CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

Ghosts in Our Machines:

Background and Policy Proposals on the "Spyware" Problem

November, 2003

Overview

Over the last several years, a loosely defined collection of computer software known as "spyware" has become the subject of growing public alarm. Computer users are increasingly finding programs on their computers that they did not know were installed and that they cannot uninstall, that create privacy problems and open security holes, that can hurt the performance and stability of their systems, and that can lead them to mistakenly believe that these problems are the fault of another application or their Internet provider.

The term "spyware" has been applied to everything from keystroke loggers, to advertising applications that track users' web browsing, to web cookies, to programs designed to help provide security patches directly to users. More recently, there has been particular attention paid to a variety of applications that piggyback on peer-to-peer file-sharing software and other free downloads as a way to gain access to people's computers. This report focuses primarily on these so-called "adware" and other similar applications, which have increasingly been the focus of legislative and regulatory proposals.

Many of these applications represent a significant privacy threat, but in our view the larger concerns raised by these programs are *transparency* and *user control*, problems sometimes overlooked in discussions about the issue and to a certain extent obscured by the term "spyware" itself.

In this report, we hope to:

- identify the range of applications referred to as "spyware;"
- clarify the core problem raised by these invasive applications;
- give examples of several varieties of applications that fall into this category;
- describe other kinds of software that have often (and we think, mistakenly) been lumped together with spyware;
- investigate the connection between spyware and peer-to-peer software;
- evaluate policy and other solutions to the spyware problem;
- and provide tips for users about what they can do today to protect their personal information and their computers from these programs.

Combating the most invasive of these technologies will require a combination of legislation, anti-spyware tools, and self-regulatory policies. However, it will be very difficult if not impossible to draft legislation that defines the spyware problem with sufficient specificity to tackle the problem in isolation from the issue of online privacy generally. We believe that it would be best to recognize this explicitly and address at least the privacy dimension of spyware as part of baseline Internet privacy legislation. At the same time, pending bills, because they focus on applications that take information from a user's computer, do not address the larger problem of control.

1. The Taxonomy of Spyware

There are at least three general categories of applications that are sometimes described as spyware. They are:

- key stroke loggers and screen capture utilities, which are installed by a third party to monitor work habits, observe online behavior, or capture passwords and other information;
- "adware" and similar applications that install themselves surreptitiously through "drive-by downloads" or by piggybacking on other applications and track users' behaviors and take advantage of their Internet connection;
- legitimate applications that have faulty or weak user-privacy protections.

It is in the first two cases that the spyware label is most appropriate. In the third case, it is not.

Programs in the first category, which are sometimes called "snoopware" to distinguish them from other categories of spyware, are typically stand-alone programs installed intentionally by one user onto a computer used by others. Some capture all keystrokes and record periodic screen shots, while others are more focused, just grabbing websites visited or suspected passwords. These programs have legal uses (e.g. for certain narrow kinds of employee monitoring) as well as many clearly illegal ones.

Software in the second category installs itself covertly, generally by piggybacking on another, unrelated application or by deceptive download practices. These programs start-up on their own and make unauthorized use of users' computers and Internet connections, in many cases transmitting information about the user or her computer back to a central location. They often resist uninstallation. By and large they do not capture keystrokes. In part because applications in this second category fall into a legal grey-zone, they have recently been the focus of a great deal of attention and concern. We focus primarily on this category of programs in this report.

It is important to distinguish these applications from software in the third category, which includes programs based on legitimate business models that incorporate features with flawed user privacy protections. Generally the problem relates to the unnecessary inclusion or inappropriate use of a unique program ID, which creates the potential for user tracking. We delve into this distinction at greater length in section four.

Of course, the lines between the three categories we present here can be fuzzy and it is sometimes difficult to tell which group any given application rightfully belongs in. Our concerns about the difficulty of translating these distinctions into precise legislative language is one basis of our preference for general baseline privacy legislation as a response to spyware. We discuss this issue in more detail in section six.

2. A Matter of Control

The vast majority of writing about the spyware problem to date has focused on the privacy dimension of the issue. Privacy is one of the major concerns raised by spyware, but the larger issues are *transparency* and *control*.[1] Users are typically unaware that spyware programs are being installed on their computers and often unable to uninstall them. These programs can change the appearance of websites, modify users' "start" and "search" pages in their browsers, or change low level system settings. They are often responsible for significant reductions in computer performance and system stability. In many cases, consumers are mistakenly led to believe that the problem is with another application or with their Internet provider, placing a substantial burden on the support departments of providers of those legitimate applications and services. Even in cases where these programs transmit no personally identifiable information, their hidden, unauthorized use of users' computers and Internet connections threatens the security of computers and the integrity of online communications. Arguably, a better term for many these applications would have been "trespassware."

