SMU | Dedman School of Law

SMU Law Review

Volume 58 | Issue 4 Article 7

January 2005

Does Spybot Finally Have Some Allies: An Analysis of Current Spyware Legislation

Alfred Cheng

DOES SPYBOT FINALLY HAVE SOME ALLIES?: AN ANALYSIS OF CURRENT SPYWARE LEGISLATION

Alfred Cheng

I. INTRODUCTION

IN a time when anti-spyware programs like Spybot—Search and Destroy[1] and Ad-Aware[2] are just as likely to be found on an average computer user's desktop as traditional applications, like Microsoft Word, it is not surprising to find state and federal congresses drafting legislation to address the problem of spyware. Spyware has become an area of great concern over the last several years as computer users are increasingly discovering programs that were surreptitiously installed without their consent and that are difficult, if not impossible (without formatting their hard drives), to uninstall.[3] Spyware programs can change the appearance of web sites, Internet browser settings, and low-level system settings.[4] They also create privacy problems and open security holes, which potentially hurt the performance and stability of users' systems.[5] Such lags in performance are sometimes mistakenly blamed on legitimate applications and services, inundating the technical support groups of distributors with help-desk requests that they have no responsibility to resolve. This burdens these organizations with unnecessary labor costs.[6] Spyware programs distribute themselves by piggybacking on the installation of legitimate applications, by using deceptive pop-up windows, and by taking advantage of security holes in e-mail attachments and browsers.[7] In some cases, spyware programs compound system security problems by enabling automatic downloads and installations of other software without user authorization (referred to as "auto-update" functionality).[8]

1. Spybot—Search and Destroy is a freeware application developed by Patrick Michael Kolla to detect and remove spyware.
2. Ad-Aware SE is an anti-spyware application written by Nicolas Stark of Lavasoft Sweden.
3. Center for Democracy & Technology, *Ghosts in Our Machines: Background and Policy Proposals on the "Spyware" Problem* (November 2003), http://www.cdt.org/privacy/031100spyware.pdf.
4. *Id.*
5. *Id.*
6. *Id.*
7. *Id.*
8. *Id.*

The issue of spyware regulation is a hotly debated topic among members of the technology industry, politicians, and the general public. Almost all parties are in agreement that spyware should not be allowed to thrive in our society, but widespread disagreement as to how to accomplish this exists. Some believe that legislation is the best means by which to curb the problem, while others believe that the technology industry, rather than the government, is responsible for preventing the use of spyware. Even among those who believe that government intervention will most effectively address this issue, much disagreement exists as to what the scope of such legislation should be. Realistically, a complete solution should involve a combination of improved enforcement of existing laws, anti-spyware technologies, self-regulatory policies, user education, and new legislation.[9]

This comment will first provide an overview of the various forms of spyware and explain how they pose a significant privacy threat and transparency and user control concerns. It is essential, in drafting legislation to address this issue, that the problem itself be clearly defined. Because spyware is such a new development in the world of the Internet, no universal definition for it exists. It is obvious from a quick reading of the various existing pieces of spyware legislation that each bill has its own definition of what constitutes spyware, and as a result, the manner in which the legislation addresses it varies.

Second, this comment will discuss the various provisions that spyware legislation tends to include. Although each bill addresses the matter based on a different perspective of what spyware includes, some commonalities exist as to how legislatures have attempted to prevent the proliferation of spyware. Wide adoption of particular provisions across state and federal legislation may lend credence to the inclusion of such provisions in subsequently drafted bills.

Third, this comment will provide a critique of the federal bills that are pending ratification. The House of Representatives passed two of these bills, the Safeguard Against Privacy Invasions Act and the Internet Spyware (I-SPY) Prevention Act, in May of 2005.[10] Another two, the Software Principles Yielding Better Levels of Consumer Knowledge Act and the Computer Software Privacy and Control Act, have been introduced to the House of Representatives but have not passed.[11]

Fourth, this comment will critique the various pieces of state legislation that address spyware. Utah's Spyware Control Act was the first piece of spyware legislation to take effect when it was signed by Governor Olene Walker in March of 2004.[12] However, enforcement of the Spyware Control Act was enjoined by the Third District Court of Utah on June 22,

9. *See* Spyware, http://www.cdt.org/privacy/spyware (last visited Aug. 29, 2005).

10. *See* Legislation Regulating Spyware, http://www.benedelman.org/spyware (last visited Aug. 29, 2005).

11. *See id.*

12. *See id.*

2004.[13] The second state anti-spyware bill was passed by the California legislature in the form of the Computer Spyware bill, and it was signed into existence by Governor Schwarzenegger in September of 2004.[14] Along with these two passed bills, this comment will analyze the five proposed bills that are currently under review by state legislatures in California, Iowa, Michigan, New York, and Pennsylvania.[15]

Fifth, this comment will propose recommendations on what provisions are necessary to include in a piece of legislation that will effectively address the problem of spyware. Accurately defining the scope of spyware is essential to the process of drafting spyware legislation. An under-inclusive or over-inclusive definition can strip a piece of legislation of its ability to properly police spyware violations. Legislation that defines spyware too narrowly fails to punish destructive misuses of technology, while overly broad legislation improperly burdens parties that commit legitimate acts with criminal or civil liability.

In conclusion, this comment will consider other methods of addressing the problem of spyware, besides legislation. As with all societal problems, government intervention through law-making is not the only legitimate and effective means by which to expunge a wrong from the general public. In the case of spyware, the onus of shielding society from the detrimental effects of spyware could be placed on providers and manufacturers of information technology, while educating computer users on how to protect themselves from spyware would also help curb its negative effects. Before considering what means can be implemented to control spyware, it is important to first understand the scope of the spyware problem.

II. WHAT CONSTITUTES SPYWARE?

Many definitions of spyware have been proposed in legislation, academia, and the technology industry, but for a term that is continually evolving with the advancement of technology, it is difficult to successfully formulate an exact definition. However, it is essential to the drafting of effective spyware legislation for the term "spyware" to be understood in its entirety. In *F.T.C. v. Seismic Entertainment Products*,[16] Steven D. Gribble, Ph.D, an assistant professor of computer science at the University of Washington, defined spyware as "software that gathers information about a computer's use and transmits that information to someone else, appropriates the computer's resources, or alters the functions of existing applications on the computer, all without the computer user's

13. *See* WhenU.com, Inc. v. State of Utah—Case Documents, *available at* http://www.benedelman.org/spyware/whenu-utah (last visited Aug. 29, 2005).

14. *See* State Spyware Legislation, http://www.benedelman.org/spyware/legislation (last visited Aug. 29, 2005).

15. *See* 2004 State Legislation Relating to Internet Spyware or Adware, http://www.ncsl.org/programs/lis/spyware04.htm (last visited Aug. 29, 2005).

16. F.T.C. v. Seismic Entm't Prods., No. Civ. 04-377-JD, 2004 WL 2403124, slip op. at 1 (D.N.H. Oct. 21, 2004).

knowledge or consent."[17] Ben Edelman,[18] who has served as an expert witness in several cases concerning spyware, succinctly defines spyware as "programs that monitor user activities, and transmit user information to remote servers and/or show targeted advertisements."[19] In contrast, subsection 4 of Utah's Spyware Control Act uses over three hundred words to define spyware in great detail.[20]

A. THE FOUR CATEGORIES OF SPYWARE

With such variations in language defining spyware, it is helpful in understanding what constitutes spyware in order to examine the different methods used by spyware to violate the privacy of individuals. Spyware can be generally classified into four categories: 1) keystroke loggers and screen capture programs; 2) software systems that secretly install them-

17. *Id.*

18. Ben Edelman has served as a consultant regarding the effects of spyware and has provided expert witness testimony in multiple spyware-related cases, for a variety of clients including the ACLU, the National Association of Broadcasters, the National Football League, the New York Times, the Washington Post, and Wells Fargo. He is the author of numerous spyware publications and has given several presentations on this subject matter. Mr. Edelman is a Ph.D. candidate at the Department of Economics at Harvard University and a student at the Harvard Law School. He received his undergraduate degree from Harvard College, where he studied economics and statistics and previously was a fellow with the Berkman Institute of Technology at Harvard Law School. *See* Benjamin Edelman—Biography, http://www.benedelman.org/bio (last visited Aug. 29, 2005).

