SPYWARE: COVERTLY INFRINGING ON YOUR INTERNET PRIVACY WHILE CIRCUMVENTING THE FEDERAL LEGISLATION RADAR

TABLE OF CONTENTS

I. Introduction 234
II. Background 236
A. What Is Spyware? 236
1. A "Simple" Definition 236
2. A "Complex" Definition 237
a. Internet Service Providers: An Illustration of Adware. 238
b. Seismic Entertainment Productions, Inc., and SmartBot.Net, Inc.: An Illustration of Spyware. 239
B. How Does Spyware Get into Computers? 241
C. What Does Spyware Do? 244
D. How Is Spyware Being Fought Outside the Courtroom? 245
III. Application of Current Federal Law 246
A. Current Law Overview 246
1. The Federal Trade Commission Act 247
2. The Computer Fraud and Abuse Act 248
3. The Electronic Communications Privacy Act 250
B. Proposed Legislation 252
1. Securely Protect Yourself Against Cyber Trespass Act 252
2. Internet Spyware (I-SPY) Prevention Act of 2005 253
IV. Application of State Law 254
A. Utah's Spyware Control Act 255
B. California's Consumer Protection Against Computer Spyware Act 256
V. Conclusion 256

I. INTRODUCTION

You are sitting in front of your computer in a trance-like state, methodically clicking the mouse as you slowly move it in circles: news, weather, email, sports, shopping, and recipes. You have no particular goal or destination in mind, but it is entertaining, educational, and relaxing. You stop for a moment at a website to read through a particularly interesting article. The article is discussing something called "spyware." You have never heard of spyware until now and as you begin to read the article, you learn that it is a type of computer software program that can cause serious problems. The article begins by listing some of the symptoms a computer may exhibit if it has a spyware problem. As you begin reading the list, you are rudely interrupted by an advertisement that pops up on the screen, obstructing your view of the article. Because you have no desire to purchase 10,000 smiley emoticons, you seamlessly glide your mouse pointer to the small "X" in the upper corner of the advertisement and click. Instead of the advertisement closing as you had hoped, a new web page appears. Again you try to close the window, but it quickly spawns out of control. There must be ten new windows open now, and they show no signs of relenting. Out of frustration and helplessness, you finally resort to a manual shutdown of your computer.

After your computer reluctantly comes back to life, your Internet home page is now a search engine, complete with a matching toolbar that consumes one-third of the viewing area on your computer screen. You also have several new links in your "favorites" folder, including some links to pornographic websites. The pop-up ads are back with a vengeance and this time you embarrassingly wish they were ads for smiley faces. Your computer is now running as if it was the first one ever made and it refuses to respond to anything you ask of it. As if all of that was not enough, someone managed to steal the username and password for your eBay account from your computer, which they subsequently used to place the winning bid on a grilled cheese sandwich.[1] They even found your credit card number, which was also stored on your computer, and went on a very productive shopping spree.

This scenario, while admittedly extreme, demonstrates the very real and devastating capabilities of spyware, the latest threat to Internet

1. For an entertaining account of unique items available for purchase on eBay's Internet auction site, see Fran Henry, *People Say So Long to Discretion on eBay*, THE PLAIN DEALER, Feb. 18, 2005, at E1.

privacy.[2] An interesting analogy has been made between the westward movement of pioneers early in our country's history and the Internet.[3] A thorough analysis certainly is not required to find the striking similarity: a large movement of people into a vast, unknown area, troubled with numerous difficulties while trying to establish organized communities. Today, just as the West has developed into densely populated areas and sprawling metropolises, cyberspace has developed into an electronic world-wide community, accessed by over 900 million people.[4] These millions utilize the Internet daily as a medium for instant communication, shopping, limitless researching, and hundreds of other uses.[5] Although the Internet has proven to be valuable to millions of people, it has not been without costs, as courts and legislatures frequently are called upon to resolve legal issues arising from Internet usage.[6]

A recent addition to the string of Internet legal issues is the use of software programs known as spyware.[7] Despite increasing efforts to educate computer users, many consumers are unfamiliar with spyware and do not take the necessary precautions to keep it from being installed on their computers.[8] Part II of this Note provides general background information about spyware, highlighting the reasons why computer users should be concerned and discussing which specific legal issues arise from the use of spyware.[9] Part II also examines various self-help methods, and their costs, that frustrated consumers are resorting to in trying to keep spyware off of their computers.[10]

Part III discusses current federal statutes that have been invoked to attack spyware and analyzes applicable court cases to determine the

2. *See* H.R. REP. NO. 108-619, at 8, 9 (2004) (providing a brief overview of the capabilities of spyware and adware programs).

3. JAN SAMORISKI, ISSUES IN CYBERSPACE: COMMUNICATION, TECHNOLOGY, LAW, AND SOCIETY ON THE INTERNET FRONTIER 2 (2002).

4. Internet World Stats, World Internet Usage Statistics & Population Stats, http://www.internetworldstats.com/stats.htm (last updated Sept. 30, 2005).

5. *See* ACLU v. Reno, 929 F. Supp. 824, 830–37, 842 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997) (providing a general description of the Internet and its uses).

6. *See generally* JONATHAN BICK, 101 THINGS YOU NEED TO KNOW ABOUT INTERNET LAW (2000) (discussing a variety of legal issues in the context of the Internet); SAMORISKI, *supra* note 3 (discussing issues such as spam emails, privacy, surveillance, tracking, monitoring, hacking, piracy, and obscene material).

7. *Protect Yourself Online*, CONSUMER REP., Sept. 2004, at 12, 12.

8. H.R. REP. NO. 108-698, at 5 (2004).

9. *See* discussion *infra* Part II.

