunkBuster, assures consumers it will not modify any files without permission or "perform 'hard disk scans' looking through large portions of users' directories and/or file systems." Privacy Policy of Even Balance, Inc., http://www.evenbalance.com/index.php?page=privacy.php (last visited Sept. 20, 2006).

21. *See* Maztopia, *supra* note 20.

22. *See* Anti-Spyware Coalition, Definitions and Supporting Documents (Oct. 27, 2005), http://www.antispywarecoalition.org/documents/20051027definitions.pdf (defining "spyware," in its broader sense, as "[t]echnologies deployed without appropriate user consent and/or implemented in ways that impair user control over . . . [c]ollection, use, and distribution of [the user's] personal or other sensitive information").

23. PunkBuster for Players, http://www.evenbalance.com/publications/cod-pl (last visited Sept. 20, 2006).

24. *See* HACKWORTH, *supra* note 14, at 2 ("Software installed after the user has viewed and agreed to a clear privacy policy or to an EULA that describes the data collection activities *does not* meet the definition of spyware described in this paper."); US-CERT: About Us, http://www.us-cert.gov/aboutus.html (last visited Sept. 20, 2006) (supplying background information about US-CERT).

25. *See* Tom Zeller, Jr., *The Ghost in the CD*, N.Y. TIMES, Nov. 14, 2005, at C1 ("[I]n [Sony BMG's] haste to stop consumers from ripping and burning CD's, a hornet's nest has been stirred.").

26. GREG HOGLUND & JAMES BUTLER, ROOTKITS: SUBVERTING THE WINDOWS KERNEL 4 (2006).

technology, scanned his computer for rootkits and found one.[27] He determined it came from his compact disc (CD) of Van Zant's album *Get Right with the Man*.[28] The CD contained copyright protection technology that required the installation of special software in order to play the CD on a computer.[29] That installation also placed the rootkit on his computer to hide certain components.[30] The rootkit hid all files, directories, registry keys, and processes with the prefix "sys."[31] He could not find any means of uninstalling the rootkit short of locating and deleting the files and registry keys himself[32]—a potentially hazardous technique beyond the capacity of the average computer user.[33] Litigants filed more than twenty lawsuits against Sony BMG, prompting the company to stop using the technology and provide consumers replacement CDs without the rootkit.[34]

While PunkBuster fails the strict test for spyware because the program obtains consumer consent, the Sony BMG rootkit arguably fails the same test because the rootkit does not report information to unauthorized parties. Nevertheless, some experts consider both programs spyware: PunkBuster, because it monitors information on the computer,[35] and the Sony rootkit, because it hides software from the consumer.[36]

---

27. *See* Mark's Sysinternals Blog, Sony, Rootkits and Digital Rights Management Gone Too Far, http://www.sysinternals.com/blog/2005_10_01_archive.html (Oct. 31, 2005) [hereinafter Russinovich, *Rootkits*]; Sysinternals Freeware – About Us, http://www.sysinternals.com/AboutUs.html (last visited Sept. 20, 2006) (discussing Mark Russinovich's technical expertise and the website he created). Analogous to the more familiar antivirus scan, a rootkit scan uses software to read through a computer's system looking for evidence of a rootkit and alerts the consumer if one is found. HOGLUND & BUTLER, *supra* note 26, at 298.

28. Russinovich, *Rootkits*, *supra* note 27.

29. *Id.*

30. *Id.*

31. *Id.* Registry keys are configuration settings that control the Windows operating system. *See* MICROSOFT WINDOWS XP PROFESSIONAL: RESOURCE KIT DOCUMENTATION 1451 (Juliana Aldous & Maureen Williams Zimmerman eds., 2001) [hereinafter MICROSOFT WINDOWS XP PROFESSIONAL] (explaining that the registry editor can be used to modify registry keys to configure certain settings for Windows). "A process is an instance of an application." *Id.* at 1336.

32. Russinovich, *Rootkits*, *supra* note 27.

33. Incorrectly editing the registry can lead to system instability or inoperability. *See* MICROSOFT WINDOWS XP PROFESSIONAL, *supra* note 31, at 1451.

34. *See* Associated Press, *Sony BMG Tentatively Settles Suits on Spyware*, N.Y. TIMES, Dec. 30, 2005, at C4.

35. *See* Maztopia, *supra* note 20 and accompanying text (discussing the overly broad license the EULA provides PunkBuster).

36. *See* eTrust Spyware Encyclopedia - XCP.Sony.Rootkit, http://www3.ca.com/securityadvisor/pest/pest.aspx?id=453096362 (last visited Sept. 20, 2006) (profiling the

B. Why Spyware Is a Problem

The Federal Trade Commission believes consumers have the right to decide whether software will be installed on their computers.[37] Spyware may compromise a computer's security and expose a consumer's private data—such as logon names and passwords, credit card numbers, and browsing habits.[38] Even traditional security measures such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), or Virtual Private Networks (VPNs) provide no protection against spyware installed on a consumer's machine.[39] Furthermore, unsolicited software can cause system instability or drain system resources to the extent that the machine becomes unusable.[40]

Any program that hides itself creates still more concerns for the consumer. First, it takes control of the computer away from the consumer. Programs that encounter errors due to spyware sometimes cause other programs to stop responding as well.[41] Consumers familiar with this problem have multiple terms for it, saying the computer is "frozen" or "hung."[42] Often a consumer experiencing this problem can use a special program called Task Manager to end the unresponsive program.[43] If the program causing the problem is hidden, the consumer will not have the

---

Sony rootkit program in a database of spyware programs).

37. *See Prepared Statement of the Federal Trade Commission on Spyware: Hearing Before the Subcomm. on Trade, Tourism, and Econ. Dev. of the S. Comm. on Commerce, Sci. & Transp.*, 109th Cong. 4 (Oct. 5, 2005) (statement of Federal Trade Commission Chairman Deborah Platt Majoras) [hereinafter *Majoras Statement*] ("The Commission's spyware law enforcement actions reaffirm the principle that consumers have the right to decide whether to install new software on their computers."). Others express this same view in significantly more colorful language. *See* Harry McCracken, *Rule One: They're Our Machines*, PC WORLD, Nov. 2005, at 17 (comparing spyware companies to "[r]andom nosy strangers" who "acted like it [was] their birthright to barge into your office or home at will").

38. HACKWORTH, *supra* note 14, at 4.

39. *See id.* at 4–5. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are two common methods used on the Internet to establish a secured communications link between the browser and the server, so anyone who intercepts the signal will receive unreadable, encrypted data. *See id.* Virtual Private Networks (VPNs) are a more sophisticated solution for secure communications where the consumer's computer runs a special application that encrypts all traffic between the computer and the server—not just data handled by the browser. *See* MICHAEL A. GALLO & WILLIAM M. HANCOCK, NETWORKING EXPLAINED 185–86 (1999) (explaining and discussing VPNs as a means of securely connecting satellite offices through the Internet).

40. *See* HACKWORTH, *supra* note 14, at 7 (discussing how poorly written spyware programs can cause the computer system to become unstable).

41. *See id.*

42. DAN GOOKIN, TROUBLESHOOTING YOUR PC FOR DUMMIES 10 (2d ed. 2005).

43. *See, e.g.*, MICROSOFT WINDOWS XP PROFESSIONAL, *supra* note 31, at 1464–65 (explaining the use of Task Manager).

ability to terminate it using the Task Manager.[44] The consumer may be forced to reboot, possibly resulting in data loss.[45] Second, a hidden program impedes the consumer's ability to perform informed troubleshooting. Every process that runs on a computer takes up some memory and system resources.[46] When a consumer closes a program, the related processes are supposed to release those resources for other programs to use.[47] A program that fails to close affects system performance by wasting resources that other programs could use.[48] Because each computer has a finite amount of system resources, wasting them causes slower response time or system instability.[49] A consumer needs to be able to see and monitor installed programs to deal with these problems when they arise.[50] Hiding the program interferes with that vital step in the troubleshooting process. Third, a hidden program can create a vulnerability.[51] The Sony BMG rootkit, for example, indiscriminately hides all files with the prefix "sys", making it possible for hackers to conceal other files and programs on consumers' machines simply by naming them with a sys prefix.[52]

Finally, the struggle against spyware and adware costs consumers and companies time and money. Removing unwanted software from computers may take hours, and it is often easier to

---

44. *Cf.* Mark's Sysinternals Blog, *More on Sony: Dangerous Decloaking Patch, EULAs and Phoning Home*, http://www.sysinternals.com/blog/2005_11_01_archive.html, (Nov. 4, 2005) (pointing out that "there's no way to remove, update or even identify hidden software that's crashing your computer").

45. *See* HACKWORTH, *supra* note 14, at 7 (explaining that poorly written spyware programs may cause the system to crash often or become unstable, "resulting in potential . . . data loss"); *cf.* GOOKIN, *supra* note 42, at 146 (explaining that restarting Windows is an effective way to troubleshoot an unresponsive program).

46. GOOKIN, *supra* note 42, at 146.

47. *See id.* at 150. When a closed program does not release memory as it should, it is said to have a memory leak. *Id.*

48. *See id.* (explaining that a program causing a memory leak "uses up all the memory in the computer and everything stops").

49. *See id.*; *see also* HACKWORTH, *supra* note 14, at 7 ("By monitoring and reporting user activity, spyware consumes system resources as well as network bandwidth. Depending on the number of spyware components loaded on a system and their functionality, users may experience significant performance degredation.").

50. *See* GOOKIN, *supra* note 42, at 146–49.

51. *See, e.g.*, TITTEL, *supra* note 1, at 348 (defining a vulnerability as "[a] design flaw, programming error, or some kind of inherent weakness in a software implementation, application, or operating system that malware can exploit").

52. *See* Russinovich, *Rootkits*, *supra* note 27 (suggesting the possibility that hackers would use the sys prefix to hide programs by explaining the process that he underwent to rid his computer of the rootkit); *see also* HOGLUND & BUTLER, *supra* note 26, at 13 ("Although a rootkit is not an exploit, it may be employed as a part of an exploit tool (for example, in a virus or spyware).").

reformat and reinstall an infected computer than to clean it.[53] Consumers without the expertise to troubleshoot the problem on their own must pay someone else to do it for them, resulting in financial expense and hours or even days without computer access.[54]

C. The Spyware Business Model

The spyware trail begins when retail or service companies hire Internet advertising brokers.[55] Brokers then engage adware companies such as Claria or WhenU to disseminate the retail or service companies' advertising on the Internet via adware programs.[56] These adware companies in turn hire affiliates, who agree to promote and distribute the adware companies' adware in exchange for a fee.[57] These affiliates have their own websites where they place advertising for the adware company's adware; the affiliates also purchase "keyword based ads on search engines" and distribute the adware in a bundle with useful or attractive software that the affiliate offers.[58] Once installed, the adware will deliver advertisements to the consumer's desktop based on the consumer's browsing activity.[59] Interested consumers will click on the advertisements and be taken to the website of the retail or service company who originally hired the Internet advertising broker.[60] This event is called a "clickthrough," and the affiliate is paid based on its clickthrough rate.[61] The more spyware the affiliate distributes, the more clickthroughs it will generate, resulting in increased revenue.[62] Some affiliates are thus tempted to ignore any

---

53. Tynan & Spring, *supra* note 2, at 71–72. (reporting that an interviewed CPA estimated his cost of spyware removal, including lost productivity, at almost $5,000); HACKWORTH, *supra* note 14, at 7 (commenting that "wiping the system clean and starting over" is sometimes employed to rid a machine of spyware).

54. *See* Tynan & Spring, *supra* note 2, at 71–72 (detailing one woman's loss of time and money, attributable to adware).

55. *Id.* at 72, 74.

56. *Id.*

57. *Id.* at 72–74.

58. *Id.* Sometimes the adware companies themselves will offer useful software with which they will distribute their own adware; the Gator eWallet is an example. *See id.* at 72; *infra* note 65. The "bundle" of software programs offered by the affiliates might include items such as free icons, screensavers, or other downloadable software. Tynan & Spring, *supra* note 2, at 72–73.

59. *See* Tynan & Spring, *supra* note 2, at 71–74 (giving several examples of adware causing multiple pop-up ads to appear).

60. *Id.* at 74.

61. *See* Whatis.com, What is Advertising Terminology on the Internet?, http://whatis.techtarget.com/definition/0,289893,sid9_gci211535,00.html (last visited Sept. 20, 2006) (defining "clickthrough").