19. *See* Introduction, http://www.benedelman.org/spyware (last visited Aug. 29, 2005).

20. [S]oftware residing on a computer that: (a) monitors the computer's usage; (b)(i) sends information about the computer's usage to a remote computer or server; or (ii) displays or causes to be displayed an advertisement in response to the computer's usage if the advertisement: (A) does not clearly identify the full legal name of the entity responsible for delivering the advertisement; (B) uses a federally registered trademark as a trigger for the display of the advertisement by a person other than: (I) the trademark owner; (II) an authorized agent or licensee of the trademark owner; or (III) a recognized Internet search engine; (C) uses a triggering mechanism to display the advertisement according to the Internet websites accessed by a user; or (D) uses a context based triggering mechanism to display the 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; and (c) does not: (i) obtain the consent of the user, at the time of, or after installation of the software but before the software does any of the actions described in Subsection (4)(b): (A) to a license agreement: (I) presented in full; and (II) written in plain language; (B) to a notice of the collection of each specific type of information to be transmitted as a result of the software installation; (C) to a clear and representative full-size example of each type of advertisement that may be delivered (D) to a truthful statement of the frequency with which each type of advertisement may be delivered; and (E) 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 services; and (ii) provide a method: (A) by which a user may quickly and easily disable and remove the software from the user's computer; (B) that does not have other effects on the non-affiliated parts of the user's computer; and (C) that uses obvious, standard, usual, and ordinary methods for removal of computer software.

H.B. 323, 2004 Gen. Sess. § 13-39-301(1)(b) (Utah 2004), http://www.le.state.ut.us/~2004/bills/hbillenr/hb0323.htm (last visited Feb. 9, 2005).

selves and monitor and transmit users' activities unbeknownst to the users; 3) programs that use computer system resources, including the Internet connection, for their own unauthorized use; and 4) programs that strictly use the Internet connection to download software updates or content such as advertising.[21]

1. *Keystroke Loggers and Screen Capture Programs*

Keystroke loggers and screen capture programs, which are sometimes referred to as "snoopware," typically exist as stand-alone programs that are intentionally installed on a user's computer by another party.[22] Variants of these programs can track all keystrokes of a user, capture screen shots at set intervals, or focus on obtaining specific information on web sites visited or suspected passwords.[23] Keystroke loggers and screen capture programs can be used for legitimate purposes, such as special situations in which an employee's activities need to be scrutinized.[24] However, these programs have great potential for illegal uses, also.

2. *Surreptitiously Installed Programs that Transmit User Information*

The second class of spyware typically installs itself without the users' knowledge by "piggybacking" on the installation of an unrelated application or by utilizing some other questionable download method.[25] These forms of spyware software often, without the consent of users, transfer information about users and their computers via the Internet to servers owned by the software distributors.[26] In addition, such spyware software commonly resists uninstallation by making the uninstall process complex, by communicating to the user that the software has been uninstalled when in actuality it has not, or by automatically reinstalling without the user's authorization.[27]

One variant of this second class of spyware software that is receiving much attention monitors what web sites a user visits and displays specific advertisements based on this information. According to Ben Edelman, this form of spyware is distinguishable from adware because spyware programs "run continuously and show advertisements specifically responding to the web sites that users visit."[28] Claria (formerly known as The Gator Corporation), WhenU, and 180Solutions are three of the most infamous alleged distributors of such spyware (though they claim their products are not spyware) and have been the target of several lawsuits.[29]

---

21. Center for Democracy & Technology, *supra* note 3.
22. *Id.*
23. *Id.*
24. *Id.*
25. *Id.*
26. *Id.*
27. *Id.*
28. *See* Introduction, http://www.benedelman.org/spyware (last visited Aug. 29, 2005).
29. *See* Pending Suits [A]gainst Designers of Spyware, http://www.benedelman.org/spyware (last visited Feb. 9, 2005).

Claria is a provider of online marketing tools.[30] Once installed on a Windows computer, its software allows its servers to send users advertisements using pop-ups, pop-unders, and sliders while they are viewing specific web sites.[31] Claria has even promised its client advertisers that its software can show their advertisements when a user views a competitor's web site.[32] Claria targets users when they are in the process of making a purchase decision or shopping by showing special offers to capture their attention.[33] As a result, Claria is able to boast a clickthrough rate of 10%, allegedly thirty-five times higher than the average web site.[34] Several organizations have sued Claria (or Gator), including the New York Times and Washington Post, L.L. Bean, Lending Tree, Six Continents Hotel, and UPS.[35]

Claria's software is considered spyware because it monitors the clickstream data[36] of a user, sends that information to its servers, and posts advertisements based on such information. Whenever users visit new web sites or sites that they have not recently visited, the software sends a message to the Claria servers that contains the second-level domain name of the website visited (for example, ftc.gov), a unique user ID, a computer ID assigned by the software, the user's zip code, and the computer IP address.[37]

Another aspect of Claria's software that is characteristic of spyware is an end-user license agreement ("EULA") that is verbose, confusing, and ineffective in granting informed consent. Claria's license agreement measures 5,936 words in length, extending to sixty-three on-screen pages and hiding important language deep within the text of different sections of the EULA.[38] One such section, located nearly three thousand words into the license, expressly prohibits users from using unauthorized means of removing Claria's software, which include popular third-party tools such as Ad-Aware and Spybot.[39] This provision would not bear much significance if Claria's software was easy to uninstall on its own.[40] However, the uninstall process requires a user to uninstall all programs that bundle Claria's software, instead of allowing a user to uninstall only Claria's software.[41] Another provision about four thousand words into the

30. Benjamin Edelman, *Documentation of Gator Advertisements and Targeting* (May 2003), http://cyber.law.harvard.edu/people/edelman/ads/gator.

31. *Id.*

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id.*

36. A user's clickstream data is composed of the URL of the various web sites that a user visits during a browser session.

37. Benjamin Edelman, *Methods and Effects of Spyware: Response to FTC Call for Comments* (Mar. 19, 2004), http://www.benedelman.org/spyware/ftc-031904.pdf.

38. Benjamin Edelman, *Gator's EULA Gone Bad* (Nov. 29, 2004), http://www.benedelman.org/news/112904-1.html.

39. *Id.*

40. *Id.*

41. *Id.*

EULA prohibits a user from using a packet-snuffer, a device that monitors Internet transmissions across a local network, which effectively prevents users from observing what Claria's software is sending to its servers.[42] In other words, the license agreement demands that the user cannot conduct testing to verify whether Claria is abiding by its privacy policy.[43] Claria has also made it difficult for a user to obtain a license agreement before he consents to it. In some cases, the EULA will not appear when requested, and in other cases, the EULA only contains the first few lines of the actual agreement.[44] When the user can view the entire license agreement, the section headings are merged with the body text to prevent the fast and easy locating of a particular section.[45] In addition, the installer does not provide the user an option to print the entire license agreement.[46] Such features of Claria's software further solidify its classification as spyware software.