10. *See* discussion *infra* Part II.

effectiveness of those statutes.[11] Part III also explores proposed legislation currently being considered in Congress and contemplates whether it will provide the necessary means for successfully combating the use of spyware.[12] Part IV analyzes state statutes which have been or could be invoked against spyware.[13] Finally, Part V concludes with the argument that the most effective long-term solution to the spyware problem would be broad Internet privacy legislation as opposed to the narrow, more direct statutes currently being considered and implemented.[14]

II. BACKGROUND

A. *What Is Spyware?*

1. *A "Simple" Definition*

In the relatively short history of the Internet, computer experts have compiled a list of computer terms and acronyms lengthy enough to fill a 422-page, computer-specific dictionary.[15] Yet a quick glance in one of these popular computer dictionaries will not yield definitions for terms such as "adware," "malware," "spyware," or "trespassware."[16] The reason is simple: universally accepted definitions for such terms do not currently exist.[17] Recently, the Federal Trade Commission (FTC) sponsored a workshop in which experts from various fields gathered to discuss spyware.[18] For purposes of facilitating uniform discussions at the workshop, the FTC supplied the expert panelists with the following tentative definition of spyware on an FTC Register Notice: "[s]oftware that aids in gathering information about a person or an organization

11. *See* discussion *infra* Part III.
12. *See* discussion *infra* Part III.
13. *See* discussion *infra* Part IV.
14. *See* discussion *infra* Part V.
15. *See* BRYAN PFAFFENBERGER, WEBSTER'S NEW WORLD COMPUTER DICTIONARY (10th ed. 2003).
16. *See id.* at 15, 226, 352, 378.
17. FTC, Monitoring Software on Your PC: Spyware, Adware, and Other Software 17–18 (Apr. 19, 2004) (transcript available at http://www.ftc.gov/bcp/workshops/spyware/transcript.pdf) [hereinafter FTC Spyware Panel] (statement of Ari Schwartz, Associate Director of the Center for Democracy & Technology).
18. *Id.* at 3–7 (listing panel members representing many industry-leading companies such as Dell Computers, McAfee Security, Semantic Corporation, America Online, and Microsoft).

without their knowledge, and that may send such information to another entity without the consumer's consent, or that asserts control over computers without the consumer's knowledge."[19] The experts on the panel agreed that the FTC definition was accurate, with the exception that some indicated it may be too broad.[20] Other terms such as "malware," "trespassware," "snoopware," and "scumware" are all variations of spyware.[21] The more egregious variety of spyware has sometimes been dubbed "trespassware" or "malware."[22] For purposes of the remainder of this Note, I will place all of the terms into two categories: (1) adware; and (2) spyware (including alternative terms such as "malware" and "trespassware").

2. *A "Complex" Definition*

Generally, spyware and adware employ the same technology, but in different ways.[23] Probably the easiest way to understand the difference between the two is to think of a sliding scale. On one end is completely legitimate adware, which is software-based advertising that the user consents to receiving.[24] On the other end of the scale is spyware. Then, think of the program in terms of how it operates, considering important key factors such as notice (whether users are fully aware that the spyware is being installed onto their computers), control (whether once the program is installed, users can easily remove all the software that was installed), and consent (whether users are clearly informed about what the program will

19. *Id.* at 16–17 (statement of Thomas B. Pahl, Assistant Director, FTC) (internal quotation omitted).

20. *Id.* at 22–23 (statement of Avi Naider, President & CEO, WhenU.com, Inc.).

21. *Id.* at 15 (statement of Thomas B. Pahl, Assistant Director, FTC); *see also* Lee Gomes, *Spyware Is Easy to Get, Difficult to Remove, Increasingly Malicious*, WALL ST. J., July 12, 2004, at B1 ("[A] better name for these programs is 'scumware.'").

22. *See* CENTER FOR DEMOCRACY & TECHNOLOGY, GHOSTS IN OUR MACHINES: BACKGROUND AND POLICY PROPOSALS ON THE "SPYWARE" PROBLEM 3 (2003), http://www.cdt.org/privacy/031100spyware.pdf [hereinafter CDT REPORT] (noting that trespassware would be a better term for spyware); *see also* Patrick Giblin, *Fake Anti-Spyware Programs Often Do More Harm*, MODESTO BEE, Oct. 7, 2004, at D1 (defining adware and spyware together as malware).

23. FTC Spyware Panel, *supra* note 17, at 147–48 (statement of James H. Koenig, Chief Practice Co-Leader, Privacy Strategy and Compliance, PricewaterhouseCoopers, LLP).

24. *See id.* at 32 (statement of Avi Naider, President & CEO, WhenU.com, Inc.) (stating that the definition of spyware was never meant to include legitimate software-based advertising, such as adware).

do, and then have the ultimate decision about whether to proceed with the installation).[25] Analyzing where these factors place the program on the sliding scale is what tends to define the program as adware or spyware.[26] The application of the defining process is explained in the examples that follow.

a. *Internet Service Providers: An Illustration of Adware.* Many Internet Services Providers (ISPs) have taken advantage of adware/spyware technology in legitimate ways in order to better serve their customers.[27] For example, an ISP may include an adware program in the installation of its service.[28] The adware then monitors the user's Internet activity and targets specific advertisements to the user's computer screen.[29] Because the adware company has to pay the ISP for access to consumers, the end result is cheaper Internet service for the consumer.[30] Consumers

25. *See id.* at 32–33 (considering notice, control, and consent as the differentiating characteristics between adware and spyware).

26. *See id.* (concluding that software fits the definition of spyware when it is given to consumers without adequate notice, control, or consent).

27. H.R. REP. NO. 108-619, at 9 (2004).

28. *See, e.g.*, NetZero, Terms and Conditons, http://www.netzero.net/legal/terms.html (last visited Oct. 2, 2005). NetZero Services and NetZero Site Terms of Service state:

> NetZero will collect, store, compile and utilize information about you, your computer, your phone number and your use of the NetZero Services including, without limitation, information regarding the Web sites you visit and information that you provide in response to NetZero questionnaires, surveys and registration forms. NetZero may provide this information to third parties including advertisers, clients, marketing organizations and others.

Id.

29. *See, e.g.*, *id.* For example, the NetZero Services and NetZero Site Terms of Service state the following:

> You expressly permit and authorize NetZero and its affiliates (and such third parties as may be authorized by NetZero, subject to the Privacy Statement) to furnish you, electronically when you use the NetZero Services or by any other means selected by NetZero, information or materials prepared by NetZero or by (or on behalf of) other entities, including advertising information and solicitations.

Id.

30. *See* MICROSOFT CORP., WHAT YOU CAN DO ABOUT SPYWARE AND OTHER UNWANTED SOFTWARE: WHAT IS SPYWARE? (2005), http://www.microsoft.com/athome/security/spyware/spywarewhat.mspx (noting that consumers can "pay" for services on the Internet by agreeing to accept targeted advertisements).

may have mixed feelings about this process. While some may find the advertisements distracting or annoying and simply tolerate them as a means for cheaper Internet service, others may find them very beneficial. For example, if a consumer is shopping online for airline tickets, the adware likely could provide the consumer with the most inexpensive source for the tickets.[31]

This use of the software technology clearly would fall on the adware end of the scale. Considering the factors listed previously,[32] computer users have notice of the adware program and what it does, consent to having the adware installed on their computers, and have full control over the installation and removal of the adware. Both the computer industry and legal authorities consider such practices to be perfectly legitimate and acceptable.[33] This monitoring technology also exists outside of the business realm of advertising. Many programs are currently available which allow parents to monitor children,[34] employers to monitor employees,[35] and even spouses to monitor each other.[36]

b. *Seismic Entertainment Productions, Inc. and SmartBot.Net, Inc.: An Illustration of Spyware.* At the opposite end of the scale are the more deceptive, disruptive, and destructive programs, frequently termed spyware. While much more egregious examples of spyware can be found,[37]

---

31. *Cf.* FTC Spyware Panel, *supra* note 17, at 32–33 (statement of Avi Naider, President & CEO, WhenU.com, Inc.) (describing how adware tracks the activity of computer users in order to target specific advertisements to them).