62. *Cf.* Annalee Newitz, *Don't Call It Spyware*, WIRED MAGAZINE, http://www.wired.com/wired/archive/13.12/spyware_pr.html (last visited Sept. 20, 2006)

rules the broker might have against stealth installs, becoming "rogue affiliates."[63]

1. Claria Case Study. The Claria Corporation presents an interesting, concrete example of how an Internet advertising company works. The company started as the Gator Corporation in 1998.[64] According to Claria's website, the software that the company provides through its advertising division, GAIN, revolutionized online advertising through "behavioral marketing and personalization technology."[65] Claria counts among its clients millions of consumers and over a thousand advertisers.[66] The company offers advertising on the Internet through the use of pop-up ads.[67] Citing its "unique permission-based relationship with tens of millions of users," Claria claims directed advertising yields "double-digit click and conversion rates—up to 20 to 40 times higher than traditional banner ads."[68]

The concept is simple enough. Consider, for example, a consumer who browses the websites of clothing retailers. That consumer is presumably interested in buying clothes online. Therefore, that consumer would be more likely to follow a pop-up ad

---

(describing the role of clickthroughs in the Internet advertising business model, noting that "[w]henever a user clicked on an ad, everyone along the chain [takes] a cut"); Tynan & Spring, *supra* note 2, at 72–74 (illustrating the trail of money that pop-ups generate).

63. Tynan & Spring, *supra* note 2, at 73. Adware companies claim to have a code of conduct that forbids affiliates from utilizing deceptive installs and drive-by downloads; rogue affiliates disregard these codes of conduct. *Id.*

64. Claria - Company Information - Corporate Overview, http://www.claria.com/companyinfo/ (last visited Sept. 20, 2006).

65. *Id.* The "behavioral marketing and personalization technology" allows Claria to deliver advertisements that are most likely to interest the consumer. *Id.* An example of Claria's early advertising software is the Gator eWallet, which Claria plans to stop supporting on October 1, 2006. *See* Gator eWallet, http://www.gator.com/home2.html (last visited Sept. 20, 2006). The eWallet is a program that helps consumers fill in online forms and store passwords to websites. More Info on the Gator eWallet, http://www.gator.com/about (last visited Sept. 20, 2006). Consumers can download the program for free in exchange for an agreement to receive ads based on their online activities. *See* Gator 7.0 Privacy Statement and End User License Agreement, http://www.gator.com/help/app_ps_v70.html [hereinafter Gator Privacy Statement] (last visited Sept. 20, 2006). The eWallet programs reports information including consumers' first name, zip code, and country back to GAIN Publishing. *Id.* The GAIN Network is the advertising service of Claria Corporation. *See* Claria Products and Services - Software, http://www.claria.com/products/software (on file with the Houston Law Review).

66. Claria - Company Information - Corporate Overview, *supra* note 64.

67. *See* Gator Privacy Statement, *supra* note 65. GAIN also employs pop-under ads (ads that appear behind the active window), embedded ads (ads displayed within supported applications), and sliders (ads that slide up from the bottom of the screen). About GAIN Ad Vehicles, http://www.gainpublishing.com/global/about (on file with the Houston Law Review).

68. GAIN Publishing - Advertise, http://www.gainpublishing.com/global/advertise/index.html (on file with the Houston Law Review).

for a site that sells clothing than a site that offered something else, like financial services. Claria's software causes pop-up ads for clothing or related items to appear on the consumer's computer screen, increasing the likelihood the consumer will click on the advertisement.[69] Of course, the technique requires that GAIN monitor the consumers' browsing habits in order to provide contextually relevant ads.[70]

Claria's privacy policy espouses concern for protecting the consumer: "Our audience consists of permission-based users who provide upfront acceptance and consent before receiving any ads. All of the behaviors that we identify, collect and analyze are anonymous."[71] Whatever "anonymous" means, that term, as used by Claria, permits the eWallet program to report a consumer's first name, city, zip code, country, browsing history, search engine history, and responses to online ads.[72] eWallet also receives information about the computer's system settings, what software is installed, and software preference settings.[73]

Despite Claria's efforts to gain acceptance in the industry, its aggressive and controversial directed advertising techniques made many enemies.[74] When consumers visited Hertz.com, for example, Claria's software would call pop-up advertisements—sometimes for Hertz's competitors—that would fill the screen and cover up the Hertz site.[75] In 2003, a number of lawsuits ensued as companies

---

69. *See id.* (explaining that consumers who download GAIN software agree to receive targeted advertisements and that these targeted advertisements result in "click and conversion rates" much higher than traditional banner ads).

70. *See* GAIN Publishing - Advertise - Case Study, http://www.gainpublishing.com/global/advertise/case_study/index.html (on file with the Houston Law Review) (explaining the "promise" of internet advertising as bringing relevance to the potential consumer by delivering advertisements for products in which the consumer has expressed an interest).

71. Claria Privacy Center, http://www.claria.com/privacy/policies (on file with the Houston Law Review).

72. *See* Gator Privacy Statement, *supra* note 65 (informing the user that the eWallet program may collect and report all of these items of information).

73. *Id.*

74. Benjamin Edelman, "Spyware": Research, Testing, Legislation, and Suits, http://www.benedelman.org/spyware [hereinafter Edelman, "Spyware"] (last visited Sept. 20, 2006) (offering detailed research on a variety of spyware and adware companies, including the lawsuits filed against these companies).

75. Hertz Corp. v. Gator Corp., 250 F. Supp. 2d 421, 423 (D.N.J. 2003). The Gator Corporation is the defendant in the above suit. *Id.* at 421.

sought to stop this type of advertising.[76] The lawsuits settled, many with undisclosed terms.[77]

The anti-Claria sentiment lingered within the information technology industry long after the lawsuits. In June 2005, word that Microsoft was considering acquisition of Claria for as much as $500 million caused an outcry.[78] The deal ultimately fell through; an anonymous source at Microsoft blamed Claria's reputation and the "PR fallout" that would have resulted from the acquisition.[79]

Ultimately, Claria realized consumers despise pop-ups and, as part of a campaign to rehabilitate its image, announced in 2006 that it was getting out of the adware business.[80] Nevertheless, as Claria's Executive Vice-President Scott Eagle noted, the adware industry "still addresses an estimated $400 to $500 million market."[81] We can therefore predict with some confidence that Claria's exit does not anticipate an industry trend away from the adware market.

2. The Broker's Lament. As the public outcry against spyware has grown, companies responsible for adware and spyware have gone on the offensive. The companies are attempting to gain acceptance for their business models by filing lawsuits, working with government agencies to develop guidelines for spyware, adding a disclosure and consent step to the software installation process, and convincing makers of antispyware software to overlook certain programs.[82]

---

76. *Id.* at 423 & n.1. Suits stemming from Gator's practices involved such companies as Extended Stay America, L.L. Bean, Lending Tree, Metrodate, OverStock.com, Quicken Loans, PriceGrabber, Six Continents Hotels, TigerDirect, United Parcel Service of America, VirtuMundo, the Washington Post, and Weight Watchers. *See id.*; Edelman, "Spyware," *supra* note 74 (enumerating the cases).

77. Newitz, *supra* note 62.

78. *See* Michael Myser, *Rumored Microsoft Adware Deal Raises Red Flags*, EWEEK, June 30, 2005, http://www.eweek.com/article2/0,1895,1833611,00.asp.

79. Zachary Rodgers, *Microsoft/Claria Deal Dead*, CLICKZ NEWS, July 12, 2005, http://www.clickz.com/news/article.php/3519521.

80. *See Gator is Dead. Long Live Claria.*, BUSINESSWEEK ONLINE, Apr. 3, 2006, http://www.businessweek.com/technology/content/apr2006/tc20060403_201560.htm. Claria announced it intended to sell off its adware assets and would require that the purchaser agree "to adhere to emerging industry standards outlined by TRUSTe and other industry coalitions." Press Release, Claria, Claria Exiting Adware Business (Mar. 21, 2006), *available at* http://www.claria.com/companyinfo/press/releases/pr060321.html. TRUSTe, an independent nonprofit group, is dedicated to promoting online privacy concerns. TRUSTe – Make Privacy Your Choice, http://www.truste.org (last visited Sept. 20, 2006).

81. Mario Sgambelluri, *Q&A With Claria's Scott Eagle*, IMEDIACONNECTION, Apr. 3, 2006, http://www.imediaconnection.com/content/8914.asp.

82. *See, e.g.*, Newitz, *supra* note 62 (detailing Claira's use of each of these

Context-marketing company WhenU, for example, argued in a court filing that consumers consent to the installation of its software[83] and that the software provides consumers a useful service.[84] In that same filing, WhenU attempted to show that its product is easily removed by claiming that tens of millions of users uninstalled it successfully.[85] One might pause to wonder why so many "informed" consumers are uninstalling software to which they purportedly consented in the first place. A survey of more than five hundred consumers with WhenU software installed found that eighty-seven percent did not know the program existed on their machines.[86] This statistic suggests WhenU employs a loose definition of "informed consent."

In another example, Ad-Aware, a popular adware detection and removal tool produced by Lavasoft, began offering to remove a particular software package called NewDotNet.[87] NewDotNet's creators, New.net, sued for an injunction to stop Ad-Aware.[88] New.net asserted that in most instances users willingly download the software as part of a bundle.[89] Therefore, Ad-Aware should not offer to remove it.[90] The skeptical judge noted that if consumers knowingly requested and desired the software, as its creators claimed, Ad-Aware's notification of NewDotNet's presence "would hardly come as a surprise" and "there would be no reason for this lawsuit."[91]

Upon being accused of spreading spyware by the New York Attorney General, DirectRevenue, yet another adware company, angrily responded, "Mislabeling our products as 'spyware' does a disservice not only to our company, but also to the public by creating an atmosphere of hysteria, confusion and inaccuracy."[92] The company asserted it had changed its practices "long ago"—an

---

techniques in an attempt to change its public image).

83. Complaint ¶ 37, WhenU.com, Inc. v. Utah, No. 040907578, (3d Jud. Dist. Ct., Salt Lake County, Utah Apr. 12, 2004) [hereinafter WhenU Complaint], *available at* http://www.benedelman.org/spyware/whenu-utah/complaint.pdf.

84. *Id.* ¶¶ 17–18.

85. *Id.* ¶¶ 43–44.

86. PC Pitstop, Eighty-Seven Percent of WhenU Users Are Unaware They Are Using It, http://www.pcpitstop.com/spycheck/ whenu.asp (last visited Sept. 20, 2006).

87. *See* New.net, Inc. v. Lavasoft, 356 F. Supp. 2d 1071, 1072–73 (C.D. Cal. 2003).

88. *Id.* at 1072–73, 1075 (explaining the background of the case and providing an explanation for the relationship between the company, New.net, and the software, NewDotNet).

89. *Id.* at 1078.

90. *Id.* at 1077–78.

91. *Id.* at 1078.

92. Press Release, Direct Revenue, Direct Revenue Rebuts New York Attorney General's Charges (Apr. 4, 2006), *available at* http://www.direct-revenue.com/news23.php.

indefinite term that the company quickly narrowed to "at least six months."[93] Despite DirectRevenue's protestations, the company soon found itself settling a California class action lawsuit and agreeing to stop engaging in conduct consistent with traditional notions of spyware.[94]

Because of situations such as those discussed above, informed consumers who read statements from adware companies claiming to oppose spyware no doubt feel the same sense of disbelief they experienced when tobacco executives argued that cigarettes were not addictive.[95]

D. Installation Methods

Having defined what spyware does and why it exists, we now turn to the means by which it is installed. There are three primary means by which spyware reaches the computers of consumers. A "drive-by download" refers to an installation that occurs without notice or consent when the consumer visits a webpage.[96] "Bundling" refers to the practice of installing spyware in a package with other software.[97] Finally, consumers may be deceived into installing spyware when they seek a program for some other purpose, such as the ability to read a certain type of file or, ironically, to improve security on the machine.[98] The phrase "bait-and-switch" adequately describes this third method of installation.

1. The Drive-By Download. The "drive-by download" occurs when a computer installs spyware merely by visiting a website.[99] Webpages on the Internet are in actuality small text files with instructions for displaying text and graphics on the screen.[100] The browser downloads and reads the file, follows the instructions for

---

93. *Id.*

94. *See* Notice of Proposed Settlement at 2–5, Battaglia v. DirectRevenue, LLC, No. 05-CV-02547-LKK-PAN (JFM) (E.D. Cal. 2005), *available at* http://www.direct-revenue.com/Complete_Settlement_Notice.pdf (enumerating the terms of the settlement and listing a fairness hearing date of December 11, 2006).

95. *See* Jolie Solomon, *Smoke from Washington*, NEWSWEEK, Apr. 4, 1994, at 45 (noting that "tobacco companies routinely deny that cigarettes are addictive," and mentioning the difficulty smokers have quitting in the face of such denials).

96. TITTEL, *supra* note 1, at 7.

97. New.net, Inc. v. Lavasoft, 356 F. Supp. 2d 1071, 1077 (C.D. Cal. 2003).

98. *See* Kim Zetter, *Spyware: What You Need to Know*, WIREDNEWS, Oct. 17, 2005, *available at* http://www.wired.com/news/privacy/0,68275-1.html?tw=wn_story_page_next1.