WhenU has developed and distributes an application similar to that of Claria, and likewise, its software constitutes a form of spyware. Each time the WhenU software displays a pop-up advertisement to a user, which is triggered by viewing a specific web site, the software sends to WhenU servers the URL of the web site that triggered the advertisement.[47] In addition, the servers receive information about the user's MSA (similar to zip code), how and when the user obtained WhenU, and the user's IP address.[48] By doing so, the WhenU software violates its privacy policy, which specifies that it will not transmit URLs of web sites visited by the user.[49] The advertisement pop-ups are displayed without the consent of the owners of the web sites that the pop-ups cover and tend to distract users from those web sites.[50] The advertiser sponsoring a pop-up does not pay the owners of the web site any amount, and a user may even be misled into believing that the sponsor of the pop-up is affiliated with the web site.[51] In addition, WhenU's license agreement requires forty-five on-screen pages to view because of its wordiness and its use of an unusually small viewing window.[52] Like Claria's software, the WhenU installer provides no functionality to print the entire text of the license agreement.[53] As a result, in a survey conducted by *PC Pitstop*, 87% of WhenU users did not know that WhenU software was installed

42. *Id.*
43. *Id.*
44. *Id.*
45. *Id.*
46. *Id.*
47. Benjamin Edelman, *WhenU Violates Own Privacy Policy* (May 2004), http://www.benedelman.org/spyware/whenu-privacy.
48. *Id.*
49. *Id.*
50. Benjamin Edelman, *Advertisers Using WhenU* (June 2004), http://www.benedelman.org/spyware/whenu-advertisers.
51. *Id.*
52. Benjamin Edelman, *WhenU License Agreement Is Forty Five Pages Long* (Apr. 2004), http://www.benedelman.org/spyware/whenu-license.
53. *Id.*

on their computers.[54]

180Solutions also distributes software that monitors the Internet browsing activities of users and reports the data to its own central servers. This software is distributed as a bundle with other freeware, and the information that is entered by a user to register those freeware products (also known as "affiliate applications") is sent to 180Solutions' servers, along with information about the web sites visited by the user and search terms used.[55] Allegedly, newer forms of this software search in the registry to find the user's email address, real name, or zip code from other applications' data and link this information to the unique identifier assigned to the user by the software.[56] Another concern raised by this software is its use of deceptive pop-ups or drive-by downloads[57] to gain user consent to download and install itself.[58] In addition, other spyware software is suspected of installing 180Solutions' software without the user's consent after the other spyware software has commandeered a user's computer.[59] As with Claria and WhenU's products, 180Solutions' software is extremely difficult to uninstall, as it remains on a computer even after the original host application has been removed.[60] Lastly, 180Solutions' software creates additional problems for a computer system by opening back-door security vulnerabilities that other applications can use for malignant purposes.[61] Only by understanding the different ways that Claria, WhenU, and 180Solutions' spyware programs surreptitiously invade the privacy of individuals and usurp control of their computer systems can a legislator strive to formulate a comprehensive response and solution to curbing the effects of such software.

3. *Programs that Commandeer System Resources*

The third form of spyware does not necessarily pose a serious privacy threat, but rather interferes with the user's control of his computer system by commandeering its resources and Internet connection without the user's authorization. An application named Altnet, developed by Brilliant Digital Entertainment ("BDE"), provides an example of such an application. Altnet piggybacks on the installation of a popular and legiti-

54. *Id.*
55. Center for Democracy & Technology, *supra* note 3.
56. *Id.*
57. Drive-by downloads prey on poorly configured security settings in Internet browsers to install software without prompting the user for consent. Even if the security settings are configured properly, the prompt given to the user requests for the user to authorize the install of software without seeing a license agreement. Often, users mistakenly believe that they must install the spyware in order to view a particular web site because of the appearance of a dialog box prompting the user's consent. Some drive-by downloads cause the downloading of software even before receiving consent and even in spite of a user's denial of consent. Benjamin Edelman, *Methods and Effects of Spyware: Response to FTC Call for Comments* (Mar. 19, 2004), *at* http://www.benedelman.org/spyware/ftc-031904.pdf.
58. Center for Democracy & Technology, *supra* note 3.
59. *Id.*
60. *Id.*
61. *Id.*

mate software application called Kazaa Media Player.[62] Once a user installs Altnet on his computer, BDE has the power to use the storage and computing resources of the computer, as it becomes part of BDE's distributed network, while notice of such usage is hidden deep within the EULA of the affiliate application, Kazaa.[63] Despite BDE's claim that users have the right to decide to allow BDE to use its computers for such purposes, the EULA clearly grants BDE access to the resources of a user's computer with an option for the user to deny access.[64] Also, BDE claims that users will receive benefits in exchange for usage of their computer resources, but the license agreement states that users have no right to compensation.[65] Lastly, the uninstall process is complicated, involving at least twelve steps if the user wants to uninstall Altnet without disabling Kazaa, and uninstalling Kazaa will not necessarily uninstall Altnet.[66] The threat of spyware that hijacks computer system resources demands that legislation should address the prevention and penalization of distribution of such software.

4. Programs that Download Updates and Content

While spyware programs that merely download updates and content do not cause distinct privacy and control concerns like the other three forms of spyware, they still are considered spyware because they can be surreptitiously installed, are difficult to uninstall, and open security holes. A spyware software produced by Aureate, which was later changed to Radiate, provides an example of this form of spyware. Although the company is now defunct, millions of copies of this software still reside on computers.[67] Radiate's software was an advertising application that downloaded advertisements from a central server and delivered them in the form of banner-ads.[68] Radiate's software was distributed within bundles with their host applications, which oftentimes prevented users from realizing that Radiate's software was even being installed.[69] Users can experience difficulty uninstalling the software as early versions cannot be removed through the standard Windows "Add/Remove Programs" menu, and later versions are not removed when the host application is uninstalled.[70] The greatest risk imposed by this software is the security holes that it opens with the regular downloading of application updates, which are installed and run without user authorization.[71] These security holes allow other unwanted applications to install themselves on a user's computer, make a computer vulnerable to system settings being changed, and

62. *Id.*
63. *Id.*
64. *Id.*
65. *Id.*
66. *Id.*
67. *Id.*
68. *Id.*
69. *Id.*
70. *Id.*
71. *Id.*

open up access to a user's computer system.[72] While legislation should forbid use and distribution of software that is classified as one of these four categories of spyware, some software with attributes similar to that of spyware should not be prohibited by legislation because they serve legitimate purposes.

B. Software Similar to Spyware that Legislation Should Not Prohibit

In the process of drafting legislation that effectively addresses the problem of spyware, representatives of the technology industry have placed a great emphasis on ensuring that legislation is not over-inclusive, as such legislation would prohibit the production and distribution of legitimate software that technology-related companies seek to market. Therefore, as important as it is to understand the various forms of spyware that currently exist, it is equally vital to possess knowledge of what applications should not be considered spyware. Such applications include media players, tracking cookies, and legitimate advertisement-supported software.