32. *See supra* note 25 and accompanying text.

33. *See* H.R. REP. NO. 108-698, at 5 (2004) (noting that some forms of legitimate adware likely would comply with proposed regulations); *see also* CDT REPORT, *supra* note 22, at 9 (emphasizing the importance of distinguishing between "legitimate ad-supported applications and their accompanying advertising components" and spyware programs). *But see* UTAH CODE ANN. § 13-40-201(1)(c) (Supp. 2004) (prohibiting "context based triggering mechanism[s] 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").

34. *See* H.R. REP. NO. 108-698, at 6 (recognizing the "spying" capabilities of parental monitor software).

35. FREDERICK S. LANE, THE NAKED EMPLOYEE 3–4, 128–29 (2003) (discussing how employers can monitor their employees by using keystroke-monitoring programs).

36. *See* O'Brien v. O'Brien, 899 So. 2d 1133, 1134 (Fla. Dist. Ct. App. 2005) (discussing whether communications intercepted by a spouse with the use of a spyware program are admissible as evidence in a divorce proceeding).

37. *See, e.g.*, H.R. REP. NO. 108-619, at 8 (discussing keyloggers, a particularly harmful type of spyware that captures personal information and can lead to identity

the practices of Seismic Entertainment Productions, Inc. (Seismic), and SmartBot.Net, Inc. (SmartBot) provide an all-too-common example of how some companies use programs in such a manner that qualifies them as spyware. In a complaint filed by the FTC,[38] Seismic and SmartBot were charged with violating § 5 of the FTC Act.[39] Specifically, the FTC found that the companies:

> [E]xploited particular vulnerabilities in certain versions of the Microsoft Internet Explorer web browser ("IE web browser") to reconfigure consumers' computers by installing software code onto their computers without their knowledge or authorization. The software code, among other things, (a) changes the IE web browser's home page; (b) modifies the IE web browser's search engine; and (c) downloads and installs various advertising and other software programs . . . and (d) causes an incessant stream of pop-up advertisements to be displayed.[40]

The FTC's four general charges can be analyzed in terms of the three key factors discussed previously: notice, control, and consent.[41] The complaint clearly states that the installation of the spyware was without the user's knowledge or consent.[42] In addition, by changing the user's

---

theft); FTC v. Verity Int'l, Ltd., 124 F. Supp. 2d 193, 195 (S.D.N.Y. 2000) (discussing the use of "dialers," another harmful form of spyware that uses a computer's modem to dial in to expensive websites).

38. Complaint for Injunction and Other Equitable Relief ¶¶ 23, 27, 30, FTC v. Seismic Entm't Prods., Inc., No. 04-377-JD (D.N.H. 2004) 2004 WL 2309585 [hereinafter FTC Complaint].

39. 15 U.S.C. § 45(a) (2000). Section 45 provides in part:

> (a) Declaration of unlawfulness; power to prohibit unfair practices; inapplicability to foreign trade
>
> (1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.
>
> (2) The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

Id.

40. FTC Complaint, *supra* note 38, ¶ 10.

41. *See supra* note 25 and accompanying text.

42. FTC Complaint, *supra* note 38, ¶ 10.

computer settings and installing programs which resulted in pop-up ads, the companies' programs limited the user's control over the spyware.[43] With respect to the pop-up ads, the FTC found that the spyware would make the user's computer exhibit bizarre behavior and then send a pop-up ad to the screen which offered to fix the problem for a fee.[44] Another aspect of the control factor is whether users can easily locate and remove the spyware once they become aware of its existence.[45] Although the FTC complaint did not address this aspect of control in relation to the spyware the defendants had distributed, many of these programs are extremely difficult, if not impossible, to remove.[46] Seismic and SmartBot's use of the adware/spyware technology is a typical example of what is considered spyware.

Because spyware and adware are essentially the same technology used in different ways, some experts argue that the best approach for defining spyware is in terms of specific practices.[47] The Center for Democracy in Technology (CDT) is one strong advocate of this approach, and it has compiled a list of specific examples of how the use of various programs qualifies them as spyware.[48] The application of the sliding scale uses this approach by considering how a particular application functions with respect to important factors.[49]

B. *How Does Spyware Get into Computers?*

A number of different techniques are used to get spyware onto users'

43. *See id.* ¶¶ 14–15.

44. *Id.* ¶ 18 (noting that some advertisements would cause the computer's CD tray to open, or cause computer programs to start up automatically, followed by a pop-up ad notifying the user that the problem was being caused by spyware and that they had to purchase defendants' spyware removal software to fix the problem).

45. FTC Spyware Panel, *supra* note 17, at 57–58 (statement of Avi Naider, President & CEO, WhenU.com, Inc.).

46. H.R. REP. NO. 108-619, at 8 (2004).

47. *See* CONSUMER SOFTWARE WORKING GROUP, EXAMPLES OF UNFAIR, DECEPTIVE OR DEVIOUS PRACTICES INVOLVING SOFTWARE VERSION 1.0 1–4, http://www.cdt.org/privacy/spyware/20040419cswg.pdf (last visited Oct. 3, 2005) (noting the shortcomings of current spyware definitions and providing a list of specific spyware practices to "help to focus technical, self-regulatory, regulatory and law enforcement efforts to protect consumers from inappropriate activities in a more targeted and effective manner").

48. *Id.* at 2–4.

49. *See supra* note 25 and accompanying text.

computer systems.[50] One of the most common methods is through the installation and use of peer-to-peer (P2P) file sharing software.[51] P2P software is commonly bundled with third party programs that are installed on the user's computer along with it.[52] Many of these programs, however, could be considered adware because, through the installation process, users are shown a user agreement in which they are notified of the program, consent to the installation,[53] and have the ability to remove it.[54] Users have the option of scrolling through and reading the agreement, which is usually quite lengthy.[55] Before users are allowed to continue the installation of the software, they are required to indicate their acceptance of the terms of the agreement.[56] Although very few people take the time to read user

50. H.R. REP. NO. 108-619, at 8.

51. FTC Spyware Panel, *supra* note 17, at 45 (statement of Ari Schwartz, Associate Director of the Center for Democracy & Technology).