99. TITTEL, *supra* note 1, at 7.

100. RON WHITE, HOW COMPUTERS WORK 366 (8th ed. 2006).

displaying the page, and displays the webpage on the monitor.[101] The file can also include embedded programs that the browser will read and then execute.[102] While this model drives the World Wide Web,[103] it also creates great challenges in maintaining security.[104] Unscrupulous programmers can take advantage of security weaknesses in web browsers by installing software without the consumer's knowledge.[105] Harvard economist and antispyware evangelist Ben Edelman placed a video on the Internet demonstrating how visiting a single webpage caused the installation of sixteen discrete spyware programs, none of which gave the consumer notice.[106]

The Russian company iFrameDollars.biz provides a particularly blatant example of using drive-by downloads. The company pays website administrators to include code in their webpages that exploits a known vulnerability and installs spyware without the consumer's knowledge.[107] The spyware hijacks the consumer's homepage, installs a toolbar, and deploys pop-up advertisements.[108] iFrameDollars.biz pays between $.06 and $.55 per download.[109] Testing by iDefense, Inc., a computer

---

101. *Id.* at 366–67.

102. *See* STUART MCCLURE ET AL., HACKING EXPOSED: NETWORK SECURITY SECRETS & SOLUTIONS 575 (5th ed. 2005) (implying that browsers read embedded programs to create complex webpages by describing the functionality of ActiveX). ActiveX, Java, JavaScript, and Active Scripting are examples of the types of programs that can be embedded within a webpage and executed on a consumer's computer. *Id.* at 575–80. The programs can provide additional functionality to a webpage, but they are easily misused by attackers to run malicious code on the consumer's computer. *See id.* (discussing vulnerabilities in ActiveX controls, Java, JavaScript and Active Script).

103. *See* WHITE, *supra* note 100, at 364–67 ("How a Web Browser Opens Web Pages").

104. *See* MCCLURE ET AL., *supra* note 102, at 579 ("To be fair, the security challenges presented by [technology that drives webpages] don't necessarily derive from problems inherent to the technologies . . . but rather from their accessibility and power being easily abused to do evil.").

105. *See, e.g.*, Brian Krebs, *Microsoft Works to Fix New Threat to Windows*, HOUS. CHRON., Dec. 31, 2005, at D3 (describing a vulnerability in Windows that allowed an attacker to run arbitrary code on a consumer's machine simply by luring the consumer to the attacker's website).

106. Ben Edelman, *Who Profits from Security Holes?*, Nov. 18, 2004, http://www.benedelman.org/news/111804-1.html (follow "See a video of the installations" hyperlink).

107. Paul F. Roberts, *Drive-By Download Sites Chauffeur Spyware*, EWEEK, June 20, 2005, http://www.eweek.com/article2/0,1895,1829174,00.asp; *see also* MCCLURE ET AL., *supra* note 102, at 583 (describing the iFrame browser vulnerability).

108. Roberts, *supra* note 107. "Hijacking the consumer's home page" means changing, without the consumer's request or permission, the default website that opens when launching the browser. TITTEL, *supra* note 1, at 5.

109. Roberts, *supra* note 107 (focusing on one high-value product for which iFrameDollars.biz pays $.55 per download); Gregg Keizer, *From Russia With Malware*, INFORMATIONWEEK, May 30, 2005, at 63 (standardizing the payments made by

security company, showed that installation of this spyware program provided a bootstrap for other spyware programs.[110] Merely by visiting one website, the computer could become infected with 111 different spyware programs.[111] One security expert estimated iFrameDollars.biz's net profit at $63,000 from just one week's worth of installations.[112]

Other adware companies like 180Solutions and DirectRevenue understand the unpopularity of spyware and insist that they do not support affiliates who install software without the consumer's consent.[113] Nevertheless, evidence available on the Internet proves 180Solutions software is installed frequently without notice to users.[114] DirectRevenue was sued recently for installing spyware on consumers' computers without displaying a license agreement.[115]

2. Bundling. In "bundling," a consumer intentionally downloads a program, but the installation includes other, unrelated software that the consumer did not request.[116] The Internet-based company, New.net, discussed above, provides an example of this technique. New.net sells nonstandard Internet domain names such as ".shop" or ".free."[117] Because these domain names are nonstandard, computers cannot resolve them using normal methods, rendering the websites unreachable.[118] Therefore, New.net deploys NewDotNet software, which helps

---

iFrameDollars.biz to an estimated $.06 per download).

110. *See* Roberts, *supra* note 107 (explaining that downloading the iFrameDollars.biz's exploit of Microsoft's iFrame triggered a second download of X.chm—presumably without the computer user's knowledge).

111. *Id.* (specifying that X.chm, a "Trojan-Downloader," put 111 distinct programs on the consumer's computer).

112. *See* Keizer, *supra* note 109, at 63.

113. *See* Tynan & Spring, *supra* note 2, at 73. 180Solutions was renamed "Zango" in June 2006. Eric Benderoff, *Class-Action Suit Dismissed Against Spyware Provider*, CHI. TRIB., Sept. 7, 2006, at C1. This Comment retains the prior name to avoid confusion.

114. *See* Ben Edelman, 180Solutions Installation Methods and License Agreement, http://www.benedelman.org/spyware/180-affiliates/installation.html (last visited Sept. 20, 2006).

115. Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219, 1223–24 (N.D. Ill. 2005).

116. *See* New.net, Inc. v. Lavasoft, 356 F. Supp. 2d 1071, 1077 (C.D. Cal. 2003).

117. *Id.* at 1075. Domain names make websites more accessible to consumers by using names such as http://uh.edu to reach web addresses instead of less user-friendly IP addresses. PAUL ALBITZ & CRICKET LIU, DNS AND BIND ix (Mike Loukides ed., 2d ed. 1997). The letters after the last dot, such as "com," "mil," "gov," or "edu" define groupings called the top-level domains. *Id.* at 17–19. Top level domains are standardized by certain conventions in order to help organize the appearance of domain names. *Id.* at 16–17.

118. *New.net, Inc.*, 356 F. Supp. 2d at 1075.

computers resolve the nonstandard domain names and find client websites.[119]

New.net acknowledges that the only way to make clients' websites accessible is to distribute the NewDotNet software to as many computers as possible.[120] New.net seeks to maximize the distribution of its software by bundling.[121] In some cases, notice of the bundled installation hides within complex user agreements that lack opt-out clauses; in other cases, the consumer receives no notification at all.[122] New.net sued Lavasoft because its Ad-Aware product offered to uninstall NewDotNet software after locating it on consumers' machines.[123] Legal counsel for New.net argued that an opt-out clause was unnecessary because the user could simply choose not to install applications that bundled NewDotNet.[124] The judge deciding the case summarized the policy in unsympathetic language: "In short, New.net includes its software with certain programs that people want, and, unless the consumer is willing to give up what he or she wants, the consumer must take the NewDotNet software. This is apparently what passes for consensual download in the world of 'foistware.'"[125] Unfortunately, bundling is not unique to New.net; the practice is widespread and has been attributed to companies including DirectRevenue, Gator, and WhenU.[126]

3. The Bait-and-Switch. Finally, makers of spyware may lie to consumers about a program's true behavior in order to facilitate the program's installation.[127] For example, some spyware programs advertise themselves as spyware removal tools, when in fact, they install spyware.[128] According to the FTC, Max Theater offered a remote, Internet-based scan of computers to look for spyware, but the scan was fraudulent.[129] Every scan

---

119. *See id.*

120. *Id.*

121. *See id.* at 1077.

122. *See id.* at 1077–78.

123. *Id.* at 1072–73. As discussed above, Lavasoft produces Ad-Aware, and New.net produces Newdotnet. *See supra* text accompanying notes 87–91.

124. *New.net, Inc.*, 356 F. Supp. 2d at 1077–78 & n.9.

125. *Id.* at 1078 n.9.

126. *See* Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219, 1223 (N.D. Ill. 2005) (stating that DirectRevenue uses bundling to deploy spyware without the consumer's informed consent); Jill E.C. Yung, Comment, *Virtual Spaces Formed by Literary Works: Should Copyright or Property Rights (or Neither) Protect the Functional Integrity and Display of a Web Site?*, 99 NW. U. L. REV. 495, 499–500 (2004) (discussing the bundling techniques of Gator and WhenU).

127. *See* Zetter, *supra* note 98.

128. *See id.*

129. Press Release, Fed. Trade Comm'n, FTC Bars Bogus Anti-Spyware Claims

informed consumers that they had a spyware infection regardless of the truth, and the program encouraged consumers to purchase an equally fraudulent antispyware program to fix the problem for $29.95.[130] Another company called Trustsoft followed the same format, except it charged $39.95.[131] Because this method of installation is so obviously fraudulent and cannot be justified by a spyware company on any reasonable theory, it is not discussed further.[132]

E. The End User License Agreement

Moving beyond the drive-by downloads, bundling, and bait-and-switch installations discussed above, a more complex facet to the spyware controversy may be found in the End User License Agreement, or EULA. EULAs claim to provide the consumer with notice of the software's activities and obtain the consumer's consent before installing.[133] Recall that US-CERT expressly excludes from its definition of spyware any program that provides the consumer notice of the software's data-collection activities through a clear privacy policy.[134] What constitutes a clear privacy policy? Two types of licenses are relevant to our discussion: the so-called clickwrap and browsewrap licenses.[135]

With a clickwrap license, the consumer agrees to be bound to the license displayed on the screen by clicking "I agree."[136] Courts

---

(Mar. 11, 2005), http://www.ftc.gov/opa/2005/03/maxtheater.htm.

130. *See id.*

131. *See* Press Release, Fed. Trade Comm'n, FTC Halts Operation's Bogus "Anti-Spyware" Claims, Freezes Assets (June 23, 2005), http://www.ftc.gov/opa/2005/06/trustsoft.htm (detailing the methodology used by Trustsoft to scam consumers).

132. *See* John Borland, *Spyware Cures May Cause More Harm Than Good*, CNET, Feb. 4, 2004, http://news.com.com/2100-1032_3-5153485.html (quoting the associate director for the Center of Democracy and Technology as saying this method of installation is "clearly . . . an unfair and deceptive practice").

133. *See* Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 21–24 (2d Cir. 2002) (describing Netscape's EULA).

134. HACKWORTH, *supra* note 14, at 2.

135. *See generally* Robert L. Oakley, *Fairness in Electronic Contracting: Minimum Standards for Non-Negotiated Contracts*, 42 HOUS. L. REV. 1041, 1050–1052 (2005) (describing "clickwrap," "shrinkwrap," and "browsewrap" licenses). The term "clickwrap" derives from the "shrinkwrap" licenses that appear inside shrinkwrapped products. *See Specht*, 306 F.3d at 22 n.4 (making the analogy between "shrinkwrap" and "clickwrap" licenses). The terms "browserwrap" and "browsewrap" are very new and appear to enjoy roughly equal support. Google Search by Author (Aug. 26, 2006) (on file with the Houston Law Review) (returning 579 hits for "browserwrap" and 629 for "browsewrap"). "Browserwrap" is harder to say and should be subsumed by "browsewrap" thanks to a linguistic phenomenon called syncope, where letters within words are dropped over time. *See* BILL BRYSON, THE MOTHER TONGUE: ENGLISH & HOW IT GOT THAT WAY 88 (1990) (discussing syncope and providing examples).

136. *See Specht*, 306 F.3d at 21–22 (describing clickwrap licenses).

have held these agreements to be enforceable.[137] A browsewrap license does not display the text of the agreement for the consumer; instead, the website displays only a hyperlink to the license.[138] The case law does not provide clear guidance on this type of license.[139] In one case, a hyperlink underneath the "Download" button led consumers to a website with the license agreement, but the hyperlink was positioned so that consumers had to use the scroll bar to find the hyperlink. The court held the agreement unenforceable because consumers had insufficient notice that by clicking "download" they were accepting an agreement.[140] To date, no court has ruled on what would happen if a webpage prominently displayed the hyperlink to a license agreement with words such as, "By clicking 'download,' you are consenting to the terms of this website."[141] On the one hand, the agreement could be held enforceable because the prominently displayed notice of terms would put consumers on "inquiry notice" that they were agreeing to a contract with terms to which they would be held.[142] However, the FTC recently sued

---

137. *See In re* RealNetworks, Inc., Privacy Litigation, No. 00-C-1366, 2000 U.S. Dist. LEXIS 6584, at *2, *16–17 (N.D. Ill. May 8, 2000) (describing the clickwrap contract employed by RealNetworks and upholding it against challenges of procedural unconscionability); Hotmail Corp. v. Van Money Pie, Inc., No. C98-20064-JW, 1998 U.S. Dist. LEXIS 10729, at *17 (N.D. Cal. Apr. 16, 1998) (binding a company to the terms of a contract assented to when the company created a Hotmail e-mail account).