Media players like Microsoft's Windows Media Player and RealJukeBox request information from central servers about CD's and DVD's when a user plays them on his computer and assign a unique identifier for the media player making the request, thereby granting Microsoft and RealNetworks the ability to monitor a user's listening and viewing habits (though they both claim to not track such data).[73] However, media players are distinguishable from spyware in several different respects. First, these media players utilize a standard installation process, installing only necessary components, and an uninstallation process that is easy to perform.[74] Second, the data transferred from the media players to the central servers is used to enhance the functionality of the application, and users can elect to disable this aspect of the program.[75] Third, the privacy policies of the media players are fully disclosed to effectively give notice to users of information that is transferred.[76]

Tracking cookies represent another form of technology that has often been confused as spyware. Tracking networks, like DoubleClick, can monitor which sites a user visits by placing a cookie on a user's browser when he hits a site affiliated with the tracking network.[77] However, cookies fundamentally differ from spyware in that they are not stand-alone applications, and therefore, do not subject users to the same problems associated with installation and uninstallation.[78] In addition, current web

72. Benjamin Edelman, *Who Profits from Security Holes?* (Nov. 18, 2004), *at* http://www.benedelman.org/news/111804-1.html.
73. Center for Democracy & Technology, *supra* note 3.
74. *Id.*
75. *Id.*
76. *Id.*
77. *Id.*
78. *Id.*

browsers can effectively deter cookies from monitoring user activities.[79]

Legitimate advertisement-supported programs can be differentiated from spyware on several bases and, therefore, should not be prevented from distribution. Ad-supported applications, like the e-mail client Eudora, offer users the option of installing free software in exchange for the right to display advertisements, which are downloaded from a central server, in a small window integrated into the application display.[80] Although the program uses the computer's Internet connection for downloading these advertisements, this software differs from spyware. A user has the choice of purchasing an advertisement-free version of the software; therefore, the user ultimately decides whether he opens up his Internet connection to the advertisement downloads.[81] Further, ad-supported software typically provides clear notice to the user that installation of the software gives authorization to use his Internet connection for these downloads, and the user is required to view only one EULA in granting consent because the advertisement component is integrated into the main application.[82] Lastly, uninstallation of the software involves a one-step process to remove both the main application and the advertising component.[83] It is important that legislation not prohibit the use of legitimate forms of technology in an effort to prevent the proliferation of spyware, as doing so would improperly punish manufacturers of such technology and deny users access to them. With a basis for understanding what constitutes spyware, it is helpful to look to provisions that are common to existing legislation to determine what specific issues related to spyware are widely recognized as important to address.

III. COMMON PROVISIONS ACROSS SPYWARE LEGISLATION

Although the various pieces of legislation that address spyware differ in their approach, they contain similar provisions. The common usage of these provisions across legislation suggests that drafters are in agreement as to the importance of these particular provisions. Subsequent adoption of these pieces of legislation with like provisions would further validate their importance and provide guidelines for drafters of subsequent bills. These common provisions can be classified as pertaining to 1) defining the scope of spyware regulation; 2) exclusions to regulation; and 3) enforcement of the legislation.

Current legislative programs that have been proposed, reviewed, or adopted mirror each other in explicitly regulating particular aspects of spyware. First, several pieces of legislation address the use of keystroke logging software. For example, California's Computer Spyware bill prohibits an unauthorized user from installing keystroke logging software on

79. *Id.*
80. *Id.*
81. *Id.*
82. *Id.*
83. *Id.*

a user's computer in order to obtain personally identifiable information.[84] Interestingly, Iowa's bill permits employers to use such software in order to monitor the activities of its employees.[85] Of the eleven bills analyzed in this comment, five contain such language.[86] Second, the transfer of personally identifiable information or clickstream data without the authorization of a user is prohibited by ten of the eleven bills.[87] The Software Yielding Better Levels of Consumer Knowledge Act, a federal bill, provides an example of such a provision, stating that it is unlawful for an unauthorized user to install software on a user's computer that gathers and transmits user information, including what Internet sites the user has visited.[88] Third, provisions that prohibit the unauthorized changing of system and security settings and the disabling of anti-virus or anti-spyware software are included in five of the eleven pieces of legislation.[89]

---

84. A person or entity that is not an authorized user, shall not . . . cause computer software to be copied onto the computer of a consumer . . . and use the software to collect, through intentionally deceptive means, personally identifiable information that. . .is collected through the use of a keystroke-logging function that records all keystrokes made by an authorized user who uses the computer and transfers that information from the computer to another person.

S.B. 1436, 2003-04 Reg. Sess. § 22947.2(b)(1) (Cal. 2004), *available at* http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb_1401-1450/sb_1436_bill_20040928_chaptered.html (last visited Aug. 29, 2005).

85. S.F. 2200, 80th Gen. Assem., Reg. Sess. § 716.6C(3)(d) (Iowa 2004), *available at* http://www.legis.state.ia.us (last visited Aug. 29, 2005) (follow "archives" hyperlink; then follow "bills and amendments: Both GA "hyperlink;" then enter "2200").

86. *See* H.R. 29, 109th Cong. § 2(a)(3) (2005), *available at* http://thomas.loc.gov (last visited Aug. 29, 2005) (follow "search bills and resolutions" hyperlink; select "bill number;" select "108th;" enter "HR29"); S.B. 1436 § 22947.2(b)(1); A.B. 2787, 2003-04 Reg. Sess. § 22581.2(c) (Cal. 2004), *available at* http://www.leginfo.ca.gov/pub/03-04/bill/asm/ab_2751-2800/ab_2787_bill_20040623_amended_sen.html (last visited Aug. 29, 2005); S.F. 2200 § 716.6C(3)(d); S.B. 186, 2005-06 Reg. Sess. § 492(1)(B)(I) (N.Y.2004), http://assembly.state.ny.us/leg/?bn=S00186&sh=T (last visited Aug. 29, 2005).

87. *See* H.R. 29 § 3(a); H.R. 4661, 108th Cong. § 1030A(b)(1) (2004), *available at* http://thomas.loc.gov (last visited Aug. 29, 2005) (follow "search bills and resolutions" hyperlink; select "bill number;" select "108th;" enter "H.R. 4661"); S. 2145, 108th Cong. § 3(a) (2004), *available at* http://thomas.loc.gov (last visited Aug. 29, 2005) (follow "search bills and resolutions" hyperlink; select "bill number;" select "108th;" enter "S. 2145"); H.R. 4255, 108th Cong. § 3(a)(1)-(2) (2004), http://thomas.loc.gov (last visited Aug. 29, 2005) (follow "search bills and resolutions" hyperlink; select "bill number;" select "108th;" enter "H.R. 4255"); S.B. 1436 § 22947.2(b)(2)-(3); S.F. 2200 § 716.6C(1); S.B. 1315, 2003-04 Reg. Sess. § 5a(5)(b) (Mich. 2004), *available at* http://michiganlegislature.org/documents/2003-2004/billintroduced/senate/htm/2004-SIB-1315.htm (last visited Aug. 29, 2005); S.B. 186 § 492(1)(B); H.B. 323, 2004 Gen. Sess. § 13-39-102(4)(b)(i) (Utah 2004), *available at* http://www.le.state.ut.us/~2004/bills/hbillenr/hb0323.htm (last visited Aug. 29, 2005); H.B. 2788, 2003-04 Reg. Sess. (Pa. 2004), *available at* http://www.legis.state.pa.us/wu01/LI/Bi/BT/2003/0/HB2788P4269.htm (last visited Aug. 29, 2005).

88. It shall be unlawful for a person who is not an authorized user of a protected computer to authorize or cause the installation on that computer that collects information about the user of the computer or about the user's Internet browsing behavior or other use of the computer and transmits such information to any other person on an automated basis or at the direction of a person other than an authorized user of the computer.

S. 2145 § 3(a).

89. *See* H.R. 29 § 2(a)(2), (8); H.R. 4661 § 1030A(b)(2); S. 2145 §4; S.B. 1436 §§ 22947.2(e), 22947.3(b); A.B. 2787 § 22581.2(b)(4)-(5).