52. *Id.*

53. *See* Kazaa End User License Agreement, http://www.kazaa.com/us/eula.htm (last visited Oct. 2, 2005) [hereinafter Kazaa EULA]. The Kazaa EULA provides:

> In order to use Kazaa, you must first read and accept the terms of this license. . . . During the process of installing Kazaa, you must install software from third party software vendors pursuant to licenses or other arrangements between such vendors and yourself . . . including[:] . . . Cydoor Technologies [which] deliver[s] advertisements to the application interface and computer, such as banner ads, buttons, or other advertising formats when you are using the application. . . . From time to time our application will connect to Cydoor's servers in order to report aggregated performance records[;] . . . . The TopSearch component [which] regularly downloads an index of available Altnet content through your Internet connection. This index contains a list of available rights managed files which can be displayed in your search results[;] . . . InstaFinder [which] is designed to redirect your URL typing errors to InstaFinder's web page[; and] [t]he RX Toolbar [which] is a software toolbar which is added to Microsoft Explorer and provides you with additional website suggestions displayed as links through the Microsoft Explorer window from Vista Interactive's advertisers based on the URL you input into your browser's address bar and/or based on the subject matter of the web page you are visiting.

Id.

54. *Id.* The Kazaa EULA incorporates separate license agreements for Vista's software (Rx Toolbar and InstaFind) which provide that the user can terminate the agreements by unistalling Kazaa "using the add/remove programs menu in the Microsoft® Windows® control panel." *Id.* In order to remove other third party software, the Kazaa EULA directs the user to contact the appropriate vendor. *Id.*

55. *See, e.g.*, *id.*

56. *See, e.g.*, *id.* ("In order to use Kazaa, you must first read and accept the

agreements, courts have upheld the enforcement of electronic user agreements.[57]

In addition to bundling, P2P file sharing introduces the more egregious forms of spyware through its file sharing process.[58] For example, consider users who download and install a popular P2P software program. Then, the users want to download a copy of the newest hit song from their favorite recording artist.[59] Users will conduct a search using the artist's name, and the P2P software will display a search result from which they can retrieve the song.[60] Some of the files, however, while displaying the desired song title, may actually contain a spyware program.[61] The users download the file expecting to receive a song and instead download spyware onto their computers.[62]

While bundling and P2P are the most common avenues for spyware to get onto users' computers, there are several other ways, many of them deceptive or unfair.[63] Some of these methods include the following: (1) telling users that they must download a certain program in order for something else to work; (2) disguising spyware as a spyware removal program; (3) sending users an on-screen prompt which does not respond to any action besides clicking "yes" to download a program; and (4) "drive-by" downloading in which the spyware is automatically downloaded when

terms of this license.").

57. *See, e.g.*, Caspi v. Microsoft Network, L.L.C., 732 A.2d 528, 532 (N.J. Super. Ct. App. Div. 1999) (upholding a forum selection clause contained in the electronic user agreement of an Internet service provider).

58. FTC Spyware Panel, *supra* note 17, at 83–84 (statement of Roger Thompson, Vice President of Product Development, Pest Control).

59. While this example may implicate numerous legal issues relating to copyright infringements, those issues are beyond the scope of this Note and are discussed thoroughly in other sources. *See, e.g.*, Robert A. Gilmore, *Peer-to-Peer: Copyright Jurisprudence in the New File-Sharing World, the Post* Grokster *Landscape of Indirect Copyright Infringement and the Digital Millennium Copyright Act*, 5 FLA. COASTAL L.J. 85 (2004) (discussing current copyright jurisprudence in P2P filesharing in advocating an application of common law indirect liability principles and the Digital Millennium Copyright Act to address illegal file sharing).

60. MGM Studios, Inc. v. Grokster, Ltd., 380 F.3d 1154, 1159 (9th Cir. 2004), *vacated*, 125 S. Ct. 2764 (2005).

61. FTC Spyware Panel, *supra* note 17, at 83–84 (statement of Roger Thompson, Vice President of Product Development, Pest Control).

62. *Id.*

63. *Id.* at 45–46 (statement of Ari Schwartz, Associate Director of the Center for Democracy & Technology).

a website is visited.[64]

C. *What Does Spyware Do?*

Just as spyware comes in many varieties, it can perform an assortment of tasks.[65] Some forms, mostly adware, are designed to facilitate targeted advertisements.[66] The adware monitors a user's website activity and records the information.[67] Then it sends the information to another site, which then determines which ads to send to the user's computer screen.[68] For example, if a user is searching the Internet for airline ticket prices, the adware monitors this and sends the information to the adware company's website. The adware company then will send a pop-up advertisement for airline tickets, from whichever company has paid the adware company for such services. As discussed previously, this software is usually classified as adware, but when it gets into the user's computer without the user's knowledge or consent, it moves closer toward the spyware end of the scale.[69]

Other forms of spyware, such as keyloggers, can keep track of every move users make on their computers.[70] Keyloggers can take from users' computers personal information such as usernames, passwords, credit card numbers, social security numbers, and any other information users may have entered into their computers.[71] This information then can be used to steal the users' identities.[72] Finally, most commonly, spyware can change settings in the users' computers.[73] This may result in a different home page being displayed, displaying of additional material on the users' computer screens, and may cause the users' computers to run slowly, malfunction, and crash.[74]

64. *Id.*
65. H.R. REP. NO. 108-698, at 3–4 (2004).
66. *Id.* at 4.
67. Gilmore, *supra* note 59, at 111.
68. *Id.*
69. *See supra* note 25 and accompanying text.
70. H.R. REP. NO. 108-698, at 3.
71. H.R. REP. NO. 108-619, at 8 (2004).
72. *Id.*
73. *Id.*
74. Prepared Statement of the FTC, Before the Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection (Apr. 29, 2004), http://www.ftc.gov/os/2004/04/040429spywaretestimony.htm.

D. *How Is Spyware Being Fought Outside the Courtroom?*

For some spyware practices, the public concern and legal issues are perfectly clear. If a company is distributing a program that is stealing credit card numbers for the purpose of facilitating identity theft, there are laws that apply to the problem.[75] But most of the spyware is hard to combat under current laws. The result is that spyware victims are taking matters into their own hands.[76]

One response is to simply tolerate the spyware, often because the user is unaware that it has caused the problems.[77] Another approach is to obtain spyware detection and removal software.[78] Most all of the reputable companies dealing in the virus scanning market have developed software programs that work along with the virus scanning programs.[79] Now, instead of just searching and removing viruses, the programs are capable of identifying most forms of spyware.[80] The cost of obtaining all these protection programs is quickly adding up, as one commentator insists a computer should be equipped with virus protection, firewalls, and now, spyware detectors.[81] Even worse, some consumers may search the Internet for spyware detectors and find numerous products available for download, not realizing that many of these programs are actually spyware disguised as anti-spyware programs, and end up harming their computer more than helping.[82]

Computer users are not the only ones to feel the effect of spyware.