138. *See* Defontes v. Dell Computers Corp., No. PC 03-2636, 2004 R.I. Super. LEXIS 32, at *15 (R.I. Super. Ct. 2004) (defining the browsewrap license).

139. *See* Pollstar v. Gigmania, Ltd., 170 F. Supp. 2d 974, 981 (E.D. Cal. 2000) ("No reported cases have ruled on the enforceability of a browse wrap license."). *But see id.* at 981–82 (suggesting that browsewrap agreements might be enforceable if websites gave adequate notice of the license).

140. *Specht*, 306 F.3d at 30, 35 (describing Netscape's presentation of the hyperlink to the license terms relative to the "download" button and then holding the license agreement unconscionable for lack of notice); *see also Defontes*, 2004 R.I. Super. LEXIS 32, at *17, *20–21 (holding an arbitration agreement presented through a hyperlink "inconspicuously located at the bottom of the webpage" was not binding).

141. *See* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 429 (2d Cir. 2004) (commenting, tangentially, on the lack of precedent regarding browsewrap licenses just before concluding that the instant case did not involve a browsewrap license) (citing *Pollstar*, 170 F. Supp. 2d at 981–82). The court in *Pollstar* refused to make a decision regarding the validity of browsewrap licenses that are conspicuously displayed because the license under consideration was artfully hidden, rendering it invalid—but not due to the license's status as a browsewrap license. *Pollstar*, 170 F. Supp. 2d at 981–82.

142. *See Specht*, 306 F.3d at 30–32 (intimating that some browsewrap licenses would be valid due to inquiry notice).

> Every person who has actual notice of circumstances sufficient to put a prudent man upon inquiry as to a particular fact, has constructive notice of the fact itself in all cases in which, by prosecuting such inquiry, he might have learned such fact. . . . These principles apply equally to the emergent world of online product delivery, pop-up screens, hyperlinked pages, clickwrap licensing, scrollable documents, and urgent admonitions to "Download Now!".

Advertising.com for deceptive trade practices because the company allegedly used a browsewrap license to obscure disclosure that the downloadable software also contained adware.[143] The case settled, so there remains no precedent.[144]

Whether through clickwrap or browsewrap licenses, installations often present EULAs with intentionally convoluted, deceptive, or dense language to discourage reading.[145] As noted on Ben Edelman's website, the Gator software license agreement is sixty-three screens long—so long that most consumers will never read all of it, missing integral provisions such as an agreement not to use third-party programs to remove Gator.[146] These unwary consumers also agree not to monitor what information Gator transmits.[147] Yet when confronted with a lawsuit, purveyors of spyware that include EULAs can simply point to the EULA and argue the consumer provided informed consent.[148]

Even more troubling, some spyware programs come bundled with software programs that target children.[149] Ben Edelman documented that Ask Jeeves deploys its toolbar through free online games that attract children, such as "Monkey Slide" and "Junk Food Jack."[150] The games bundle the toolbar, but children who install it are unlikely to read, comprehend, or legally accept

---

Id. at 31 (citation omitted). While recognizing a potential argument that would support browsewrap contracts, the court disagreed that the particular facts of the case supported the conclusion that the plaintiffs were put on inquiry notice. *Id.* The screen where the plaintiffs pressed "download" did not include any indication that they were assenting to a contract, nor did the screen encourage consumers to scroll down for more information. *Id.* at 31–32.

143. *See* Complaint ¶ 6, *In re* Advertising.com, Inc., No. C-4147, 2005 WL 2329812 (F.T.C.) (2005), *available at* http://www.ftc.gov/os/caselist/0423196/050916comp0423196.pdf; *see also infra* text accompanying notes 271–280 (discussing this case).

144. *See* Press Release, Fed. Trade Comm'n, Advertising.com Settles FTC Adware Charges (Aug. 3, 2005), http://www.ftc.gov/opa/2005/08/spyblast.htm.

145. *See* Larry Ponemon, *Internet Economics 101*, DARWIN, May 23, 2005, http://www2.darwinmag.com/read/feature/may05_ponemon.cfm (noting that 78% of consumers in a spyware study admitted not reading EULAs because the license agreements were too complicated or difficult to understand).

146. *See* Ben Edelman, *Gator's EULA Gone Bad*, Nov. 29, 2004, http://www.benedelman.org/news/112904-1.html (offering excerpts from Gator's EULA).

147. *Id.*

148. *See* Sotelo v. DirectRevenue, LLC, 348 F. Supp. 2d 1219, 1227–28 (N.D. Ill. 2005) (arguing that "every time Spyware is installed . . . the computer user is presented with the opportunity through a hyperlink to read the EULA prior to downloading the software").

149. *See* Bob Sullivan, *Spyware Firms Targeting Children*, MSNBC.COM, May 5, 2005, http://www.msnbc.msn.com/id/7735192 (observing that many sites that are laced with spyware tempt children with free games).

150. Ben Edelman, Ask Jeeves Toolbar Installs via Banner Ads at Kids Sites, http://www.benedelman.org/spyware/installations/askjeeves-banner (last visited Sept. 20, 2006).

the 108-paragraph EULA linked to the installation page.[151] Edelman documents similar activity on thekidzpage.com, which deploys a spyware program called Hotbar.[152] The abuses discussed above suggest the spyware-adware industry is ripe for some form of regulation.

F. Opposition to Legislation

Andrew McLaughlin, senior policy council for Google, argued that the industry should correct itself through technology, rather than regulation: "'We didn't look to laws to stop viruses, we looked to technology like Norton Antivirus that stops viruses.'"[153] Three problems plague that argument. First, we do look to laws to stop viruses: virus writers get arrested.[154] Second, spyware is not a virus. A virus is a program that replicates itself and exhibits destructive or mischievous behavior.[155] Spyware programs are supported by marketers and advertisers and create revenue streams.[156] Finally, technology has *not* stopped viruses.[157] Viruses have been infecting personal computers for a quarter-century and they continue to be a problem today.[158] Virus coders constantly invent new methods of attack, creating the need for constantly updated detection software.[159] If we rely on technology, we maintain an intolerable status quo: spyware companies and their affiliates grow richer while consumers pay the price for

---

151. *See id.* (noting that while Ask Jeeves's license agreement asks children under the age of thirteen not to download its software, this limitation is stated in the next to last paragraph of its lengthy agreement).

152. Ben Edelman, Hotbar Installs via Banner Ads at Kids Sites, http://www.benedelman.org/spyware/installations/kidzpage-hotbar (last visited Sept. 20, 2006).

153. Emily C. Kumler, *What's the Best Way to Stop Spyware?*, PC WORLD, Apr. 20, 2004, *available at* http://www.pcworld.com/news/article/0,aid,115765,00.asp.

154. *See, e.g.*, Steven Levy, *Biting Back at the Wily Melissa*, NEWSWEEK, Apr. 12, 1999, at 62, 64 (recounting the identification and arrest of the Melissa virus coder).

155. WHITE, *supra* note 100, at 384.

156. *See id.* at 380.

157. *See* Matthew Schwartz, *Security Managers Report Virus Problem Worse*, ENTERPRISE SYSTEMS, Mar. 31, 2004, http://esj.com/security/article.aspx?EditorialsID=913 (reporting "the opinion of 9 out of ten security managers . . . in the ninth annual Computer Virus Prevalence Survey" that the computer virus problem is worsening).

158. *See* PETER SZOR, THE ART OF COMPUTER VIRUS RESEARCH AND DEFENSE 17 (2005) ("The first viruses on microcomputers were written on the Apple-II, circa 1982."). Virus and antivirus coders have been sparring ever since with no end in sight. *See, e.g.*, Tony Bradley, *The New Virus Fighters*, PC WORLD, Mar. 2006, at 82, 84 (reviewing the latest products that combat ever evolving viruses).

159. Andrew Sullivan, *Programs in Peril*, PC WORLD, Mar. 2006, at 16, 18 (discussing the need to update antivirus software regularly).

antispyware programs, update subscriptions, and technical support for compromised systems.[160] Legislation, not technology, can cut off the revenue streams and help put an end to spyware.

Critics may also argue that a legislative solution is no more likely to eliminate spyware than the CAN-SPAM Act has eliminated unsolicited commercial email, or spam.[161] It is true that CAN-SPAM failed miserably.[162] However, even as it passed into law, critics of CAN-SPAM argued its provisions were too weak to be effective.[163] As California State Senator Debra Bowen put it, "The bill doesn't can spam, it legalizes it . . . it is full of loopholes. It's difficult to enforce. It's weaker than many state laws."[164] The lesson of CAN-SPAM is that any truly effective antispyware law must be strong, free of loopholes, and easy to enforce.

The next section examines steps taken by state legislatures in dealing with spyware.

II. STATE LEGISLATIVE SOLUTIONS

State legislators have considered various approaches for controlling spyware.[165] Very broadly, the statutes considered and passed by the states fall into three models. The first type denies spyware purveyors the ability to obtain a consumer's legal authorization through a EULA and by requiring an authorized user to install these products. The second type requires the installer to be an owner or authorized operator of the computer on which spyware is installed in order for authorization to be valid. The third type requires a standardized, plain-language warning before a consumer continues the installation.

---

160. *See Spyware Developers Net Huge Profits, Outrage*, MSNBC.COM, July 7, 2006, http://www.msnbc.msn.com/id/13757388 (stating that Spyware companies earn approximately $2 billion a year in revenue).

161. Christopher Conkey, *FTC Wins Order to Shut Down Spam from Adult Web Sites*, WALL ST. J., Jan. 12, 2005, at D2 (discussing how unsolicited commercial e-mail actually increased in 2004 despite the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM")).

162. *Id.*

163. *See* Erin Elizabeth Marks, Comment, *Spammers Clog In-Boxes Everywhere: Will the CAN-SPAM Act of 2003 Halt the Invasion?*, 54 CASE W. RES. L. REV. 943, 952–56 (2004) (enumerating weaknesses in the CAN-SPAM Act).

164. *Id.* at 952 n.70.

165. Ben Edelman, State Spyware Legislation, http://www.benedelman.org/spyware/legislation (last visited Sept. 20, 2006) (chronicling over forty separate pieces of legislation in a range of states, including Alabama, Texas, and California).

A. Invalidating the EULA

Some state plans invalidate the EULA as a means of obtaining authorization to install spyware on a computer. In California, software that behaves like spyware may only be installed by authorized users.[166] California denies authorized user status to "a person or entity that has obtained authorization to use the computer solely through the use of an end user license agreement."[167] Other states, including Alabama, Illinois, Kansas, Massachusetts, Missouri, Nebraska, and New York, currently are considering bills that emulate California's exclusion clause; moreover, none of these statutes or bills offer an alternative, legal method by which affiliates may obtain consent to install spyware.[168]

Despite this get-tough sounding approach, critics of California's statute believe it will prove ineffective.[169] The statute requires intentional deception for the software to fall under the ban.[170] The statute states that a person who is not an authorized user shall not, "through intentionally deceptive means," install software that modifies Internet settings, collects personally identifiable information, or resists efforts to remove it.[171] The statute defines "intentionally deceptive means" as false statements, omissions, misrepresentations, or "an intentional and material failure to provide any notice to an authorized user regarding the download or installation of software in order to

---

166. Consumer Protection Against Computer Spyware Act, CAL. BUS. & PROF. CODE § 22947.2 (West Supp. 2006).

167. *Id.* § 22947.1(b).

168. *See* S.B. 122, 2005 Reg. Sess. (Ala. 2005), *available at* http://alisdb.legislature.state.al.us/acas/searchableinstruments/2005rs/bills/sb122.htm; H.B. 380, 94th Gen. Assem. (Ill. 2005), *available at* http://www.ilga.gov/legislation/94/HB/PDF/09400HB0380lv.pdf; H.B. 2343, 2005 Leg. Sess (Kan. 2005), *available at* http://www.kslegislature.org/bills/2006/2343.pdf; H.B. 1444, 184th Gen. Court, Reg. Sess. (Mass. 2005), *available at* http://www.mass.gov/legis/bills/house/ht01/ht01444.htm; H.B. 902, 93d Gen. Assem., 1st Reg. Sess. (Mo. 2005), *available at* http://www.house.mo.gov/bills051/biltxt/intro/HB0902I.htm; L.B. 316, 99th Leg., 1st Sess. (Neb. 2005), *available at* http://www.unicam.state.ne.us/pdf/INTRO_LB316.pdf; S.B. 3600, 2005–2006 Leg., Reg. Sess. (N.Y. 2005), *available at* http://assembly.state.ny.us/leg/?bn=A00549&sh=t.