For example, the Securely Protect Yourself Against Cyber Trespass Act ("SPY ACT") forbids an unauthorized user from changing a user's computer settings, including security settings, in order to harm the user and from disabling technology that protects computers, like anti-spyware software.[90]

In addition to sharing common provisions regarding the regulation of spyware, several of the pieces of legislation contain similar exceptions that allow law enforcement agencies and service providers to lawfully utilize spyware-like software to perform legitimate tasks. Four of the bills explicitly call for an exception to regulation for the purposes of law enforcement.[91] An example of such a provision is found in the federal Internet Spyware Prevention Act ("I-SPY"), which "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States."[92] The second type of exception that is included in some of the current spyware legislation permits telecommunications carriers, cable operators, providers of information services, or providers of computer hardware and software to interact with a user's computer network, Internet connection, or computer.[93] The SPY ACT contains a detailed version of such a provision, which states that the Act's prohibitions do not extend to service providers that are interacting with a user's computer or network for beneficent purposes, such as diagnostics and technical support.[94]

Another provision that almost all of the current legislation share in common is an enforcement provision that explains how violators of the acts will be penalized and punished. Four of the bills provide for strictly civil causes of action,[95] four of them detail only criminal liability,[96] and

---

90. It is unlawful for any person, who is not the owner or authorized user of a protected computer, to engage in deceptive acts or practices that involve . . . (2) modifying settings related to use of the computer or to the computer's access to or use of the Internet by altering security or other settings of the computer that protect information about the owner or authorized user for the purposes of causing damage or harm to the computer or owner or user. . .(8) removing, disabling, or rendering inoperative a security, anti-spyware, or anti-virus technology installed on the computer.

H.R. 29 § 2(a)(2)(D), (9).

91. *Id.* § 5(a); H.R. 4661 § 1030A(e); S.F. 2200 § 716.6C(3)(c); S.B. 1315 § 5a(6)(e).

92. H.R. 4661 § 1030A(e).

93. *See* H.R. 29 § 5(b); S. 2145 § 6(b); S.B. 1436 § 22947.3(d), 22947.4(b); S.F. 2200 § 716.6C(3)(b); S.B. 1315 § 5a(6)(d); H.B. 323, 2004 Gen. Sess. § 13-39-102(5)(a).

94. Nothing in this Act shall apply to any monitoring of, or interaction with, a subscriber's Internet or other network connection or service, or a protected computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service, to the extent that such monitoring or interaction is for network or computer security purposes, diagnostics, technical support, or repair, or for the detection or prevention of fraudulent activities.

H.R. 29 § 5(b)(1).

95. *See* H.R. 29 § 4; S.B. 1436; A.B. 2787 § 22580.3; H.B. 323 § 13-39-301.

96. H.R. 4661 § 1030A(a)-(c); S.B. 1315 § 7; S.B. 186, 2005-06 Reg. Sess. § 493 (N.Y. 2004), *available at* http://assembly.state.ny.us/leg/?bn=S00186&sh=T (last visited Aug. 29,

three other bills administer civil and criminal liability.[97] Several of the acts preclude parties from bringing civil suits against violators, except for the attorney general of a state or the Federal Trade Commission,[98] while others provide for a wider class of possible plaintiffs.[99] By limiting the class of potential plaintiffs, the acts can effectively curb the number of frivolous lawsuits; but in the process, such an absolute ban on litigation initiated by the general public could also hinder, or even prevent, legitimate cases from being reviewed. Recognizing the commonalities among spyware legislation provides a foundation for understanding how the individual bills compare to one another.

IV. ANALYSIS OF INDIVIDUAL LEGISLATION

Although the various pieces of current spyware legislation have some fundamental commonalities, the relative scope of each bill differs. As a result, the potential effectiveness of each of them is not equal. In order to sufficiently address the spyware problem, legislation cannot be either over or under-inclusive in its scope. Legislators must strike a balance in drafting the scope of regulation to ensure that the definition prescribed for spyware is not too general, as that would make the legislation over-inclusive. However, legislators must also avoid defining spyware too specifically; such a narrowly construed definition would fail to cover some current and potentially all future spyware issues. The goal of examining the relative strengths and weaknesses of existing legislation is to learn how to structure future legislation to address the problem of spyware more effectively and comprehensively. The intent of performing such an analysis of federal and state spyware legislation is to further the process of refining the tools that the general public will use to combat spyware.

A. FEDERAL LEGISLATION

Of the four pieces of federal spyware legislation that are currently being considered, the Securely Protect Yourself Against Cyber Trespass Act ("SPY ACT") and the Software Principles Yielding Better Levels of Consumer Knowledge Act ("SPY BLOCK Act") are the more comprehensive acts, whereas the Internet Spyware ("I-SPY") Prevention Act and Computer Software Privacy and Control Act are very narrow in scope. The SPY ACT, introduced to the House of Representatives in July of 2003 by Representative Mary Bono, and later reintroduced in January of 2005, creates a civil cause of action for deceptive acts or practices relating to spyware and for the unauthorized collection of personally identifiable

2005); H.B. 2788, 2003-04 Reg. Sess. § 7662(c) (Pa. 2004), *available at* http://www.legis.state.pa.us/WU01/LI/BI/BT/2003/0/HB2788P4269.HTM (last visited Aug. 29, 2005).

97. S. 2145 §§ 7-9; H.R. 4255, 108th Cong. § 4 (2004), *available at* http://thomas.loc.gov (last visited Aug. 29, 2005) (follow "search bills and resolutions" hyperlink; select "bill number;" select "108th;" enter "H.B. 4255"); S.F. 2200 § 716.6C(1)-(2).

98. *See* H.R. 29 § 4, 6; S. 2145 §§ 7-9; H.R. 4255 § 4; A.B. 2787 § 22580.3.

99. S.F. 2200 § 716.6C(2); H.B. 323 § 13-39-301(1)(b).

information.[100] The legislation's strength is the level of detail and the scope of coverage it contains. It prohibits the use of keystroke loggers, the use of most deceptive install practices, the unauthorized transfer of personally identifiable information and clickstream data, the use of pop-up ads that pull a user away from the original site visited or cause browser or system failure, the hijacking of system resources, the changing of system settings, the unauthorized disabling of anti-spyware programs, the use of most deceptive EULA practices, and the prevention of software uninstallation.[101] In addition, by merely requiring that the EULA disclose the information that is transferred, the bill avoids being over-inclusive because it does not prohibit the use of legitimate software such as virus definition updaters, search engine toolbars, media players, and ad-supported software. Despite the breadth of coverage, the bill still fails to prohibit the use of drive-by installs triggered by pop-ups and the use of security holes to install other programs without the user's consent. It also does not address common deceptive practices associated with license agreements. One example of this is the problem of EULA's that prohibit uninstallation of spyware using third-party applications (e.g. anti-spyware software). The bill should also address use of license agreements that prohibit the use of packet-snuffers or network monitors to view what the spyware is actually transmitting to its servers. Lastly, a clause should be added to require that EULA's are printable in their entirety for the user's benefit. Another shortcoming of this Act is that it allows an installer for applications like Grokster to load an infinite amount of programs on a computer as long as it provides notice that the program will collect information on web sites accessed and display ads based on this information.[102] The installation of bundled software can significantly reduce the speed and reliability of a computer; therefore, when a user expects for only one program to be installed and the bundle of software has no relationship to that program, a bundled install should be prohibited.[103] In addition, for bundled applications that display advertising, the installation should provide a sample of the different advertisements and disclose the frequency of such advertisement displays.[104]

The SPY BLOCK Act, introduced to the Senate in February of 2004 by Senators Conrad Burns and Ron Wyden,[105] is similar to the SPY ACT in regards to the breadth of the bill's coverage. Like the SPY ACT, the SPY BLOCK Act prohibits the use of most deceptive install practices, the unauthorized transfer of personally identifiable information and clickstream data, the use of pop-up ads that pull a user away from the original site

100. H.R. 29 §§ 2-4.
101. *Id.* §§ 2-3.
102. Benjamin Edelman, *Grokster and Claria Take Licenses to New Lows, and Congress Lets Them Do It* (Oct. 9, 2004), http://www.benedelman.org/news/100904-1.html.
103. *Id.*
104. *Id.*
105. S. 2145, 108th Cong. § 3(a) (2004), *available at* http://thomas.loc.gov (last visited Aug. 29, 2005) (follow "search bills and resolutions" hyperlink; select "bill number," select "108th," enter S. 2145).