In some egregious cases, these invasive applications closely resemble more traditional viruses. While many spyware programs piggyback on other applications or trick users into authorizing installations through deceptive browser pop-ups, some spread themselves by exploiting security vulnerabilities in email attachments or browsers.[2] In addition, many of these programs create major new security vulnerabilities by including capabilities to automatically download and install additional pieces of code without notifying users or asking for their consent and typically with minimal security safeguards. This capability is often part of an "auto-update" component, and it opens up a world of concerns on top of those posed by objectionable behaviors in the originally installed application itself.

Users should have control over what programs are installed on their computers and over how their Internet connections are used. They should be able to count on a predictable web-browsing experience and they should have the ability to remove for any reason and at any point programs they don't want. A growing body of invasive applications takes away this control.

[1] One of the first people to bring the issue of spyware to public attention, Steve Gibson, defines spyware as any program that fails to abide by the "Code of Backchannel Conduct:" "Silent background use of an Internet 'backchannel' connection must be preceded by a complete and truthful disclosure of proposed backchannel usage, followed by the receipt of explicit, informed, consent for such use." See <http://grc.com/oo/cbc.htm>.

[2] For example, the many variants of an invasive application called "CoolWebSearch" are believed to be spread through a security vulnerability in the Java "Virtual Machine" in some versions of Internet Explorer. Variants of this application reportedly integrate themselves with the user's browser, and can change the user's home page and search page, redirect mistyped URLs to pornographic sites, and serve pop-up advertising.

3. Examples of Spyware

Spyware applications differ with respect to the uses they make of their hosts' computers and Internet connections. These programs can be further divided into three categories on this basis:

- programs that collect information about the user, potentially including personally identifiable information, and send it back to a central server;
- programs that hijack a user's Internet connection (and potentially other resources as well) for the software's own use—for example as part of a distributed computing network or as a spam remailer;
- programs that use the connection only to download updates to the software or content it uses (such as advertisements).

To illustrate these categories, we describe in more detail a typical example of each.

nCase

The first category of spyware includes programs that collect information from a user's computer—in some cases including personally identifiable information such as a name or email address. This can compromise both a user's control over his computer and Internet connection and his privacy. Of course, the most egregious forms of keystroke logging or screen capturing spyware, for which the primary advertised purpose is monitoring or spying, clearly fall into this category, but so do many applications which piggyback on free downloads as a vehicle to serve advertising. One notable example of spyware of this variety is nCase, produced by 180Solutions.[3]

nCase is bundled with an array of free products, including some peer-to-peer applications. Once installed, it registers a unique identifier and tracks websites viewed, including monitoring search terms. In some cases, this information is reportedly aggregated with registration data collected by the affiliate application. There have also been reports that newer versions of the software attempt to read an email address, real name, or ZIP code from other applications' data in the registry, and to associate this information with the user's unique ID. 180Solutions reports that it keeps track of demographic information for at least 40% of its user base. This information can include age, sex, home and work location, and household income. nCase uses the information it collects to deliver targeted pop-up ads and sells the data to third parties. The company

[3] "Gator" is perhaps a better known example of privacy-invading spyware, which, like nCase, is often bundled with free downloads or finds its way onto user's computers through click-through installs in web pop-ups. Historically, Gator has been among the most frequently cited pieces of privacy-invading spyware. To target the advertisements it displays, Gator can track users' web-browsing, including gathering and transmitting information on search terms. Reportedly, some versions of the software also keep track of locale, zip code, and a user and machine ID Additionally, some versions of Gator include a "trickler" component that can remain after the rest of the software is uninstalled and redownload the main application in the background. The Gator Corporation, makers of Gator software, recently changed its name to Claria. Whether a change in Gator's practices will accompany the corporation's name change remains to be seen. Hoping that this will prove to be the case, we have opted not to highlight Gator in this report, despite its long history.

advertises the ability to “see a 360-degree view of the user's behavior—24 hours a day, 7 days a week.”[4]

On top of these substantial privacy problems, nCase raises significant user control issues. In addition to bundling with other applications, nCase has been accused of deceiving users into granting permission to download and install the application by presenting potentially deceptive or confusing pop-ups on various websites or by taking advantage of poorly configured security settings in users’ browsers (a practice known as “drive by downloads”). In addition, there have been reports of other spyware programs installing nCase in the background once they have gained access to a user’s computer. Although nCase does appear in the Add/Remove programs menu in Windows, its uninstallation process is notoriously long and complicated, and in instances where nCase is installed alongside another application, nCase generally remains on a user’s computer even after the original host application is uninstalled. On top of everything else, nCase has been reported to open up back doors into users’ computers, creating a significant security hazard.