---

75. *See* 15 U.S.C. § 45(a) (2000) (declaring unlawful unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce); 18 U.S.C. § 1029 (2000 & Supp. II 2002) (addressing credit card theft); *id.* § 1030 (addressing unauthorized access to computers); *id.* § 2511 (prohibiting interception of electronic communications).

76. Toddi Gutner, *What's Lurking in Your PC? How to Keep Spyware from Tracking Your Habits—or Hijacking Your Computer*, BUS.WK., Oct. 4, 2004, at 108 (discussing various self-help methods to prevent and remove spyware).

77. *See Protect Yourself Online*, *supra* note 7, at 15 (citing surveys finding that while 91% of the participants had spyware, only 41% use preventative measures against spyware).

78. Gutner, *supra* note 76, at 109.

79. *Id.*

80. *Id.*

81. *See* J.D. Biersdorfer, *Leave No Footprints in Online Transactions*, N.Y. TIMES, Oct. 21, 2004, at G6 (recommending a blended defense of programs to protect personal information on your computer).

82. *See* Giblin, *supra* note 22 (describing how some programs disguised as anti-spyware software can cause more harm than benefit).

ISPs are dealing with increased technical support calls and are losing customers who erroneously believe the problem is caused by the ISP.[83] The same is true for the computer manufacturers who also spend a great deal of time trying to help customers with technical issues resulting from spyware.[84] One of the most popular operating systems used today, Microsoft Windows, recently released an update to its system that has built-in security enhancements.[85] Popular ISPs are also helping out by providing their customers with enhanced security features.[86] Further, many groups and organizations are developing better ways to educate computer users about spyware.[87] Once users are provided with accurate information they will be able to quickly recognize a problem as spyware and know how to remove it from their system. Finally, the costs to ISPs and computer manufacturers will be greatly reduced and users will be able to provide authorities with useful information to assist officials in tracking down the responsible company if problems do arise.

III. APPLICATION OF CURRENT FEDERAL LAW

A. *Current Law Overview*

As spyware companies continue to grow and prosper, the need for legal action to combat the spyware problem is becoming quite clear.[88] Currently there are no federal laws that target spyware directly; however, there arguably are a few federal statutes that could be applied in certain situations.[89] Ultimately, because the current statutes were not drafted to

83. FTC Spyware Panel, *supra* note 17, at 95–97 (statement of Austin Hill, Co-Founder and Chief Privacy Expert, Zero-Knowledge Systems) (stating that increased technical service calls to ISPs due to spyware are consuming companies' profit margins and costing them customers).

84. *Id.* at 70–72 (statement of Maureen Cushman, Legal Counsel for U.S. Consumers, Dell) (stating that 12% of Dell's technical service calls are caused by spyware).

85. Mike Musgrove, *SP2 Fights Worms, Has Bugs*, WASH. POST, Sept. 12, 2004, at F7.

86. *See, e.g.*, Dave Gussow, *AOL's Latest Upgrade Has Compelling Features*, ST. PETERSBURG TIMES, Aug. 4, 2003, at 1E (describing the various new security features on AOL's new version 9.0 software, including a feature to diagnose and repair spyware-related problems).

87. CDT REPORT, *supra* note 22, at 13.

88. *See id.* at 12 (noting that even though some federal legislation may be applicable, it has not been effective thus far).

89. *See, e.g.*, 15 U.S.C. §§ 41–58 (2000) (declaring unlawful unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or

directly target spyware, their effectiveness becomes questionable when applied to the typical spyware case.[90]

1. *The Federal Trade Commission Act*

The Federal Trade Commission Act (FTC Act)[91] authorizes the FTC to issue and enforce orders prohibiting the use of "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[92] The act or practice in question must "cause[] or [be] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[93]

As mentioned previously, the FTC recently filed suit against Seismic and Smartbot, two large spyware companies, claiming violations of the FTC Act.[94] In applying the FTC Act to the activities of the defendants, the court noted that "[t]he defendants' activities in the new arena of Internet advertising do not necessarily fit easily into the traditional concepts of unfair and deceptive acts and practices under the [FTC Act]."[95] The court, however, found that computer users had experienced "substantial injury" including changes to home pages, incessant pop-up ads, and general difficulties in using their computers.[96] To support its finding the court cited several declarations from computer users, which demonstrate the effects that spyware has on users.[97] One of the key elements of the defendants' actions was the fact that "[t]he affected users were not notified of the defendants' activities and did not know what had caused the problems with their computers."[98] Thus, the court applied the factors discussed previously: notice, control, and consent.[99] As a result, the court granted

affecting commerce); 18 U.S.C. § 1030 (2000 & Supp. II 2002) (prohibiting unauthorized access to computers); 18 U.S.C.A. §§ 2510–22, 2701–12 (West 2000 & Supp. 2005) (prohibiting interception of electronic communications).

90. CDT REPORT, *supra* note 22, at 10–11.

91. 15 U.S.C. §§ 41–58.

92. *Id.* § 45(a)(1).

93. *Id.* § 45(n).

94. FTC v. Seismic Entm't Prods., Inc., No. 04-377-JD, 2004 WL 2403124, at *1 (D.N.H. Oct. 21, 2004); *see supra* Part II.A.2.b (providing a detailed analysis of the complaint filed by the FTC).

95. *Seismic Entm't Prods., Inc.*, 2004 WL 2403124, at *3.