visited or cause browser or system failure, the hijacking of system resources, the changing of system settings, the unauthorized disabling of anti-spyware programs, the use of most deceptive EULA practices, and the prevention of software uninstallation.[106] Unlike the SPY ACT, it forbids the use of drive-by installs triggered by pop-ups and the use of security holes to install other programs without the user's consent.[107] However, the SPY BLOCK Act fails to address keystroke logging programs and installers that install an application despite the user declining such an installation.[108] The SPY BLOCK Act does succeed in avoiding over-inclusiveness. Section 5(b)(1) states that software that collect information functionally related to the software (for example, media players) fall outside of the prohibitive scope of the Act.[109] Other legitimate software that collect information about the user are allowed to operate without violating the Act by merely providing disclosures that detail the type of information collected and the ways that the information will be used. Like the SPY ACT, though, it falls short in its prevention of deceptive license agreements. In the case of software that is distributed in a bundle, the SPY BLOCK Act does not require that each program ask the user for consent to install. Therefore, the entire bundle of software could install after the user has given consent to one application. Also, from an uninstallation standpoint, this Act does not require software that is installed as a bundle to be uninstalled as a bundle.[110] As a result, a user may be led to believe that, by uninstalling a host application, all other programs associated with it will be uninstalled. In actuality, only the host application is required to be uninstalled by this Act. In many cases, the uninstalled programs associated with the host application are spyware, unbeknownst to the user. As with the SPY ACT (and every other piece of legislation that is reviewed in this comment), the SPY BLOCK Act fails to address the problem of EULA's that prohibit uninstallation of spyware using third-party applications, the use of license agreements that prohibit the use of packet-snuffers, and the necessity of printable EULA's in their entirety.

The I-SPY Prevention Act, introduced into the House by Representative Bob Goodlatte in June of 2004,[111] is narrow in scope and mainly focuses on criminalizing the unauthorized access of computers for the purpose of causing injury through fraud or other illegal activity, as opposed to a general ban on the collection of user personally identifiable information. This Act specifically prohibits the use of spyware to commit a federal criminal offense or to injure or defraud. As a result of its nar-

106. *See id.*
107. *See id.*
108. *See id.*
109. *Id.* § 5(b)(1).
110. *See id.* § 2(c)(2)(B).
111. H.R. 4661, 108th Cong. (2004), http://thomas.loc.gov (last visited Aug. 29, 2005) (follow "search bills and resolutions" hyperlink; select "bill number;" select "108th;" enter "H.R. 4661").

row focus, this piece of legislation does not provide a comprehensive tool to combat spyware and is likely not intended to be. The I-SPY Prevention Act basically addresses three specific topics and does not attempt to cover any other aspect of spyware. First, it prohibits the unauthorized access of a computer using spyware in furtherance of a federal criminal offense. Second, the Act explicitly forbids the unauthorized transfer of a user's personally identifiable information with the intent of defrauding or injuring the user. Third, impairing system security and anti-spyware software is prohibited when done with intent to defraud or injure. As a whole, this piece of legislation does not provide a comprehensive approach to fighting spyware, and its utility is limited to imposing criminal penalties for violations involving particular types of spyware activity.

The Computer Software Privacy and Control Act, introduced by Representative Inslee to the House in April of 2004,[112] is similar to the Internet Spyware Prevention Act in the narrowness of its scope. The goal of the Act is to "prevent deceptive software transmission practices in order to safeguard computer privacy, maintain computer control, and protect Internet commerce."[113] Unfortunately, the legislation only achieves this goal to a very limited extent. The Act's scope is essentially restricted to the prohibition of the unauthorized transfer of a user's personal information and the nonconsensual modification of system settings. It requires that advertising software gain the user's consent before installation, but fails to provide an adequate definition of consent. The Act merely states that the directions for uninstallation must be included and that the notice cannot be materially false or misleading. In addressing consent, no provisions address deceptive installation practices or the use of EULA's that fail to grant effective consent. Other key topics that the legislation fails to address include the use of difficult uninstall processes and programs that hijack system resources. As with the I-SPY Prevention Act, the Computer Software Privacy and Control Act does not achieve much in the way of spyware prevention and requires revision before it can give the general public an effective means of combating spyware. Although the federal spyware bills prescribe enforcement against the use of spyware on a national level, several states have introduced their own pieces of legislation to combat spyware in their respective jurisdictions.

B. State Legislation

Like the federal bills, the scope of current state spyware legislation varies between bills, though none are as comprehensive as the SPY ACT or SPY BLOCK Act. Utah and California's spyware legislation are the

112. H.R. 4255, 108th Cong. (2004), http://thomas.loc.gov (last visited Aug. 29, 2005) (follow "search bills and resolutions" hyperlink; select "bill number;" select "108th;" enter "H.R. 4255").

113. *Id.*

most comprehensive of the state bills, while bills in the Iowa and New York legislatures provide examples of narrowly-defined legislation.

Although enforcement of Utah's Spyware Control Act was subsequently enjoined by Judge Fratto of the Third District Court of Utah,[114] it represents the first enacted legislation to address the spyware problem and provides a helpful model for future legislation. The Act is comprehensive in its stance against spyware. It prohibits the use of keystroke loggers, the unauthorized installation of software, the unauthorized transfer of personally identifiable information and clickstream data, the use of pop-up ads that partially or wholly cover the original site visited, the use of most deceptive EULA practices, and the prevention of software uninstallation.[115] Another strength of the Act is that it is not over-inclusive in its prohibitions. It requires any software that transmits user information to provide notice in plain language and full presentation, include what type of information is collected by the software, and provide a reasonable uninstall routine.[116] For advertising software, the disclosure requirement also includes identification of who is providing the advertisement, displaying an example advertisement, and detailing the frequency of advertisement display and method of distinguishing advertisements delivered by the installed software from another program. Most legitimate software abides by these requirements and, therefore, is not prohibited by the Act. Any type of software that does not meet these two requirements should be viewed with skepticism and adding such requirements for all software would be a positive step for the general public.[117] The Spyware Control Act falls short in its coverage by failing to address pop-ups that cause browser or system failure, the hijacking of system resources, software that cause system settings changes, the unauthorized disabling of anti-spyware programs, and the unauthorized automatic reinstallation of software after uninstallation. Despite these shortcomings, this Act represents one of the most effective pieces of state spyware legislation drafted to date.

The Spyware Control Act was unjustly enjoined from enforcement, as the rationale for issuing the injunction is flawed. Judge Fratto issued the injunction on the basis that there was a substantial likelihood that the plaintiff, WhenU, would succeed in its claim that parts of the Act violated the Constitution, that the plaintiff would experience irreparable harm, and that such harm would outweigh harm to the defendant.[118] The court ruled that there was a substantial likelihood that the Act violated the Commerce Clause to the extent that it forbids the use of pop-up advertis-

114. *See* WhenU.com, Inc., v. State of Utah - Case Documents, *available at* http://www.benedelman.org/spyware/whenu-utah (last visited Aug. 29, 2005).

115. H.B. 323, 2004 Gen. Sess. (Utah 2004), *available at* http://www.le.state.ut.us/~2004/bills/hbillenr/hb0323.htm (last visited Aug. 29, 2005).

116. *See* Benjamin Edelman, *A Close Reading of Utah's Spyware Control Act* (Mar. 2004), http://www.benedelman.org/spyware/utah-mar04.