169. *See, e.g.*, Michael L. Baroni, *Spyware Beware*, ORANGE COUNTY LAW. MAG., at 36, 39–40 (2005) (criticizing California's antispyware legislation because (1) it does not prohibit spyware; (2) it only prohibits software with a wrongful effect; (3) it does not prohibit all software installed without a user's informed consent; (4) it requires a showing of intent to deceive the consumer; (5) it does not define what type of notice is adequate notice; and (6) it has no enforcement or damages provision).

170. *See id.* at 39.

171. Consumer Protection Against Computer Spyware Act, CAL. BUS. & PROF. CODE § 22947.2(a)–(c) (West Supp. 2006).

deceive the consumer."[172] Is a lengthy EULA intentionally deceptive if it uses jargon like "directed marketing" to refer to pop-ups delivered based on browsing habits? Few courts are likely to find this language deceptive,[173] so most spyware companies that use EULAs would remain unaffected by the statute. Thus, a purveyor of spyware who had a one-hundred page browsewrap license agreement with the hyperlink visible, but tucked away in one corner of the screen, could remain untouched by this provision.

B. Requiring Authorization

Other states simply require that the person or entity installing the software be an owner or authorized operator of the computer. Arizona, Georgia, Indiana, Texas, and Washington passed statutes that use this owner-operator language;[174] Delaware and Rhode Island are considering nearly identical language.[175] These states allow owners or operators of computers to install software of their choosing; rather than focusing on the use of EULAs, the legislatures focus on the deceptive nature of silent installations. For example, the Arizona statute states that "an intentional and material failure to provide any notice to an owner or operator of a computer regarding the installation or execution of computer software in order to deceive the owner or operator" is "intentionally deceptive."[176] The Texas and Indiana legislatures adopted essentially the same definition for the term.[177] The recursive nature of these definitions renders them

---

172. *Id.* § 22947.1(h).

173. The use of technical terms or terms of art within contracts is acceptable, and such words are given the meaning that an expert in the industry would give them. *See* Foster Wheeler Enviresponse, Inc. v. Franklin County Convention Facilities Auth., 678 N.E.2d 519, 526 (Ohio 1997).

174. ARIZ. REV. STAT. ANN. § 44-7301(7) (Supp. 2005); GA. CODE ANN. § 16-9-151(2) (Supp. 2005); IND. CODE ANN. § 24-4.8-1-8 (LexisNexis 1996 & Supp. 2005); TEX. BUS. & COM. CODE ANN. § 48.002(7) (Vernon Supp. 2006); WASH. REV. CODE ANN. § 19.270.010(7) (West Supp. 2006). For example, the Arizona statute defines the owner or operator as "the owner or lessee of a computer or someone using the computer with the owner's or lessee's authorization. Owner or operator does not include any person who owns a computer before the first retail sale of the computer." ARIZ. REV. STAT. ANN. § 44-7301(7).

175. *See* S.B. 124, 143d Gen. Assem., Reg. Sess. (Del. 2005), *available at* http://www.legis.state.de.us/LIS/lis143.nsf/vwLegislation/SB+124/$file/legis.html?open; H.B. 6211, 205th Gen. Assem., Reg. Sess. (R.I. 2005), *available at* http://www.rilin.state.ri.us/BillText/BillText05/HouseText05/H6211.pdf.

176. ARIZ. REV. STAT. ANN. § 44-7301(5)(c). Arizona's definition of "intentionally deceptive" follows California's definition. *See supra* text accompanying note 172 (providing California's definition, which is almost identical).

177. *See* IND. CODE ANN. § 24-4.8-1-8 (defining intentionally deceptive in the context of computer downloads); TEX. BUS. & COM. CODE ANN. § 48.056(3) (same).

practically meaningless. Of course an intentional failure to notify with intent to deceive is intentionally deceptive. This definition serves only to raise significant challenges for a complainant, who now must show that the spyware company's failure to notify the complainant of the installation was intentional, material, and designed to deceive. Equally awkward is the New Hampshire bill, which defines an authorized user as "a consumer who owns or is permitted to use a computer."[178] The statute does not define the term "consumer." Does it include business entities who access the computer remotely? And what form of permission is required?[179] In these states, any spyware company with a EULA has an effective shield against charges of a violation.

C. Disclosing the Details

Finally, some states have considered calling for explicitly worded notices that apprise the consumer of the software's true purpose. For example, antispyware statutes considered in Massachusetts and Oregon required a list of information the software reports, a representative sample of the type of advertisements that the software delivers, and a statement of the frequency with which those ads are delivered.[180] Similar provisions exist in bills considered by Pennsylvania[181] and Tennessee.[182]

These provisions appear to address adequately the problem of drive-by downloads.[183] They do little else, however. The provisions do not provide protection beyond that already provided in a browsewrap license.[184] When presented as underlined, differently colored hyperlinks to EULAs, browsewrap licenses arguably make the notice clearly distinguishable.[185] Furthermore,

---

178. N.H. REV. STAT. ANN. § 359-H:1(II) (LexisNexis Supp. 2005).

179. *See id.* § 359-H:1.

180. *See* H.B. 3739, 184th Gen. Court, Reg. Sess., § 21(1)(c)(i)(B)–(C) (Mass. 2005), *available at* http://www.mass.gov/legis/bills/house/ht03/ht03739.htm (defining spyware as software that fails to obtain consent regarding the specific information the program will transmit and that does not obtain consent for advertisements that the program will bring to the user's screen); H.B. 2302, 73d Leg., Reg. Sess., § 2(3) (Or. 2005), *available at* http://www.webanalyticsassociation.org/attachments/files/17/OR_HB_2302.pdf (same).

181. *See* H.B. 574, 2005 Sess., Gen. Assem., § 662(a)(1) (Pa. 2005).

182. *See* H.B. 1742, 104th Gen. Assem., 2d Reg. Sess., § 2(4)(C)(i)(b)–(e) (Tenn. 2005), *available at* http://www.legislature.state.tn.us/bills/currentga/Chapter/PC0929.pdf (enacted 2006).

183. *See supra* Part I.D.1 (explaining drive-by downloads as surreptitious installations of software).

184. *See supra* Part I.E (discussing browsewrap licenses).

185. *See* Ben Edelman, *What Hope for Federal Anti-Spyware Legislation?*, Jan. 31, 2005, http://www.benedelman.org/news/011905-1.html (pointing out that spyware

many overly lengthy EULAs already provide information of the type demanded in the Massachusetts and Oregon bills, albeit buried under several paragraphs of legalese.[186]

D. Utah's Spyware Control Act

Utah's Spyware Control Act, one of the first comprehensive spyware acts, prohibited the "use [of] a context based triggering mechanism to display an advertisement that partially or wholly covers or obscures paid advertising or other content on an Internet website in a way that interferes with a user's ability to view the Internet website."[187] Moreover, the statute established strict requirements for obtaining consent from a consumer before installing.[188] WhenU, an advertising broker, immediately challenged the statute and argued it was unconstitutional, for reasons set out below.[189] The result drew keen interest from other state legislatures intent on passing similar antispyware bills[190] and raised issues likely to plague other states in the near future.

1. A Demand for Uniformity. WhenU challenged Utah's antispyware legislation and sought a permanent injunction to prohibit enforcement. WhenU described itself as a "contextual marketing" company that delivered directed advertisements to consumers on behalf of over 400 companies.[191] It complained that the statute violated the Commerce Clause of the U.S. Constitution by impermissibly regulating commerce outside of Utah's borders.[192] WhenU argued that the statute "contained no

---

companies could satisfy the notice requirement of a federal antispyware bill by creating a hyperlink to their EULAs).

186. For example, Gator's EULA provides consumers with a link to a website where they may view examples of the advertisements that will be displayed on their computers, as well as the frequency with which the advertisements will be displayed. Ben Edelman, Claria's License Agreement – As Copied from Kazaa Installer (Nov. 2004), http://www.benedelman.org/spyware/claria-license/license-112504.html.

187. Spyware Control Act, 2004 Utah Laws Ch. 363, sec. 3, § 13-39-201(c), *recompiled & codified as* UTAH CODE ANN. § 13-40-201 (2004), *amended by* UTAH CODE ANN. § 13-40-201 (2005); *see also* Polly Samuels McLean & Michelle M. Young, *SPYWARE: Living in a Cyber-Fishbowl*, 19 UTAH BAR J. 34, 35 (2006) (introducing the Utah bill).

188. *See* Spyware Control Act, § 13-39-102(4)(c).

189. WhenU Complaint, *supra* note 83, ¶ 1.

190. *See* Mich. Senate Fiscal Agency, *Second Analysis of S.B. 53 (S-2), 54 (S-3), & 151 (S-2)*, Mar. 22, 2005, http://www.legislature.mi.gov/documents/2005-2006/billanalysis/senate/htm/2005-SFA-0053-B.htm (discussing Utah's Spyware Control Act as part of the legislative background in the fight against spyware).

191. WhenU Complaint, *supra* note 83, ¶¶ 29, 36. WhenU's clients include Bank of America, Delta Airlines, H&R Block, and Lloyd's of London. *Id.* ¶ 36.

192. *Id.* ¶¶ 65–70. WhenU also alleged other violations: First, the statute violated the First and Fourteenth Amendments by prohibiting truthful and nonmisleading

nexus to Utah" and could be interpreted as affecting Internet commerce in all fifty states.[193] WhenU expanded upon this argument, postulating that even if the statute contained a nexus provision, WhenU could not filter its software geographically because of "the mobility of computer users, the realities of the Internet, and WhenU's own" policy against collecting personally identifiable information.[194] Further, WhenU argued that permitting states to regulate spyware would lead to intolerable results:

> If the Act is allowed to become effective, the Act would threaten WhenU with the specter of being required to comply with numerous local regulatory schemes. One jurisdiction might require license agreements to be presented in "plain language;" another might require the use of particular technical terms. One jurisdiction might require license agreements to be in large type; another might require them to fit on a single screen. Each new statute would require WhenU to review 50 states' laws to make sure that complying with the new statute would not create a compliance issue with respect to a previously enacted statute.[195]

The difficulty may be overstated. Nationwide homeowners' insurance companies and pharmaceutical companies somehow manage to juggle variations in state laws.[196] WhenU argues that anything making its software more cumbersome to download would reduce its client base.[197] But if consumers

---

commercial speech. *Id.* ¶¶ 71–76. Second, Utah violated the Federal Copyright Act by impermissibly expanding the rights of copyright holders. *Id.* ¶¶ 93–98. Third, WhenU alleged a violation of the state constitution because the statute "chilled free expression," did not "operate uniformly," and took WhenU's property "by denying WhenU economically viable use of its licensed, installed user base." *Id.* ¶¶ 77–92, 99–104. Because the court did not grant the injunction based on those causes of action, they are not discussed further in the text of this Comment.

193. *Id.* ¶ 56.

194. *Id.* WhenU has a valid point here; computers are as mobile as the consumers who own them. In addressing jurisdictional issues, state legislators must consider consumers who own portable computers and travel. If a CEO who lives in Virginia and works in Washington, D.C. takes a company notebook computer to Utah, signs onto the Internet and gets spyware from Massachusetts, which laws apply? Questions like this make a good case for adopting federal legislation.

195. *Id.* ¶ 57.

196. *See* Craig M. Collins, *Flood Insurance Is Not All Created Equal*, 74 N.D. L. REV. 35, 35 (1998) (noting most types of homeowners' insurance is governed by state law); *see also* P. Greg Gulick, *E-Health and the Future of Medicine: The Economic, Legal, Regulatory, Cultural, and Organizational Obstacles Facing Telemedicine and Cybermedicine Programs*, 12 ALB. L.J. SCI. & TECH. 351, 370 (2002) ("[E]ach individual state has the power to regulate the sale of pharmaceuticals within their borders.").

197. WhenU Complaint, *supra* note 83, ¶ 59.

want WhenU's software, as WhenU claims,[198] would they mind an installation form with a drop-down box in order to specify state citizenship before beginning installation?

2. Notice and Consent Requirements. Utah's Act identified five requirements, set out below, for obtaining a consumer's consent to install software. WhenU addressed each of these requirements in its pleading and attempted to show why the requirement was unenforceable.[199] In doing so it made two compelling arguments and three weak arguments.

First, the software must display a license agreement "presented in full" and "written in plain language."[200] WhenU argued that "presented in full" lacked specificity—did it mean that the agreement had to be presented on one screen, without a scroll-bar?[201] That argument sounds contrived until one recalls *Specht v. Netscape*, where a company suffered litigation, in part for hiding a link to its license agreement on the "next scrollable screen."[202] The statute also did not make clear whether browsewrap licenses would comply with the "presented in full" requirement.[203] WhenU made a valid argument; the statute was unclear.