96. *Id.*

97. *Id.*

98. *Id.*

99. *See supra* note 25 and accompanying text.

the FTC a temporary restraining order (TRO) that provided:

> defendants . . . are hereby required to remove, within twenty-four (24) hours, from any web site, bulletin board, or Internet server controlled by defendants any software script that exploits the web browser security vulnerabilities . . . to install, download, or deposit onto any computer any software code, program, or content, *without the user's authorization*.[100]

Seismic and SmartBot offered little resistance to the TRO, arguing only that the FTC was inaccurately characterizing their activities in a negative light and that some of their activities are widely accepted Internet advertising practices.[101] The court rejected this argument, noting the lack of persuasion in the "everyone is doing it" argument.[102]

In light of the FTC's recent suit, it is clear that at least one federal law, the FTC Act, may be applicable in situations where spyware companies use deceptive tactics, including those used by Seismic and SmartBot. In other cases, such as those when spyware companies use very long user agreements and require the user to affirmatively accept the installation of the spyware program,[103] the FTC Act loses much of its bite. In those cases, a persuasive argument could be made that under § 45(n) of the Act, any substantial injury to consumers is reasonably avoidable when the consumers do not accept user agreements or otherwise consent to the installation. The substantial injury would thus fall outside the definition of "unfair."[104]

2. *The Computer Fraud and Abuse Act*

At first glance, the Computer Fraud and Abuse Act (CFAA)[105] appears to have very limited use in typical spyware cases because the Act was drafted primarily for use in cases where there is a compelling federal interest, such as with federal government computers and certain financial institutions.[106] On closer examination of the terms and language, however, the CFAA packs more of a punch. The primary difference between the

100. *Seismic Entm't Prods., Inc.*, 2004 WL 2403124, at *6 (emphasis added).
101. *Id.* at *2.
102. *Id.* at *2 n.2 (internal quotation marks omitted).
103. *See, e.g.*, Kazaa EULA, *supra* note 53.
104. *See* 15 U.S.C. § 45(n) (2000).
105. 18 U.S.C. § 1030 (2000 & Supp. II 2002).
106. S. REP. NO. 99-432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482.

FTC Act and the CFAA is the agency authorized to bring suit: under the FTC Act, only the FTC is authorized to bring suit,[107] while under the CFAA, the authority to bring suit is broader, encompassing the United States Secret Service.[108]

Under the CFAA, it is a crime to "knowingly cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage *without authorization*, to a *protected computer*."[109] Similar to the FTC Act, the CFAA would also lose its force when spyware companies obtain consent, albeit deceptively, because the CFAA is violated only when the conduct occurs without authorization.[110] A spyware company could present the user a lengthy End User License Agreement (EULA) and require the user to accept the agreement before proceeding.[111] Courts generally enforce these agreements, regardless of how unfair they may seem.[112]

A second problem with the applicability of the CFAA to spyware cases is the definition of "protected computer." A "protected computer" applies only to government and financial institution computers or any computer used in interstate commerce.[113] Today, computers with access to the Internet have the capability of selling and buying goods all over the country.[114] As a result, any computer used in such a manner could be

---

107. 15 U.S.C. § 45(b).

108. 18 U.S.C. § 1030(d)(1).

109. *Id.* § 1030(a)(5)(A) (emphasis added).

110. *Id.* § 1030(a)(5)(A)–(B).

111. *See supra* notes 55–56 and accompanying text.

112. *See supra* note 57 and accompanying text.

113. 18 U.S.C. § 1030(e)(2). Section 1030(e)(2) defines "protected computer" as a computer:

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> (B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

Id.

114. *See* ACLU v. Reno, 929 F. Supp. 824, 842 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997) (stating that the Internet may be used for purchasing goods).

considered a protected computer. But not all users engage in online transactions and, therefore, those computers are not used in interstate commerce.

3. *The Electronic Communications Privacy Act*

For some of the more egregious forms of spyware, such as keyloggers, the Electronic Communications Privacy Act (ECPA)[115] is applicable. Under the ECPA, it is unlawful for a person to "intentionally intercept[] . . . any wire, oral, or electronic communication."[116] The Act defines the term "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[117] As discussed previously, keyloggers are programs that monitor and record a computer user's keystrokes, allowing the program to obtain information such as passwords, usernames, and credit card numbers in order to facilitate identity theft.[118] Applying the ECPA, a keylogging program would be considered either an "electronic device" or an "other device"; a computer user's information would be considered an "electronic communication"; and obtaining such information would be an "interception."

While the ECPA is clearly applicable to the more egregious forms of spyware programs, it would be difficult to apply to the spyware programs that only take information that is *stored* on a user's computer. When users type in a website address or click on a link that takes them to a website, that action is essentially a request for the website to send the webpage to the users' computer screens.[119] Hence, a visit to a website would be an electronic communication. But, after the website is displayed and the information is stored onto the computer, it would no longer be considered a communication.[120] Therefore, under the ECPA, a spyware program that collects information from a computer's hard drive would not be intercepting a communication for purposes of the ECPA.[121]

Despite the applicability of current federal law to certain situations, legislators argue that current law is insufficient and that a more targeted

115. 18 U.S.C.A. §§ 2510–22, 2701–12 (West 2000 & Supp. 2005).
116. 18 U.S.C. § 2511(1)(a) (2000).
117. *Id.* § 2510(4).
118. *See* discussion *supra* Part II.C.
119. *Reno*, 929 F. Supp. at 836.
120. CDT REPORT, *supra* note 22, at 10.
121. *Id.*

approach is necessary.[122] The Committee on the Judiciary found current laws to have "insufficient emphasis upon and enforcement of such crimes by Federal prosecutors to have the desired deterrent value."[123] In addition, the Committee found "that some spyware related behavior may not be easily prosecuted under existing Federal criminal laws that were not designed to explicitly deal with the relatively new phenomenon of spyware."[124] As a solution, federal legislators have proposed bills that are directed primarily at spyware.[125]

The defects in current federal laws can be illustrated by cases dealing with the use of Internet cookies. In *In re Doubleclick Inc. Privacy Litigation*,[126] the court defined cookies as "computer programs commonly used by Web sites to store useful information such as usernames, passwords, and preferences, making it easier for users to access Web pages in an efficient manner."[127] In *Doubleclick*, the class of plaintiffs accused Doubleclick of using cookies to monitor and collect private information about computer users for the purpose of targeting advertisements.[128] The plaintiffs brought suit under the ECPA, Federal Wiretap Act, CFAA, and state tort law.[129]

Pursuant to the ECPA claim, the court held that because the websites accessed by the plaintiffs were "users" who authorized the use of Doubleclick's cookies, the user-authorized exception to the ECPA was applicable.[130] Further, the court held that the users' information was not held in "electronic storage" as required by the Act.[131] Likewise, the plaintiffs' Wiretap Act claim failed because under the Act, if one of the users consents to the interception of the communication, there is no violation of the Act.[132] Finally, the plaintiffs' CFAA claim failed to meet the $5,000 minimum damages requirement;[133] however, it must be noted

122. H.R. REP. NO. 108-698, at 7–8 (2004).
123. *Id.*
124. *Id.*
125. *See, e.g.*, Securely Protect Yourself Against Cyber Trespass Act, H.R. 29, 109th Cong. (2005) (prohibiting a variety of spyware practices); Internet Spyware (I-SPY) Prevention Act of 2005, H.R. 744, 109th Cong. (2005) (same).
126. *In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).
127. *Id.* at 502–03.
128. *Id.* at 503.
129. *Id.* at 500.
130. *Id.* at 513–14.
131. *Id.*
132. *Id.* at 519.
133. *Id.* at 526.

that this claim may be more successful under the current version of the statute, as the $5,000 minimum damages requirement was repealed in 2001.[134] The *Doubleclick* case is an example of the difficulty that exists in trying to apply the current federal laws to modern Internet technology.