117. *Id.*

118. Transcript of Preliminary Injunction Ruling, *available at* http://www.benedelman.org/spyware/whenu-utah/pi-ruling-transcript.html (last visited Aug. 29, 2005).

ing and requires adherence to a protocol for gaining user consent for software installation.[119] However, the Spyware Control Act does not prohibit the use of pop-ups, it merely prevents the use of pop-ups that cover other browser windows, that display content in response to a user's clickstream data, and that do not identify the providers of advertisements. In addition, the standards established by the Act for obtaining user consent are not overly burdensome and do not interfere with commerce, unless an entity engages in business that benefits from users giving uninformed consent to installing its software. The court also found that WhenU would suffer irreparable harm if the Act was not enjoined because it would "incur expense, an inability to conduct business, a loss of necessary business partners, all resulting in economic damages and litigation from those seeking to enforce violations of the statute."[120] However, the Act was created to prohibit the use of software, like WhenU's, that violate user privacy. Therefore, any irreparable harm that WhenU suffers is the equitable result of the Act doing exactly what it was intended to do, eliminate spyware from our society. Based on these flaws in reasoning, this injunction should not cause legislators to rethink how they draft their spyware legislation, for the result would be toothless legislation.

The two California examples of spyware legislation, the Computer Spyware bill introduced by Senator Kevin Murray and subsequently signed by Governor Schwarzenegger[121] and the Computer Adware and Spyware bill introduced by Assembly Member Tim Leslie,[122] provide relatively good examples of comprehensive state spyware legislation. The two bills are similar in language with some identical provisions. Both bills expressly prohibit the use of pop-up ads that cause browser or system failure, the hijacking of system resources, unauthorized system settings changes, the unauthorized disabling of anti-spyware programs, and the prevention of software uninstallation. Both bills also forbid a variety of deceptive installation practices, such as piggyback installs and installs despite a user's declining the software, but fail to address the issue of installations that occur without the user's explicit consent. In addition, the bills do not impose any guidelines or restrictions on what can and cannot be included in a license agreement. By not addressing these issues, spyware developers can take advantage of users by either gaining uninformed consent using deceptive license agreements or installing software without the user's authorization. The bills differ in that the Computer Spyware bill prohibits the transfer of information relating to clickstream data and personally identifiable information, while the Computer Adware and

119. *Id.*

120. *Id.*

121. S.B. 1436, 2003-04 Reg. Sess. (Cal. 2004), *available at* http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb_1401-1450/sb_1436_bill_20040928_chaptered.html (last visited Aug. 29, 2005).

122. A.B. 2787, 2003-04 Reg. Sess. (Cal. 2004), *available at* http://www.leginfo.ca.gov/pub/03-04/bill/asm/ab_2751-2800/ab_2787_bill_20040623_amended_sen.html (last visited Aug. 29, 2005).

Spyware bill does not mention this issue. Lastly, although both bills are relatively comprehensive, neither is over-inclusive because the bills are particular in regard to prohibitions. For example, media players or other legitimate software that extract information from a computer are not prohibited if the information extracted is related to the purpose of the software.

The legislation proposed by the Iowa, Michigan, and New York legislatures differ in many respects from the California and Utah bills because they are limited in the breadth of their coverage. The Iowa, Michigan, and New York bills require that the transfer of personally identifiable information be accompanied by the consent of the user. The Iowa legislation, which was introduced by Senator Keith Krieman in March of 2004,[123] emphasizes clear notice and disclosure of the software's ability to transmit information, the name and address of who will receive the information, and instructions on how to disable the software. The Michigan bill, which was introduced in June of 2004 to the Michigan Senate, requires the provider of software to identify himself, detail how the installation will affect the user's computer, disclose any fees associated with the installation, state what information is obtained by the provider, give any necessary warning of sexual explicitness, provide a method for refusing the installation, and gain the user's affirmative grant to perform the installation.[124] The New York legislation, which was reintroduced to the New York Senate in January of 2005,[125] merely states that consent can be obtained through an end user license agreement.[126] The Michigan bill also prohibits the display of advertisements in response to the usage of the computer. The New York legislation explicitly prohibits the use of keystroke logging software,[127] while the Iowa legislation grants employers an exception, allowing them to monitor computer usage while an employee is acting within the scope of his employment.[128] But aside from these requirements, these pieces of legislation suffer from deficiencies in coverage. None address certain fundamental spyware issues that should not be overlooked. Important issues like deceptive installation practices, pop-up advertisements that cover or distract a user from the original web site visited, advertisements that cause system or browser failure, the commandeering of system resources, unauthorized system settings changes, the disabling of anti-spyware programs, the use of deceptive end user li-

123. S.F. 2200, 80th Gen. Assem., Reg. Sess. (Iowa 2004), *available at* http://www.legis.state.ia.us (last visited Aug. 29, 2005) (follow "archives" hyperlink; then follow "bills and amendments: 80th GA" hyperlink; then enter "2200").

124. S.B. 1315, 2003-04 Reg. Sess. (Mich. 2004), *available at* http://michiganlegislature.org/documents/2003-2004/billintroduced/senate/htm/2004-SIB-1315.htm (last visited Aug. 29, 2005).

125. S.B. 186, 2005-06 Reg. Sess. (N.Y. 2004), *available at* http://assembly.state.ny.us/leg/?bn=S00186&sh=T (last visited Aug. 29, 2005).

126. *Id.* § 492.

127. *Id.* § 492 (1)(B)(I).

128. S.F. 2200 § 3(d).

cense agreements to obtain uninformed consent, and illusory uninstall routines are not considered in any of these three pieces of legislation.

Unfortunately, Pennsylvania's bill does only a slightly better job at addressing some of the spyware issues that the Iowa, Michigan, and New York legislatures failed to include in their versions of spyware legislation. Like the other three bills, the Pennsylvania bill prohibits the unauthorized transfer of user information and requires that a software download disclose the type of spyware, the type of tracked information, to whom the information is transmitted, an e-mail address of the spyware provider, and uninstall instructions.[129] The bill improves upon the scope of the other three bills by detailing prohibitions against some deceptive installation practices like piggyback installs and drive-by installs through pop-up windows.[130] By doing so, the Pennsylvania bill provides a broader coverage of spyware-related issues, but as a whole, like the Iowa, Michigan, and New York bills, it represents an inadequate legislative solution to the spyware problem. By analyzing the relative strengths and shortcomings of each bill, it is possible to formulate specific recommendations on how to draft an effective piece of spyware legislation.

V. RECOMMENDATIONS ON DRAFTING LEGISLATION

The greatest shortcoming of the existing federal and state legislation is their failure to outline a sufficiently broad basis for attacking spyware. Every piece of current legislation could be improved upon by adding provisions that address particular aspects of spyware that are omitted in the current bills.

In regards to the installation process used by software, legislation should prohibit the installation of bundled software when the user only requests the installation of one program (also known as piggybacking). Bills should also specifically forbid installers that proceed to perform their install routines when the user has declined the installation or has not given explicit authorization to install. The use of drive-by installs are another aspect of the spyware installation process that should be regulated. Drive-by installs that obtain uninformed consent of the user to perform the install through the use of pop-up boxes, or by leading the user to believe that installation is required to view a web site, are widely used by spyware programs and deserve attention in spyware legislation. Another deceptive installation practice occurs when an application loaded on a user's computer takes advantage of security holes in the user's system to install spyware without the user's consent. Finally, legislation needs to prohibit the use of installers that communicate misleading information about the program, such as false names of the software producer.

Functionality that interferes with a user's privacy, autonomy, and computer security should also be explicitly prohibited by spyware legislation.

129. H.B. 2788, 2003-04 Reg. Sess. (Pa. 2004), *available at* http://www.legis.state.pa.us/wuol/LI/BI/BT/2003/0/HB2788P4269.htm.