Second, the Act required the software to give "a clear and representative full-size example of each type of advertisement that may be delivered."[204] WhenU responded that it could not comply because it had so many types of advertisements and because it frequently added more.[205] Perhaps WhenU could provide consumers updates through pop-up notices that contain hyperlinks to new EULAs that explain the new advertisements and provide consumers an opportunity to assent to the updated service.[206] Unfortunately, the statute's

---

198. *Id.* ¶ 37 ("The use of SaveNow is entirely consensual. Consumers obtain the SaveNow software because they choose to do so.").

199. *Id.* ¶ 55(a)–(e).

200. Spyware Control Act, 2004 Utah Laws Ch. 363, sec. 2, § 13-39-102(4)(c)(i)(A), *recompiled & codified as* UTAH CODE ANN. § 13-40-102 (2004), *amended by* UTAH CODE ANN. § 13-40-102 (2005).

201. WhenU Complaint, *supra* note 83, ¶ 55(a).

202. Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 30 (2d Cir. 2002).

203. Spyware Control Act, § 13-39-102(4)(c)(i)(A)(I).

204. *Id.* at § 13-39-102(4)(c)(i)(C).

205. WhenU Complaint, *supra* note 83, ¶ 55(c). WhenU's advertisement forms include "pop-ups, pop-unders, panoramics, scroll-ups and sliders." *Id.*

206. Using pop-ups to communicate with consumers who have the company's adware installed is not only possible, it has been done. In June 2005, 180Solutions sent pop-up notices to twenty million consumers, notifying them that they had the 180Solutions software and providing removal instructions. Tynan & Spring, *supra* note 2, at 73.

wording does not make clear whether these approaches would comply.[207]

WhenU's less compelling arguments address the additional burdens the statute would place on WhenU. First, WhenU complained that the statutory provision requiring the software to give "notice of the collection of each specific type of information to be transmitted as a result of the software installation"[208] would unreasonably require WhenU to inform consumers about mundane details that have "nothing to do with user privacy," like the fact that the software reports the computer's IP address.[209] However, IP addresses can and do identify individual computers on the Internet.[210] Anyone with access to the records of the computer's Internet service provider (ISP) could determine the identity of the subscriber.[211] Furthermore, it is hard to grasp why WhenU feels adding the words "consumer's IP address" to a list of the information reported by the software is so difficult.

Second, the statute required software to give "a truthful statement of the frequency with which each type of advertisement may be delivered."[212] WhenU balked at this provision, saying it could not possibly know such information because the browsing habits that trigger the advertisements will vary from consumer to consumer.[213] WhenU overstates the difficulty. If the frequency of pop-ups depends on the consumer's browsing habits, WhenU could simply explain the variables in its EULA and offer a representative example of a consumer who browses ten websites in an hour.

Finally, Utah's Act required "for each type of advertisement delivered by the software, a clear description of a method by which a user may distinguish the advertisement by its appearance from an advertisement generated by other software

---

207. Spyware Control Act, § 13-39-102(4).

208. *Id.* § 13-39-102(4)(c)(i)(B).

209. WhenU Complaint, *supra* note 83, ¶ 55(b).

210. A couple of examples demonstrate the point. The Recording Industry Association of America (RIAA) uses IP addresses to identify the consumer's Internet Service Provider and to subpoena the names of illegal downloaders. *See In re* Charter Commc'ns, Inc., 393 F.3d 771, 774 (8th Cir. 2005) (discussing the RIAA's use of IP addresses to identify illegal downloaders). Law enforcement uses IP addresses to track down cybercriminals. *See* United States v. Hamilton, 413 F.3d 1138, 1140–41 (10th Cir. 2005) (describing how the police tracked use of child pornography websites by the IP addresses of visitors).

211. *See Charter Commc'ns*, 393 F.3d at 774 (elucidating how IP addresses link to specific computers); *Hamilton*, 413 F.3d at 1140–41 (same).

212. Spyware Control Act, § 13-39-102(4)(c)(i)(D).

213. WhenU Complaint, *supra* note 83, ¶ 55(d).

services."[214] WhenU argued that its advertisements are clearly branded with the WhenU name, the "SaveNow" service mark, and a neon green "$" logo.[215] It complained that the statute would require explaining what these "obvious branding symbols" mean.[216] It is unclear why it would be a hardship to simply state, "Advertisements are clearly branded with the WhenU name, 'SaveNow' service mark, and neon green "$" logo."

3. The Outcome. However critical some may be of WhenU's arguments,[217] they worked. The court granted the injunction in June 2004 on grounds that the statute violated the Commerce Clause of the U.S. Constitution.[218] The statute banned delivery of pop-up advertisements and created complex protocols for obtaining consumer consent; both features violated the Constitution, according to the court.[219]

Utah revised its statute in 2005; the new statute prohibits delivery of pop-up ads through spyware if the advertisement "is displayed in response to a specific mark" or web address, infringes on a trademark, and is purchased by someone other than the mark's owner, licensee, or authorized user or agent of the mark.[220] The revision also removed from the definition of spyware all language requiring specific means of obtaining consent.[221] It remains too soon to tell whether Utah's revised statute will withstand another challenge from WhenU.

E. Critics of State Legislation

State legislation has a number of detractors. First and foremost, critics of states' antispyware legislation echo WhenU by decrying a lack of uniformity in the states' laws and argue only a federal law would be workable.[222] One critic argues that all state

---

214. Spyware Control Act, § 13-39-102(4)(c)(i)(E).

215. WhenU Complaint, *supra* note 83, ¶ 55(e).

216. *Id.*

217. *See* Ben Edelman, *Report from* WhenU v. Utah, June 11, 2004, http://www.benedelman.org/news/061104-1.html (dismissing WhenU's claims that compliance would be difficult and costly).

218. Transcript of Proceedings at 5–6, WhenU.com, Inc. v. Utah, No. 040907578, (3d Jud. Dist. Ct., Salt Lake County, Utah Apr. 12, 2004), *available at* http://www.benedelman.org/spyware/whenu-utah/pi-ruling-transcript.pdf.

219. *See id.* at 4–6.

220. UTAH CODE ANN. § 13-40-201(1) (2005).

221. *Compare id.* § 13-40-102(8)(b), *with* H.B. 323, 2004 Gen. Sess., sec. 1, § 13-39-102(4)(c) (Utah 2004) (demonstrating the change from the original bill, which specified how spyware must obtain consent, to the current statute, which does not even mention consent).

222. *See, e.g.*, Peter S. Menell, *Regulating "Spyware": The Limitations of State*

spyware legislation is subject to the same inherent constitutional infirmity as the Utah statute.[223] Based on *WhenU.com v. Utah*, that prediction seems at least possible. In the final analysis, the most likely impact of state legislation will be its role in encouraging promulgation of comprehensive federal legislation.

III. FEDERAL SOLUTIONS

In discussing the federal legislature's efforts to address the spyware problem, Senator Ron Wyden said, "We're pushing this rock up the hill."[224] Whether Senator Wyden intended his statement as a metaphor for Capitol Hill and the difficulties of creating and passing a good spyware bill, or as an allusion to Sisyphus and his stone,[225] the senator's comments seem apt. In 2004, the House of Representatives passed the Securely Protect Yourself Against Cyber Trespass Act, or "SPY ACT."[226] The Senate took no action, and the bill died.[227] The House passed it again in 2005, and again the bill stalled in the Senate.[228] Currently, Congress has competing, cleverly-named statutes, I-SPY and SPY BLOCK Acts, on the table.[229] Unfortunately, the

---

"Laboratories" and the Case for Federal Preemption of State Unfair Competition Laws, 20 BERKELEY TECH. L.J. 1363, 1375–76 (2005) (suggesting that businesses on the Internet will comply with the most restrictive state laws to reduce potential liability); Jeffrey M. Becker & Purvi J. Patel, *Recent Trademark Challenges in Cyberspace and the Growth of the Initial Interest Confusion and Nominative Fair Use Doctrines*, 9 COMPUTER L. REV. & TECH J. 1, 29–30 (2004) (noting that challenges to state spyware legislation are likely due to the potential impact on advertising businesses).

223. *See* Susan P. Crawford, *First Do No Harm: The Problem of Spyware*, 20 BERKELEY TECH. L.J. 1433, 1436 & n.5 (2005) (observing that the Utah statute was "widely imitated in other states" and that the state bills implicate dormant Commerce Clause and First Amendment issues).

224. McCracken, *supra* note 37, at 17.

225. According to Homer, Sisyphus was cursed for eternity to push a large stone towards the top of a hill, only to have it roll back down again. ALBERT CAMUS, THE MYTH OF SISYPHUS, AND OTHER ESSAYS 88 (Justin O'Brien trans., Vintage Books 1960) (1955).

226. Securely Protect Yourself Against Cyber Trespass Act, H.R. 2929, 108th Cong. (2004) (specifying that the statute may be called "SPY ACT").

227. Thomas (Library of Congress), H.R. 2929, http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR02929:@@@X (last visited Sept. 20, 2006) (indicating that the Senate took no action on the bill once received).

228. Securely Protect Yourself Against Cyber Trespass Act, H.R. 29, 109th Cong. (2005) (reinstating the 2004 bill); Thomas (Library of Congress), S.687, http://thomas.loc.gov/bin/bdquery/z?d109:SN00687:@@X (last visited Sept. 20, 2006) (indicating the Senate has taken no constructive action regarding the SPY ACT since its reintroduction to the Senate in March of 2005).

229. *See* Internet Spyware (I-SPY) Prevention Act of 2005, H.R. 744, 109th Cong. (2005) (addressing unauthorized use of protected computers); Software Principles Yielding Better Levels of Consumer Knowledge, S. 687, 109th Cong. (2005) (addressing surreptitious downloads of software). Obviously someone puts a great deal of thought into these creative acronyms. As some readers may recall, *I Spy* was a television program in

federal legislation under consideration, like the state laws already discussed, does not adequately address the issue of what constitutes proper consent.

A. *SPY ACT*

Section 3 of the SPY ACT is entitled "Prohibition of Collection of Certain Information Without Notice and Consent."[230] It describes notice as "clear and conspicuous notice in plain language."[231] The Act enumerates some requirements that must be met to constitute adequate notice but leaves the details to the Federal Trade Commission.[232] That said, even the general requirements provided by the SPY ACT face criticism.

First, notice must be clearly distinguished from "any other information visually presented contemporaneously on the computer."[233] This wording suffers the same vagaries found in Utah's statute: Many spyware installations already distinguish notice by offering a browsewrap license.[234] The hyperlinks to these licenses appear as underlined, differently colored text.[235] The statute does not make clear whether this form of presentation would satisfy the requirement.[236]

Second, if the software either collects and transmits personal information, including web browsing history, or if the software uses that information to send advertising to the computer, the notice must disclose such activity.[237] The installation program then must ask consumers to accept the software before proceeding.[238] The Act offers an example: "This program will collect and transmit information about you and will collect

---

the 1960s. *See I Spy: So Long, Patrick Henry* (NBC television broadcast Sept. 15, 1965) (the series premiere). In keeping with the theme, should Congress need other creative acronyms in the future, I offer Unscrupulous Networking Compels Law Enforcement ("UNCLE"); and The House of Representatives' Ultimate Spyware Hijack ("THRUSH"). *See The Man from U.N.C.L.E.: The Vulcan Affair* (NBC television broadcast Sept. 22, 1964) (introducing rival organizations U.N.C.L.E. and THRUSH).

230. H.R. 29, 109th Cong. § 3 (2005).

231. *Id.* § 3(c)(1).

232. *See id.* §§ 3(c), 4(a) (outlining basic provision for notice, explicitly empowering the Federal Trade Commission (FTC) to provide details and vesting enforcement power of the Act in the FTC).

233. *Id.* § 3(c)(1)(A).

234. *See supra* text accompanying notes 138–144 (describing browsewrap licenses).

235. *See* Edelman, *supra* note 185 (deflating the argument that statutes that require different-styled text to identify notices will improve the situation, noting that hyperlinks already achieve this result).

236. H.R. 29, 109th Cong. § 3 (2005) (neglecting to mention hyperlinks or browsewrap licenses).

237. *See id.* § 3(c)(1)(B).

238. *See id.* § 3(c)(1)(C).

information about Web pages you access and use that information to display advertising on your computer. Do you accept?"[239] There are two opposing criticisms to this provision.

One side argues it is too lax.[240] The notice given need not follow the exact wording found in the Act, so long as the notice is "substantially similar."[241] A sixty-page agreement with an embedded disclosure might be considered substantially similar.[242] The other side argues that no notice should be required at all because the notices themselves will become annoying pop-up disclosures, and consumers will not understand the notices anyway: "In effect, the government will be requiring users to click helplessly along, assenting to something they do not understand over and over again."[243] This argument has little merit. It dismissively characterizes the majority of Internet users as unsophisticated operators who do not care to be informed about the installation of third-party software on their computers.[244] The argument assumes consumers will click "Accept" just to make the notification screen go away. While that may be true of some Internet surfers, other people telecommute, or otherwise use computers daily for their livelihood.[245] These people are undoubtedly interested in what software is installed on their machines and are entitled to a choice. If consumers do not understand the license agreements, the right solution is to require plain language licenses, not to eliminate notice.