B. *Proposed Legislation*

1. *Securely Protect Yourself Against Cyber Trespass Act*

Currently, Congress is considering new laws that would directly proscribe the use of most forms of spyware. The Securely Protect Yourself Against Cyber Trespass Act[135] is a comprehensive bill that targets nearly every type of known spyware activity. Section 2 of the Act applies primarily to most of the annoying and disruptive spyware practices such as redirecting Internet browsers, altering home pages, adding website links to "bookmark" lists, delivering persistent pop-up ads, and installing dialers and keyloggers.[136] In addition, the Act also prohibits many of the deceptive tactics by which spyware programs are installed onto users' computers, such as misrepresenting to the user that installation of a program is required for some reason.[137]

Section 3 of the Act applies to the collection of information without notice to and consent of the user.[138] Section 3 is extensively detailed in terms of notice and consent requirements, providing that notice must be "clear and conspicuous" and "in plain language."[139] In addition, this section provides representative statements, which must be included in the notice.[140] While the comprehensiveness of the Act is impressive, the most

134. 18 U.S.C. § 1030(e)(8)(A) (2000) (repealed 2001).

135. Securely Protect Yourself Against Cyber Trespass Act, H.R. 29, 109th Cong. (2005).

136. *Id.* § 2(a).

137. *Id.* § 2(a)(6).

138. *Id.* § 3.

139. *Id.* § 3(c)(1).

140. H.R. 29 § 3(c)(1)(B) provides:

> The notice contains one of the following statements, as applicable, or a substantially similar statement:
>
> (i) With respect to an information collection program described in subsection (b)(1)(A): "This program will collect and transmit information about you. Do you accept?".

powerful aspect of the Act clearly is in the enforcement provision of section 4. Section 4 allows for the FTC to file a civil suit against a violator who, if found guilty, could face a staggering $3 million fine *for each violation* of section 2, and $1 million *for each violation* of section 3.[141] With the prospect of facing such incredible fines, a spyware company surely would think twice before sending strings of incessant pop-up ads to computer users.

2. *Internet Spyware (I-SPY) Prevention Act of 2005*

The Internet Spyware (I-SPY) Prevention Act[142] is a similar proposal directed primarily at spyware which amends 18 U.S.C. § 1030 by adding § 1030A.[143] In comparison to the Securely Protect Yourself Against Cyber Trespass Act, the I-SPY Act is considerably shorter and covers fewer activities.[144] The I-SPY Act provides:

> "Whoever intentionally accesses a protected computer without authorization, or exceeds authorized access to a protected computer, by causing a computer program or code to be copied onto the protected computer, and by means of that program or code—

> (ii) With respect to an information collection program described in subsection (b)(1)(B): "This program will collect information about Web pages you access and will use that information to display advertising on your computer. Do you accept?".
>
> (iii) With respect to an information collection program that performs the actions described in both subparagraphs (A) and (B) of subsection (b)(1): "This program will collect and transmit information about you and will collect information about Web pages you access and use that information to display advertising on your computer. Do you accept?".

Id. § 3(c)(1)(B).

141. *Id.* § 4(b)(1)(A)–(B).

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

143. *Id.* § 2.

144. *Compare id.* (compiling six pages of text addressing the copying of a code onto a protected computer in order to obtain or transmit personal information or to "impair[] the security protection of the protected computer with the intent to defraud or injure a person or damage a protected computer"), *with* H.R. 29 (compiling thirty-one pages of text addressing activities such as "[t]aking control of the computer," diverting the Internet browser, hijacking the modem or Internet connection, delivering advertisements that the user "cannot close without undue effort," modifying computer settings, collecting personal information, and numerous other disruptive and annoying activities).

> "(1) intentionally obtains, or transmits to another, personal information with the intent to defraud or injure a person or cause damage to a protected computer; or
>
> "(2) intentionally impairs the security protection of the protected computer . . . shall be fined under this title or imprisoned not more than 2 years, or both.[145]

Additionally, the I-SPY Act seeks to ensure that fiscal concerns are not a roadblock in enforcement of the Act, as it provides the Attorney General with $10 million for prosecuting violations.[146]

Ultimately, however, the I-SPY Act is too narrow to be an effective tool because it is only applicable when a computer is accessed without or beyond authorization, and it would not apply to the spyware tactics in which authorization is obtained in a misleading and deceitful way,[147] such as using lengthy EULAs.[148]

IV. APPLICATION OF STATE LAW

Due to a lack of adequate federal remedies and the growing seriousness of the spyware problem, many states have either already enacted new laws directed at spyware,[149] or quickly began considering such laws in 2005.[150] In early 2004, Utah became the first state to enact a law

145. H.R. 744 § 2(a).

146. *Id.* § 3.

147. *See id.* § 2 (requiring the access to be without authorization or in excess of authorization).

148. *See supra* notes 55–56 and accompanying text.

149. *See*, *e.g.*, ARIZ. REV. STAT. ANN. §§ 44-7301 to -7304 (West, Westlaw through 1st Reg. Sess. 2005); Consumer Protection Against Computer Spyware Act, ARK. CODE ANN. §§ 4-110-101 to -105 (West, Westlaw through Reg. Sess. 2005); Consumer Protection Against Computer Spyware Act, CAL. BUS. & PROF. CODE §§ 22947–22947.6 (West Supp. 2005); Georgia Computer Security Act of 2005, GA. CODE ANN. §§ 16-9-150 to 16-9-157 (Interim Update Serv. 2005); Computer Spyware Protection Act, 2005 Iowa Legis. Serv. 266–69 (West) (codified at IOWA CODE §§ 714F.1–714F.8 (2005)); Spyware Control Act, UTAH CODE ANN. §§ 13-40-101 to -401 (Supp. 2004).