130. *Id.*

An example of such misuse of a user's computer is the unauthorized sending of user information, including personally identifiable information and information on computer usage like clickstream data, to another party. In conjunction with such a prohibition, acts should not allow spyware to deliver advertisements on the basis of what web sites users visit. Legislation should prohibit pop-ups that cover the original web site visited or distract the user from the site and forbid the concurrent displaying of multiple pop-ups to cause users to shutdown their browsers or entire computer system to continue operation of their computers. Software should not be allowed to hijack a user's system resources for the sole benefit of the developer of the spyware, nor change a user's system settings, including security settings. Lastly, software that disables anti-spyware or anti-virus software on a user's computer should be expressly prohibited because it assists spyware in achieving its goals.

One of the specific characteristics of spyware that most pieces of current legislation fail to properly address is the use of deceptive end user license agreements. Many of the bills require consent before software can install itself, but few define what constitutes informed and effective consent. Legislation should specifically state that verbose and confusing license agreements will not grant effective consent, and that software is required to provide a means for the user to view the license agreement in its entirety, whether in a hard or soft copy. Bills should require license agreements to disclose what type of information the software will transfer and for what purpose the information is collected. In the situation where multiple applications are installed by a single installer, a separate license agreement should exist for each application being installed. Lastly, legislation should also explicitly block the use of license agreements that prohibit users from uninstalling the loaded software using a third-party tool, like anti-spyware software, or that prohibit the use of a packet-snuffer or other technology to monitor what information is transmitted by the software.

In addition, all spyware legislation should address deceptive uninstallation practices. A solution to spyware cannot be complete if it allows software to create a difficult barrier to uninstallation. Effective legislation requires that the uninstall process is easy to understand and perform, and should require that the software provide uninstallation instructions. Such legislation should define what constitutes an unusually difficult uninstall process. A common method of complicating the uninstall process that legislation might describe is an uninstall process that allows software installed as a bundle to be uninstalled only by uninstalling every program in the bundle. Another deceptive uninstallation practice that legislation needs to address is the displaying of confirmation boxes that notify the user of a successful uninstall when in actuality, the software still remains on the user's computer. This illusory uninstall could allow the continued transfer of information or hijacking of system resources without the user's knowledge or consent. Lastly, legislation should prohibit

the distribution of software that automatically reinstalls itself after the uninstall process has completed.

The disadvantage of adding provisions that detail specific prohibitions associated with spyware is that such legislation can potentially become outdated over a short period of time as newer forms of spyware are introduced into the Internet community. The other alternative, crafting the language of spyware legislation in broad terms, would likely result in legislation that is over-inclusive and therefore ineffective in combating the problem. Legislators can either strive to strike a balance between being over and under-inclusive in drafting legislation, or they can pass legislation with the intent of periodically updating the act to address new issues that arise concerning spyware over time. The disadvantage of legislation that will require regular updating is that amending legislation and drafting new legislation to address new issues is a lengthy process, thus rendering the legislatures less effective in responding to new trends in spyware technology. However, the immediate spyware problems that affect the general public on a daily basis call for the passage of comprehensive acts that will stand to prevent the current problems associated with spyware, regardless of what the future holds. In order to have a comprehensive approach to attacking the spyware problem, society will need to partner such legislation with private means of curbing spyware.

VI. OTHER METHODS OF ADDRESSING SPYWARE

Although legislation will play a key role in preventing the proliferation of spyware, it is not a complete solution to the spyware problem. The use of technology, self-regulation, and user education are necessary to combat the problem of spyware.

From a technological standpoint, anti-spyware software, such as Spybot Search and Destroy and Ad-Aware, search computer hard drives and remove spyware software[131] but cannot guarantee identification of all spyware residing on a hard drive.[132] Newer technological innovations currently in the process of development would detect and prevent the installation of spyware completely.[133] In addition, standards like the Platform for Privacy Preferences ("P3P") will aid users in identifying spyware.[134] Developed by the World Wide Web Consortium ("W3C"), P3P facilitates the publication of "standard machine-readable statements of privacy policies" on web sites, which will assist users in distinguishing between spyware and legitimate software.[135]

Users can take a few simple precautions to greatly decrease the likelihood that spyware will infect their computers. Users should avoid install-

131. Center for Democracy & Technology, *supra* note 3.
132. *See* Spybot Search and Destroy License § II.b. Warranty, www.safer-networking.org/en/license/index.html (last visited Aug. 29, 2005).
133. Center for Democracy & Technology, *supra* note 3 .
134. *Id.* at 13.
135. *Id.*

ing advertisement-supported software, especially if a third party developed the advertising component, unless the software is distributed by a trusted entity.[136] Users should also research new software that they plan on installing and thoroughly read the license agreement before consenting to installation.[137] Users should be especially wary if the language of the license agreement is confusing and should seek clarification of the terms of the license before proceeding.[138] The privacy policies of software developers are also important items to scrutinize before installing software, and users should be suspicious if they cannot readily find one on a company web site.[139] In addition, users should deny download offers that appear in pop-ups and from unknown web sites.[140] Lastly, users can curb the malicious effects of spyware by maintaining strong passwords,[141] changing passwords often, and avoiding the use of public computers to access sensitive information.[142]

VII. CONCLUSION

The various forms of spyware that exist today pose a serious threat to the privacy and security of the average computer user. In order to draft effective spyware legislation, legislators need to have a comprehensive understanding of what forms of spyware exist and the problems that they create. They need to recognize that spyware includes software such as keystroke loggers, programs that surreptitiously install and transmit users' activities, programs that hijack computer system resources, and programs that strictly use the Internet connection to download software updates or content. Applications such as media players, tracking cookies, and legitimate advertisement-supported software do not pose the same level of security and privacy risks as spyware. Remaining informed of current developments in spyware is difficult, as new software that encroaches upon users' privacy and security is continually developed.

Even with a thorough understanding of the issue, drafting legislation is difficult because language that is under-inclusive fails to prohibit the use of some spyware programs and over-inclusive language unjustly prevents manufacturers from distributing legitimate forms of software. In light of this, legislation should contain some specific provisions that address common concerns of spyware. Bills should prohibit software from using deceptive install practices such as piggyback installs and drive-by installs. In addition, they should forbid software from interfering with a user's privacy, autonomy, and computer security, which spyware commonly performs through actions such as collecting and transmitting users'

136. *Id.* at 14.
137. *Id.*
138. *Id.*
139. *Id.*
140. *Id.*
141. Strong passwords do not use names or words found in the dictionary and contain a combination of letters, numbers, and symbols. *Id.*
142. *Id.*

personally identifiable information or disabling anti-spyware software. The use of deceptive end-user license agreements to gain user consent for spyware downloads is another aspect of spyware that every piece of legislation should address. Lastly, legislation should require that the uninstall routine is not overly cumbersome and actually accomplishes the removal of the software program from the user's computer. The difficulties associated with drafting effective legislation should encourage legislatures to fully understand the scope of the spyware problem before drafting, but they should not prevent legislatures from passing bills. It is impossible to predict every form of spyware that will plague computers in the future; therefore, legislation will never be able to perfectly address every spyware issue. Society needs some government intervention in curbing the effects of spyware, and passing comprehensive, yet imperfect, legislation will meet this need.

Although legislation provides a strong tool to wield against unscrupulous spyware programs, it alone cannot eradicate spyware. Technological innovations, such as anti-spyware programs and technology standards, will play a critical role in restricting spyware's effectiveness. In addition, computer users need to become more educated about how spyware works and take simple steps to prevent spyware from reaching their computers and networks. By combining legislative enactments with the resources of private industry and public education and self-regulation, spyware will hopefully cease to find its way into our computers and our lives.