The statute requires that the software company provide computer users with the option to see details regarding any bundled software, the type of information collected and sent, and the purpose for which that information is collected.[246] The statute does not require that the computer user actually see this information. This requirement implicitly allows browsewrap

---

239. *Id.* § 3(c)(1)(B)(iii).

240. *See* Edelman, *supra* note 185 (dissecting the problems with H.B. 29).

241. H.R. 29 § 3(c)(1)(B).

242. *See* Edelman, *supra* note 185.

243. Crawford, *supra* note 223, at 1457.

244. MARY J. CULNAN, BENTLEY SURVEY ON CONSUMERS AND INTERNET SECURITY: SUMMARY OF FINDINGS 2 (2004), *available at* http://www.bentley.edu/events/iscw2004/survey_findings.pdf (discussing survey findings that show a "majority of the public is concerned about Internet security and believe each person can make a difference in helping secure the Internet").

245. David L. Margulius, *Dream of Telecommuting May Become More Elusive*, INFOWORLD, Feb. 3, 2006, http://www.infoworld.com/article/06/02/03/74943_06OP analysts_1.html (estimating the number of employees who telecommute on a regular basis at almost one quarter of "corporate workers").

246. H.R. 29 § 3(c)(1)(D).

licenses for bundled software.[247] The statue does not require the software to display a separate notice for each bundled program, so long as the notice displayed applies to all of them.[248] Thus the statute encourages bundling by making it convenient and permits companies to continue hiding disclosures in lengthy text that the consumer might never see.

B. I-SPY

I-SPY defines penalties for unauthorized activities related to computers.[249] It states that the intentional, unauthorized installation of a program that transmits information or impairs the computer's security onto a protected computer is punishable by a fine or up to two years in prison, or both.[250] The software is considered illegal only if, "with the intent to defraud or injure a person or cause damage to a protected computer," it either (1) gathers or transmits personal information or (2) intentionally impairs the machine's security.[251] Of the three federal bills compared in this Comment, I-SPY does the least to protect consumers against spyware.[252] First, it does not define how authorization might be obtained.[253] Second, and more damning, its mens rea requirement of intent to damage, defraud, or injure would be difficult to prove.[254]

C. SPY BLOCK

The Software Principles Yielding Better Levels of Consumer Knowledge ("SPY BLOCK") Act is currently in the Senate.[255] SPY BLOCK generally prohibits the installation of software without notification.[256] Unfortunately, nothing in the statute defines what

---

247. *See supra* Part I.E (describing the browsewrap license as being available to the consumer through a hyperlink rather than visible on the screen).

248. H.R. 29 § 3(c)(2) (allowing a single notice for multiple programs).

249. *See* H.R. 744, 109th Cong. (as received by Senate, May 24, 2005).

250. *Id.* § 2(a) (amending 18 U.S.C. § 1030A(b) with language specifying the penalty).

251. *Id.* (itemizing the elements of the offense).

252. *See* Michael D. Lane, Student Article, *Spies Among Us: Can New Legislation Stop Spyware from Bugging Your Computer?*, 17 LOY. CONSUMER L. REV. 283, 304 (2005) (assessing I-SPY as helpful in the fight against identity theft, but concluding "it leaves something to be desired in the fight against spyware").

253. H.R. 744, 109th Cong. § 2(a) (requiring authorization, defining the phrase "exceeds authorized access," but remaining silent on the definition of legal authorization).

254. *Id.*

255. Thomas (Library of Congress), S.687, http://thomas.loc.gov/cgi-bin/bdquery/z?d109:SN00687:@@@X (last visited Sept. 20, 2006) (tracking the Senate bill and recording that in June 2006, the Senate placed the bill on the calendar to consider).

256. S. 687, 109th Cong. § 2(a)(1) (2005).

constitutes sufficient notice.[257] Most spyware companies sued under this Act will be granted summary judgment with nothing more than a two-page motion and a copy of a EULA that provides some sort of notice.[258]

With the shortcomings reviewed above in the proposed federal acts, perhaps it is a good thing that none have passed yet. Congress would do well to review and repair the flaws now, before passing the laws, rather than to pass flawed legislation with the expectation of revising and amending in the future.

IV. EXISTING CAUSES OF ACTION

Some critics argue that the deceptive abuses targeted by federal spyware bills could be addressed by existing causes of action.[259] They argue that any new act will only undermine the fight against spyware by invalidating existing remedies[260] and make some intrusive techniques lawful.[261] As discussed below, some spyware companies have already been hauled into court under existing causes of action. This section examines remedies already in use and whether they render further legislative action unnecessary.[262]

A. FTC Cases

In 2005, the FTC began prosecuting spyware companies vigorously for deceptive acts.[263] The FTC's strategies are

---

257. *Id.* §§ 1–14 (suffering the same shortfall as H.R. 744, 109th Cong. § 2(a) in that it requires authorization but fails to define how to obtain authorization).

258. *See supra* text accompanying notes 169–173.

259. *See, e.g.*, Edelman, *supra* note 185 (noting that many of the deceptive practices prohibited in the SPY ACT are already illegal).

260. *See id.*

261. *See* Tynan & Spring, *supra* note 2, at 80 (expressing the pessimistic view of consumer advocates on the prospect for improvement through federal legislation on this issue).

262. One currently existing law sometimes mentioned is the Computer Fraud and Abuse Act of 1986 (CFAA), § 18 U.S.C. 1030(a) (2000 & Supp. II 2004). The Act forbids accessing a protected computer without authorization or exceeding authorized access knowingly and with intent to defraud. *Id.* § 1030(a)(4). However, the claimant is required to show at least $5,000 in damage over any one year period in order to bring suit. *Id.* There is some debate as to whether the $5,000 in damage pertains to one computer or an aggregation of damages. *See* Lane, *supra* note 252, at 290–93 (discussing courts' divergent applications of the CFAA's threshold amounts). Either way, the threshold is prohibitive for individuals who would bring claims against spyware companies. At today's prices, a person could be forced to replace his or her computer several times before reaching the required $5,000. *See id.* at 291. Therefore, this Act is not useful in the spyware context and is not further discussed.

263. *Majoras Statement*, *supra* note 37, at 1–2 (noting the initiation of five enforcement actions in the past year).

especially important to consider because the federal legislation currently under consideration gives enforcement authority to the FTC.[264] A string of cases brought in 2005 sheds some light on the FTC's position regarding spyware.

The FTC recently sued Seismic Entertainment for deceptive practices.[265] The company allegedly uses vulnerabilities in Microsoft's web browser to install software on victims' machines without their knowledge or authorization.[266] The software changes the browsers' homepages, alters search engines, barrages victims with "an incessant stream of pop-up advertisements,"[267] and causes computer malfunctions, slow response times, or even complete system failure.[268] The software also downloads and installs other spyware programs.[269] The FTC's allegation of deception hinges on the fact that Seismic Entertainment caused these changes without permission from the computers' owners, implicitly alleging that drive-by downloads are, by definition, deceptive.

In another action, the FTC demonstrated disapproval of browsewrap licenses.[270] The FTC sued Advertising.com for offering consumers an antispyware product called SpyBlast that in fact deployed spyware.[271] The FTC alleged Advertising.com failed to provide sufficient notice that the SpyBlast program actually installed its own spyware that collected the consumer's browsing history for directed advertising.[272] According to the FTC, consumers received pop-ups informing them that their machines were susceptible to hackers.[273] Consumers who clicked on the ad received a dialog box offering to install SpyBlast.[274] Although the dialog box included a hyperlink to the license, it allowed the consumer to accept by clicking "Yes" without viewing

---

264. H.R. 29, 109th Cong. § 4(a) (2005); S. 687, 109th Cong. § 8(a) (2005).

265. Complaint for Injunction and Other Equitable Relief ¶ 1, FTC v. Seismic Entm't Prods., Inc., No. 04CV377, 2005 WL 2309585 (D.N.H. Oct. 6, 2004).

266. *Id.* ¶¶ 10, 20.

267. *Id.* ¶¶ 10, 21.

268. *Id.* ¶ 21.

269. *Id.* ¶¶ 10, 16–17.

270. *See* FED. TRADE COMM'N, DOT COM DISCLOSURES: INFORMATION ABOUT ONLINE ADVERTISING 7–10 (2000), *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.pdf [hereinafter DOT COM DISCLOSURES] (discouraging the use of hyperlinked disclosures such that the disclosure is separated from the relevant claims).

271. *See* Complaint ¶¶ 3, 6, 8, 9, *In re* Advertising.com, Inc., No. C-4147, 2005 WL 2329812 (Fed Trade Comm'n Sept. 12, 2005), *available at* http://www.ftc.gov/os/caselist/0423196/050916comp0423196.pdf.

272. *Id.* ¶¶ 8–9.

273. *Id.* ¶ 5.

274. *See id.*

the license.[275] Consumers who followed the link received notice that the program would deliver pop-up ads, report their IP address, and collect browsing history.[276] The FTC asserted that the failure to provide adequate disclosure of the bundled spyware constituted a deceptive trade practice.[277] Unfortunately, the case settled and there remains no legal precedent.[278] Under the terms of that settlement, for the next twenty years, any product offered by Advertising.com that purports to enhance security or privacy must display a clear and prominent disclosure to consumers that they will be receiving advertisements.[279] The disclosure must be unavoidable and displayed prior to downloading any software.[280]

If applied to other cases, this approach will help eliminate the practice of acquiring consumers' acceptance to EULAs they never see, but making EULAs unavoidable does not address the practice of using lengthy, convoluted EULAs to discourage consumers from reading them. The FTC has yet to take a clear stance on lengthy EULAs. In a sample case, the FTC obliquely addressed lengthy EULAs in its claim against Odysseus Marketing. The FTC alleged that Odysseus Marketing advertised software that would permit anonymous peer-to-peer file sharing, but instead the software bundled a spyware program called Clientman that "secretly downloads dozens of other software programs, degrading consumers' computer performance and memory."[281] This misinformation would probably qualify as a deceptive practice by anyone's definition.

More interesting is the FTC's charge that Odysseus Marketing hid its disclosure within a lengthy EULA on the website.[282] The FTC additionally charged Odysseus with

---

275. *See id.* ¶¶ 5–6.

276. *See id.* ¶ 6.

277. *Id.* ¶¶ 9–10 ("The failure to adequately disclose [the nature of the product being downloaded], in light of the representation made, was and is, a deceptive act or practice.").

278. *See* Press Release, Fed. Trade Comm'n, Advertising.com Settles FTC Adware Charges, (Aug. 3, 2005), http://www.ftc.gov/opa/2005/08/spyblast.htm.

279. *See id.*; Agreement Containing Consent Order at 3, 5, *In re* Advertising.com, Inc., No. C-4147, 2005 WL 2329812 (Fed Trade Comm'n 2005), *available at* http://www.ftc.gov/os/caselist/0423196/050803agree0423196.pdf.

280. Consent Order, *In re Advertising.com*, No. 042-3196, at 3.

281. Press Release, Fed. Trade Comm'n, FTC Seeks to Halt Illegal Spyware Operation (Oct. 5, 2005), http://www.ftc.gov/opa/2005/10/odysseus.htm [hereinafter FTC Spyware Press Release]; *see also* Complaint for Injunction and Other Equitable Relief, FTC v. Odysseus Marketing, Inc., No. 05-CV-00330, 2005 WL 3026853 (D.N.H. Sept. 21, 2005).

282. FTC Spyware Press Release, *supra* note 281 ("[T]hey hide their disclosure in the middle of a two-page end-user licensing agreement buried in the 'Terms and Conditions' section of their Web site.").

deliberately making the software "difficult to detect and impossible to remove using standard software utilities."[283] The FTC claims these practices are unfair, deceptive, and in violation of the FTC Act.[284] Unfortunately, the FTC did not make clear whether the defendant's deception arose purely from the use of a lengthy EULA, or if the EULA merely contributed as one element in a series of practices that, in the aggregate, created the deceptive practice.[285] It is too soon to tell what the result of the FTC litigation will be. There is cause for cautious optimism, but the impact of these cases will not be clear until a court rules on the FTC's arguments.