150. *See*, *e.g.*, S.B. 122, 2005 Reg. Sess. (Ala. 2005); S.B. 140, 24th Leg., 1st Reg. Sess. (Alaska 2005); S.B. 124, 143d Gen. Assem. (Del. 2005); S.B. 2162, 107th Reg. Sess. (Fla. 2005); H.B. 380, 94th Gen. Assem. (Ill. 2005); H.B. 1714, 114th Gen. Assem., 1st Reg. Sess. (Ind. 2005); H.B. 2343, 81st Leg., Reg. Sess. (Kan. 2005); S.B. 151, 93d Leg., 1st Reg. Sess. (Mich. 2005); L.B. 316, 99th Leg., 1st Reg. Sess. (Neb. 2005); H.B. 47, 159th Sess. (N.H. 2005); Assem. B. 549, 228th Leg. Sess. (N.Y. 2005);

directed primarily at spyware.[151] California quickly followed suit, enacting its own spyware law in September 2004.[152] A brief discussion of these laws follows, but it should be noted that any state spyware law is likely to be short lived. If Congress passes a federal spyware law, it will preempt the states' efforts at combating spyware at the state level.[153]

A. *Utah's Spyware Control Act*

Similar to the Securely Protect Yourself Against Cyber Trespass Act, Utah's law, the Spyware Control Act,[154] is similarly quite comprehensive. The Spyware Control Act approaches the spyware problem by considering the three factors discussed previously.[155] The drafters were clearly concerned with not making the law overbroad to avoid prohibiting valid and beneficial uses of spyware technology, as evidenced by the statute's extensive list of what is not spyware.[156] By taking the three-factor

---

H.B. 2302, 73d Leg. Assem. (Or. 2005); H.B. 574, 189th Gen. Assem., Reg. Sess. (Pa. 2005); H.B. 1742, 104th Gen. Assem. (Tenn. 2005); H.B. 1012, 59th Leg., 1st Reg. Sess. (Wash. 2005).

151. Richard Raysman & Peter Brown, *Spyware: Time to Keep an Eye on Things?*, N.Y.L.J., Nov. 9, 2004, at 3.

152. *Id.*

153. *See* Securely Protect Yourself Against Cyber Trespass Act, H.R. 29, 109th Cong. § 6(a) (2005) (expressly preempting state spyware laws); Internet Spyware (I-SPY) Prevention Act of 2005, H.R. 744, 109th Cong. § 2(c) (2005) (providing that "[n]o person may bring a civil action under the law of any State if such action is premised in whole or in part upon the defendant's violating this section"); *see also* Cipollone v. Liggett Group, Inc., 505 U.S. 504, 516 (1992) (noting that "it has been settled that state law that conflicts with federal law is 'without effect'" (quoting Maryland v. Louisiana, 451 U.S. 725, 746 (1981))).

154. UTAH CODE ANN. §§ 13-40-101 to -401 (Supp. 2004).

155. *See id.* § 13-40-102(4)(b), (c) (defining spyware as software that monitors the computer's usage and sends the information to a remote user, displays pop-up ads, fails to fully identify its legal name, infringes on trademarks without *consent* or *notice*, and fails to provide a method by which the user can quickly and easily *disable* the software); *see also supra* note 25 and accompanying text.

156. *Id.* § 13-40-102(5). This section provides:

> Notwithstanding Subsection (4), "spyware" does not include:
> (a) software designed and installed solely to diagnose or resolve technical difficulties;
> (b) software or data that solely report to an Internet website information previously stored by the Internet website on the user's computer, including:
> (i) cookies;
> (ii) HTML code; or
> (iii) Java Scripts; or

approach,[157] the Spyware Control Act is not relying on a definition, but instead focuses on specific activity that is harmful or offensive to users.[158] As a deterrence measure, the Act provides for damages of at least $10,000 for each separate violation, and if the conduct was willful or knowing, the damages may be increased by three times that amount.[159]

B. *California's Consumer Protection Against Computer Spyware Act*

In early 2005, shortly after Utah passed its Spyware Control Act, California enacted the Consumer Protection Against Computer Spyware Act.[160] California's law also addresses the three main concerns associated with spyware:[161] (1) notice;[162] (2) control;[163] and (3) consent.[164] As a deterrent for violating California's spyware law, the California legislature is considering an addition to the current spyware law that allows for actual damages, a $1,000 fine, or both for each violation, and additionally makes a violation a crime subject to criminal penalties.[165]

V. CONCLUSION

It is clear that spyware is a serious problem in the realm of Internet privacy. It costs businesses substantial sums of money and interferes with

---

(c) an operating system.

Id.

157. *See supra* notes 154–56 and accompanying text.

158. *See supra* notes 154–56 and accompanying text.

159. UTAH CODE ANN. §§ 13-40–301(2)(ii), (3)(a).

160. Consumer Protection Against Computer Spyware Act, CAL. BUS. & PROF. CODE §§ 22947–22947.6 (West Supp. 2005).

161. *See supra* note 25 and accompanying text.

162. *See, e.g.*, Consumer Protection Against Computer Spyware Act § 22947.2(a)–(b) (making it a violation to modify a user's computer settings, or collect personally identifiable information through *intentionally deceptive means*).

163. *See id.* § 22947.3(c) (making it unlawful to "[p]revent . . . an authorized user's reasonable efforts to block the installation of, or to disable, software, by . . . [p]resenting the authorized user with an option to decline installation of software with knowledge that, when the option is selected by the authorized user, the installation nevertheless proceeds).

164. *See*, *e.g., id.* § 22947.4(a)(1) (making it unlawful to "[i]nduce an authorized user to install a software component onto the computer by *intentionally misrepresenting* that installing software is necessary for security or privacy reasons or in order to open, view, or play a particular type of content" (emphasis added)).

165. S.B. 92, 2005–2006 Reg. Sess. (Cal. 2005).

computer users' privacy.[166] Spyware also causes significant problems with users' computers, thereby consuming a great deal of time and money to remedy the problems.[167] While much advancement has been made in the way of self-help remedies, legal remedies are desperately needed to help curb the use of spyware.

Some experts argue that current laws are adequate to handle the spyware problem.[168] While it is true that many forms of spyware would fall under the current laws, this alone is insufficient. As the analysis of the most applicable current federal laws revealed, each has its own weak point when applied to the typical spyware case.[169] With the spyware problem still growing, and inadequate remedies at law, the need for a direct spyware law is necessary in order to curb the problem. By enacting spyware laws that require user notice, control, and consent, Congress will be able to effectively protect people's main concern: their privacy.

Benjamin J. Patterson *

166. *See* discussion *supra* Part II.C–D.

167. *See* discussion *supra* Part II.D.

168. FTC Spyware Panel, *supra* note 17, at 261 (statement of Mark Eckenwiler, Deputy Chief of the Department of Justice's Computer Crime and Intellectual Property Section) (stating that "we have in our quiver a number of arrows that we can use in prosecution").

169. *See* discussion *supra* Part I.A.1–3.

* B.S., Western Illinois University, 2002; J.D. Candidate, Drake University Law School, 2006. I would like to give special thanks to Adam McAuley for suggesting the topic for this Note and for providing helpful research sources.