Altnet

A second category of spyware consists of programs that do not represent an immediate privacy threat because they do not collect user information, but still hijack the user’s computer and Internet connection for their own purposes. The most prominent recent example is “Altnet.”

In April of last year, it was discovered that software with undisclosed networking capabilities was being bundled with the popular Kazaa Media Desktop. Installing the Kazaa file-sharing program also installed a companion program, “Altnet,” created by a company called Brilliant Digital Entertainment (BDE). Through Altnet, BDE had the ability to activate the user’s computer as a node in a distributed storage and computing network distinct from Kazaa’s existing peer-to-peer network. Users were never clearly told that software with the capability to use their computers and network connections in this way was being installed.

Since the discovery of BDE’s intentions in a securities filing, the company has acknowledged its intent to launch the Altnet network, publishing the following description on its website:

> Altnet is giving you the opportunity to opt in to making certain parts of your computing power, disk space and bandwidth available to Altnet business partners. You will know exactly how a business would use your source at the time of use. You choose what jobs can use your machine and which ones cannot. Altnet will charge its business partners for this service and pass on benefits to you. All this will be conducted with absolute respect for your privacy and your choices.[5]

[4] See <http://www.180solutions.com/License/nCASEExplained.aspx>.

[5] See <http://www.brilliantdigital.com/content.asp?ID=779>.

However, the section of the Kazaa/Brilliant end user license agreement (EULA) dealing with Altnet paints a somewhat different picture:

> You hereby grant BDE the right to access and use the unused computing power and storage space on your computer/s and/or internet access or bandwidth for the aggregation of content and use in distributed computing. The user acknowledges and authorizes this use without the right of compensation. Notwithstanding the above, in the event usage of your computer is initiated by a party other than you, BDE will grant you the ability to deny access.

There are several major problems with Altnet from the perspective of user control. Although BDE included a statement of the purposes of the Altnet program buried in the EULA that comes with Kazaa, this hardly represents the kind of clear, conspicuous notice that should accompany requests to access a user's Internet connection. The widespread dismay that accompanied the disclosure of BDE's intentions to construct a distributed computing network demonstrates that the consent BDE was receiving from users of Kazaa was not, by any stretch of the imagination, well-informed.

Moreover, the terms BDE set forth in the EULA provide for substantially more permissive access to users' computers than what BDE now claims on its website will be done with the Altnet network. Whereas BDE now claims that the service will be "opt-in," the EULA reserved the right to make it "opt-out." Whereas BDE says it will "pass on benefits" to users in exchange for use of their computers, in the EULA, BDE reserved the right to make use of user's processing power and bandwidth "without … compensation."

Finally, while Brilliant points out that it is possible to uninstall BDE/Altnet without disabling Kazaa, it is an extended process that involves at least twelve steps, including tracking down and deleting files scattered across Windows' "System" folders. Additionally, although the BDE application piggybacked on Kazaa during installation, uninstalling Kazaa generally does not uninstall Altnet.

Aureate/Radiate

The third category of spyware includes programs that are primarily used for advertising but do not track users. Because these programs do not monitor users in order to target ads, they typically do not represent as much of a privacy threat as the first group of programs. And while they may be a major annoyance to the average user, they are unlikely to take over control of a user's computer to the same extent as software in the second category.

One of the "granddaddies" of spyware, Aureate/Radiate, is a typical example of spyware in this category. Aureate sparked much of the initial public concern about spyware. Aureate later changed its name to "Radiate." The company is now defunct, but millions of copies of the software remain installed on users' computers, and the example is still instructive.

Aureate/Radiate is an advertising application that was bundled with a variety of freeware products. It downloaded advertisements from a home server and presented them as banner-ads integrated with its host application.

As privacy advocate Steve Gibson writes in his extended analysis of the program:

> Aureate deserved—and continues to deserve today—the "Spyware" moniker **not** (apparently) because it is sending sensitive personal data out of the user's computer, but because it deliberately slips into the user's system secretly, uses the user's Internet backchannel without the user's knowledge or permission, takes pains to remain secretly installed (instructing its hosting software to leave it installed upon the host's removal), masks its presence by deliberately suspending its use of the backchannel in the absence of keyboard or mouse activity and fails to disclose any of this to the typical user who is **never fully informed** about what's going on. [6]

Originally, many of the products that included Aureate as a bundled component did not include Aureate's EULA, though this was fixed by the company in subsequent releases. While the later versions of the program can be uninstalled from Windows' "Add/Remove Programs" menu (though earlier versions cannot), even later versions of Aureate/Radiate are generally not uninstalled when its host program is removed.