B. Trespass to Personal Property

1. A Cause of Action Reborn. In 1996, online service provider CompuServe faced the growing problem of unsolicited commercial e-mail (spam) on its servers.[286] One particular company, Cyber Promotions, Inc., continued to bombard CompuServe's servers with spam, even after CompuServe sent cease-and-desist letters.[287] CompuServe sought to enjoin Cyber Promotions from sending spam to any CompuServe account.[288] In searching for potential causes of action against the spammer, attorneys for CompuServe dusted off their history books and found trespass to chattels, now called trespass to personal property.[289]

According to the Restatement of Torts, a person commits trespass to personal property when he or she intentionally dispossesses another of the property or uses or intermeddles with another's property.[290] While dispossession does not require a showing of actual damages, intermeddling does.[291] At the time of *CompuServe*, trespass to chattels "had been largely relegated to a

---

283. *Id.* Uninstalling applications is supposed to be as easy as launching a utility called "Add or Remove Programs," selecting the unwanted software, and clicking a button that says "Change/Remove." MICROSOFT WINDOWS XP PROFESSIONAL, *supra* note 31, at 1416–17.

284. FTC Spyware Press Release, *supra* note 281.

285. *Id.* (describing the case brought by the FTC).

286. CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1017 (S.D. Ohio 1997).

287. *See id.*

288. *Id.* at 1020.

289. *Id.*

290. RESTATEMENT (SECOND) OF TORTS § 217 (1965).

291. *Id.* § 218 cmts. d & e.

historical note in legal textbooks,"[292] but CompuServe moved forward with this cause of action, seeking to enjoin Cyber Promotions.[293] The court approved, albeit weakly: "While authority under Ohio law respecting an action for trespass to chattels is extremely meager, it appears to be an actionable tort."[294]

The spammers suggested that trespass to personal property required a showing of physical dispossession or damage, but the court held that diminution of the personal property's quality, condition, or value provided a sufficient predicate for liability.[295] The court found that Cyber Promotions' spam diminished CompuServe's available server disk space and processor time, inconvenienced CompuServe's clients, prompted complaints from CompuServe's clients, and even caused service cancellations.[296] These results sustained the trespass to personal property action.[297]

This decision breathed new life into the action for trespass to personal property, and other Internet email providers such as America Online and Hotmail brought similar claims in suits against spammers.[298] However, the courts have not characterized unsolicited commercial email as a per se trespass to personal property. For example, Intel sued a former employee for using the company's server to send current employees email critical of Intel's employment practices.[299] Intel claimed trespass to personal property.[300] Intel argued the content of the email created dissent among employees, diminished productivity, and increased costs because of attempts to block the critical email.[301] The court, however, held there was no trespass because the electronic communications did not impair the functioning of Intel's computer systems.[302]

In *eBay, Inc. v. Bidder's Edge*, the court identified two elements for a computer trespass: "(1) defendant intentionally

---

292. Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219, 1230 (N.D. Ill. 2005).

293. *CompuServe*, 962 F. Supp. at 1020.

294. *Id.* at 1021.

295. *Id.* at 1021–22 (citing RESTATEMENT (SECOND) OF TORTS § 218(b)).

296. *Id.* at 1022–23.

297. *Id.* at 1023.

298. *See, e.g.*, Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 549 (E.D. Va. 1998); Hotmail Corp. v. Van Money Pie, Inc., No. C98-20064 JW, 1998 U.S. Dist. LEXIS 10729, at *8–9 (N.D. Cal. Apr. 16, 1998).

299. Intel Corp. v. Hamidi, 71 P.3d 296, 299 (Cal. 2003).

300. *Id.*

301. *Id.* at 300.

302. *Id.*

and without authorization interfered with plaintiff's possessory interest in the computer system; and (2) defendant's unauthorized use proximately resulted in damage to plaintiff."[303] In this case, Bidder's Edge employed programs called robots to scan eBay's site, causing a load on eBay's servers estimated at 1.53%.[304] The court found this small load sufficient damage to support an injunction because a denial of injunctive relief could result in other companies using robots and the aggregate effect could overwhelm eBay's servers.[305]

Register.com, Inc. v. Verio, Inc.,[306] where the court upheld a preliminary injunction against the use of robots, arguably broadened *eBay*. The court did not focus on quantifying the load placed on the server but rather reasoned that unauthorized robots interfere with a finite amount of computer resources, risking congestion that could disrupt the plaintiff's authorized operations.[307]

2. Application to Spyware. Applying the above principles, any software that arrives on a consumer's computer uninvited and impairs the functioning of the computer system is actionable as trespass to personal property. One of the first cases to use trespass to personal property against spyware is *Sotelo v. DirectRevenue, LLC*.[308] Apparently mindful that the cause of action required a claim of sufficient damages resulting from DirectRevenue's spyware, Sotelo took no chances and claimed every conceivable damage:

> According to plaintiff, Spyware "bombards" users' computers with pop-up advertisements that obscure the web page a user is viewing and "destroys other software on a computer." Plaintiff also alleges that Spyware and the

---

303. eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069–70 (N.D. Cal. 2000).

304. *Id.* at 1066 & n.14. The court defines a software robot as "a computer program which operates across the Internet to perform searching, copying and retrieving functions on the web sites of others." *Id.* at 1060.

305. *Id.* at 1066.

306. Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004).

307. *Id.* at 438–39. For a discussion of *eBay*, *Register.com*, and the evolution of trespass to chattels in a computer context, see Michael R. Siebecker, *Cookies and the Common Law: Are Internet Advertisers Trespassing on Our Computers?*, 76 S. CAL. L. REV. 893, 912–23 (2003) (supporting the application of trespass to chattels to thwart use of cookies, and referencing the *eBay* and *Register.com* cases); Geoffrey D. Wilson, *Internet Pop-up Ads: Your Days Are Numbered! The Supreme Court of California Announces a Workable Standard for Trespass to Chattels in Electronic Communications*, 24 LOY. L.A. ENT. L. REV. 567, 579–89 (2004) (arguing the conclusions reached in these trespass to personal property cases can be applied to adware).

308. Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219, 1229–33 (N.D. Ill. 2005).

> resource-consuming advertisements sent to a computer by Spyware cause computers to slow down, take up the bandwidth of the user's Internet connection, incur increased Internet-use charges, deplete a computer's memory, utilize pixels and screen-space on monitors, require more energy because slowed computers must be kept on for longer, and reduce a user's productivity while increasing their frustration.[309]

Perhaps these damages are somewhat overstated, but the court indulged Sotelo and succinctly summarized the damages caused as over-burdening the plaintiff's resources and diminishing their functionality.[310] The court denied defendant's motion to dismiss for plaintiff's failure to properly plead causation and damages to his computer.[311] The case itself settled in 2006,[312] but denial of the defendant's motion promises to be an important precedent because the court recognized trespass to personal property as a viable claim against spyware.

3. Criticism. While courts have approved of trespass to personal property as a viable option to combat spyware, some academics oppose taking this cause of action out of its historic confines. Professor Dan L. Burk, who specializes in intellectual property and cyberlaw,[313] cautions that the application of trespass to personal property in the computer arena creates a hybrid of real and personal property heretofore unknown.[314] He notes that the hybrid seems to suggest that the exchange of electrons on a network is sufficient cause for a trespass action.[315] He warns that a computer trespass action might go too far by preventing beneficial technologies and leading to a "detrimental over-propertization of the Internet."[316] He suggests that the creation of a computer nuisance action would be more appropriate.[317] The nuisance cause of action would permit the continued, reasonable use of technologies that benefit society yet give companies

---

309. *Id.* at 1230.

310. *Id.* at 1231.

311. *Id.*

312. Eric Benderoff, *Class-Action Suit Dismissed Against Spyware Provider*, CHI. TRIB., Sept. 7, 2006, at C1.

313. Dan L. Burk - Faculty Profiles - University of Minnesota Law School, http://www.law.umn.edu/FacultyProfiles/BurkD.htm (last visited Sept. 20, 2006).

314. *See* Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 33 (2000) (suggesting that cases like *CompuServe* set back common law remedies).

315. *Id.* at 34.

316. *Id.* at 52–53.

317. *Id.* at 53–54.

overwhelmed by unreasonable use a cause of action.[318] Based on the cases discussed above, Professor Burk's criticisms arrive too late; computer trespass is already making inroads as a cause of action and will probably continue to do so unless Congress intervenes.

C. *The Need for Legislation*

With the FTC currently pursuing spyware vendors for deceptive trade practices, and individuals pursuing private causes of action, one may wonder why legislators began to develop state or federal antispyware legislation at all. First, the active involvement of the FTC is a new development.[319] Although the FTC published Internet advertising guidelines for proper notice and consent in 2000,[320] the practices discussed in this Comment show that these guidelines have had little impact. Also, until very recently, the FTC has been slow to prosecute spyware companies.[321] State legislators began considering spyware laws before the FTC became an active player.[322] More significantly, the trespass to personal property remedy does not address the notice and consent issue; a defendant could use its EULA as a shield against such claims, arguing there can be no trespass if there was consent.[323] One can easily imagine a disclaimer of liability for any damages from the use of the software and an arbitration clause that binds the consumer to remote and inconvenient locales.[324] As a result, trespass to

---

318. *Id.*

319. *Majoras Statement*, *supra* note 37, at 1–3, 8 (describing the FTC's initiation of new enforcement actions over the past year and placing a priority on spyware investigations and enforcement).

320. DOT COM DISCLOSURES, *supra* note 270, at 4–14 (calling for clear and conspicuous notice and plain language in a company's Internet advertising).

321. Edelman, *supra* note 185 ("Experience shows the FTC to be slow to pursue spyware perpetrators: The FTC has filed only a single anti-spyware case to date [in January 2005], and has failed to act on (among scores of other problematic activities) the installation of dozens of programs through security holes, even when documented in research posted months ago . . . .").

322. *See* Edelman, *supra* note 165 (providing links to forty pieces of legislation that consider spyware, most of which were passed or introduced in 2005 or before).

323. *See* Lane, *supra* note 252, at 301.

324. In an extreme example, one software bundle had a forum selection clause subjecting the agreement to the laws of an island in eastern Africa. Ben Edelman, The PacerD Installation Bundle, http://www.benedelman.org/spyware/installations/pacerd (last visited Sept. 20, 2006). Courts should not enforce such a provision for public policy reasons. *See* Williams v. Am. Online, Inc., No. 00-0962, 2001 Mass. Super. LEXIS 11, *10 (Mass. Super. Ct. Feb. 8, 2001) (suggesting an arbitration provision requiring Massachusetts consumers to bring suit in Virginia when their damages amount to only a few hundred dollars would be against public policy), *cited in* Jane K. Winn, *Contracting Spyware by Contract*, 20 BERKELEY TECH. L.J. 1345, 1352 (2005).

personal property appears to be a remedy only for individuals who are the victims of drive-by downloads, and not a true panacea for the myriad ills of spyware. Only strong legislation will give all spyware victims an effective claim to bring to court.

V. CONCLUSION

Clearly the goal of an effective and comprehensive solution to the spyware problem will not be reached anytime soon. An effective policy against spyware abuses requires bold change, and such change always meets powerful resistance.

First and foremost, we need federal laws. Federal laws would provide uniformity, and they would be immune to the type of Commerce Clause attack WhenU unleashed on Utah.[325] To be effective, however, laws must be free from the loopholes described in this Comment. They must identify specific protocols for acquiring authorization to install software. Protocols should include standardized language and define formatting and placement requirements of notice and consent clauses so that consumers can make informed decisions about the software before installation. Browsewrap licenses should be discouraged as a matter of public policy because consumers might not realize there is an underlying contract. This is especially true when the terms permit invasive access to a consumer's data. Laws should require a separate EULA for each application in a bundle to alert consumers and help them make informed choices. For reasons of public policy, behaviors like resisting detection and removal should be actionable whether or not the consumer accepted a EULA. Consumers should not have to prove intentional damage or deception to bring a claim.

Second, retail and service companies should bear some responsibility for the deployment of improperly authorized software that advertises their products. As explained previously, it is their money that drives and motivates the spread of spyware.[326] They are in the best position to effect change. Retail or service companies facing potential liability for illegal spyware would more closely monitor advertising brokers and discourage the spread of spyware.

Finally, if the FTC is to become the national enforcer against spyware, it must stop trying to build a consensus with an industry that wants no regulation at all. If Congress does not pass federal laws defining strict and clear requirements, then the

---

325. *See* discussion *supra* Parts II.D.1–3.

326. *See* discussion *supra* Part I.C.

FTC must publish guidelines based on the enforcement methods at its disposal. These guidelines must establish a definition of spyware and identify what practices it considers deceptive with regard to notice, consent, and browsewrap licenses.

Making the Internet a safer place to work and play remains an achievable goal and a worthwhile pursuit. Spyware companies have already shown they can adapt and innovate; it is time for Congress to show that it can, too.

John Edward Sharp[**]

[**] J.D. Candidate, Dec. 2006; Microsoft Certified Trainer (MCT); Microsoft Certified Systems Engineer (MCSE); Master Certified Novell Instructor (MCNI); Master Certified Novell Engineer (MCNE); CompTIA Certified Technical Trainer (CTT+); Novell CNE of the Year (2001).

***