Aureate/Radiate did collect demographic data, but it was in a labeled survey that popped up when the software was installed. The software also monitored ad-views and click-throughs, but other tracking of users has not been confirmed.

Probably the biggest problem with Aureate/Radiate is that, like many other spyware applications, it can silently and insecurely download "updates," which it installs and runs without user prompting. By opening this insecure back door into the user's computer, the software creates a host of control issues on top of those raised by the installation of the application itself. Although Radiate has gone out of business, the security holes created by Aureate/Radiate remain open on computers that have the software installed. The program is also known to cause Windows and Internet browser crashes.

4. Spyware's Relatives

Several other pieces of software and user-tracking technologies have often been grouped together with the core spyware programs. These include applications that unnecessarily send user information back to a central server, whether or not that data is actually used for tracking. They also include tracking cookies, which, while they share many features of spyware, are not standalone applications. The concerns raised by these other technologies differ in important ways from the concerns raised by spyware specifically.

Overcollection of information

Version 8 of Windows Media Player and RealJukeBox for Windows 98 were both accused of being spyware after the release of widely publicized studies outlining ways in which the software could potentially be used to track user behavior. In February of 2002, privacy and security consultant Richard Smith discovered that what was then the current version of Microsoft's Media Player contacted a Microsoft web server to get title and

[6] See <http://grc.com/oo/aureate.htm>.

chapter information every time a new DVD movie was played. This request included a cookie that uniquely identified the player. In theory, this would have allowed Microsoft to track the viewing habits of the user of a particular player. At the time of Smith's discovery, Microsoft's privacy statement did not disclose that this contact was being made and did not give the user a chance to opt-out. In response to Smith's criticism on this point, Microsoft pointed out that there were ways to reset the unique ID associated with the player or to block use of the DVD lookup feature altogether, and clarified that it was not using the data for tracking of any sort. Microsoft also updated the privacy policy associated with Windows Media Player.[7] Subsequent versions of Media Player have been revamped to include more visible privacy options and more carefully thought out privacy defaults.

The RealJukeBox software for Windows 98 had a very similar problem, also discovered by Richard Smith. The software sent back a unique ID to RealNetworks along with requests for track information every time the user put in a new CD. In the RealJukeBox case, this was the same ID used when the software was registered, meaning it could potentially be linked with personal information submitted during registration. RealNetworks, like Microsoft, said it did not store or link the usage data in this way and changed its privacy policy to give notice about the transmission after Smith publicized the problem. [8]

When Smith posted his findings about RealJukeBox and the Windows Media Player, both programs were accused of being spyware.[9] While the functioning of both pieces of software was of concern from a privacy perspective, they differ from spyware in important ways. In particular, the programs only installed components directly related to their core functionality; they did not include "piggyback" applications; and both programs were relatively easy to uninstall through standard means. While their privacy protections were poorly designed, both programs transmitted the objectionable information as part of communications to serve the primary purpose of the application and did not initiate wholly secondary connections for advertising or other purposes. In short, these were media applications with poor attention to privacy, not advertising or distributed computing applications piggybacking on some other program.

Tracking cookies

User-tracking cookies have also frequently been grouped with spyware, although cookies themselves are not applications. DoubleClick is one of the most well-known and largest advertising and tracking networks. A wide array of high traffic sites, including websites like CheapTickets.com and Lycos.com, use embedded ads that are drawn from DoubleClick's central servers. Using browser cookies, DoubleClick is able to track users as they move from one DoubleClick site to another. While DoubleClick previously used

[7] For Smith's full account of the story, see Richard Smith, "Serious privacy problems in Windows Media Player for Windows XP", February 20, 2002, <http://www.computerbytesman.com/privacy/wmp8dvd.htm>.

[8] See Richard Smith, "The RealJukebox monitoring system," October 31, 1999, <http://www.computerbytesman.com/privacy/realjb.htm>.

[9] See, e.g. Don Labriola, "Is Media Player Spyware?," *ExtremeTech,* March 6, 2002, <http://www.extremetech.com/print_article/0,3998,a=23649,00.asp>.

browsing profiles to generate targeted advertising, the company has since dropped targeted Web ads as a major component of its business model.

User-tracking cookies like DoubleClick's can pose privacy concerns, which CDT has addressed before.[10] But while tracking cookies are often grouped with spyware, unlike spyware they are not standalone applications—they take advantage of poor practices in the way some (particularly older) browsers handle cookies. For this reason, tracking cookies can only affect users so long as they are browsing DoubleClick affiliated websites. Similarly, many of the issues regarding installation and uninstallation that come up with spyware do not arise in the case of cookies because newer browsers offer a variety of ways for users to control how cookies are handled, including allowing users to block all cookies from a particular domain.

Legitimate ad-supported software

Finally, it is important to distinguish spyware-carrying programs from legitimate ad-supported applications and their accompanying advertising components. The Eudora email client is an example of an application that has, for some time, been distributed in an ad-supported version. Users are able to get the software for free provided they are willing to tolerate a small advertisement window that accompanies the program. In this "sponsored" mode, Eudora periodically contacts a central server to download updated advertisements.

Although it uses the user's Internet connection to download advertisements (a task that is not directly connected to the primary function of the application), Eudora differs from spyware in several ways. First, it is possible to purchase an ad-free version of Eudora—the user is given the choice between paying for the software normally and paying by watching ads. Eudora also provides conspicuous notice of its advertising and the fact that the user's Internet connection will be used to retrieve ads. Moreover, the advertising component is directly linked with the main email application—it is not produced by a third party, meaning that the user does not have to deal with multiple points of consent and different EULAs, Eudora cannot just "pass the buck" on any problems that arise with the advertising component, and the advertising component is automatically uninstalled when Eudora is uninstalled. In contrast, spyware-carrying applications typically require the user to read different EULAs for different parts of the program, pass off responsibility for the privacy practices of bundled components, and fail to link uninstallation of the advertising software to uninstallation of the main software.

5. Spyware and Peer-to-Peer

A great deal has been made of the connection between spyware and widely downloaded peer-to-peer file sharing programs. Peer-to-peer has been accused of causing, or at the least greatly accelerating, the spread of spyware. The video and music industries have publicized the bundling of spyware with peer-to-peer programs as a way to discourage use of those services and the copyright infringement for which they are often used.

[10] See e.g. CDT, et al.'s Statement of Additional Facts and Grounds for Relief regarding DoubleClick's Abacus Online Alliance, filed with the FTC February, 2000. Available at <http://www.cdt.org/testimony/000225ftcdcstatement.shtml>.

There is validity to these concerns. Many of the most popular file sharing applications do come bundled with spyware. The millions of downloads of these applications are likely in no small part responsible for the spread of spyware, and the sometimes obscure origins of peer-to-peer programs can make accountability problematic. Peer-to-peer applications are some of the worst culprits when it comes to obscuring notice by bundling EULAs together and making uninstallation of spyware components as difficult as possible.

At the same time, not all peer-to-peer file sharing applications carry spyware; some peer-to-peer programs do respect user control. Open source "Gnutella" clients like Gnucleus are particularly noteworthy in this regard.

There are also many ways for spyware programs to find their way onto users' computers other than peer-to-peer programs. Among the most common are deceptive or confusing pop-ups in web browsers and bundling with non-peer-to-peer "free" utilities. A recent informal PCMagazine study found that the computers of "non-file-sharing" users contained many of the same spyware programs as the computers of users who regularly used file-sharing software, including CyDoor, Alexa, BDE, Gator, and Aureate.[11]

It is also worth noting that, especially since coming under heavy fire for bundling spyware, some peer-to-peer software companies are apparently beginning to change their practices. Kazaa, for example, now offers a commercial version that the company claims is free of add-ins.

6. Legal Responses to Spyware

Existing Law

Three existing laws may have relevance to at least the most extreme examples of spyware, although none of the three laws are directly responsive to some of the technology's unique features and all may fail to cover some of the most common cases. The Electronic Communications Privacy Act (ECPA)[12] makes it illegal to intercept communications without a court order or permission of one of the parties. ECPA only covers communications, not data stored on the hard drive of a personal computer, but collecting click-through data and other web browsing information can constitute a violation of ECPA. However, applications that work with the consent of the user (however deeply buried in a user agreement the relevant terms may be) or the consent of the websites being visited probably do not violate ECPA.

The Computer Fraud and Abuse Act (CFAA)[13] may also apply to some uses of spyware. Programs that are spread by exploiting security vulnerabilities in network software and that co-opt control of users' computers or exploit their Internet connection may constitute a violation of the CFAA, especially in cases where those programs are used to steal passwords and other information. However, spyware that infects a computer without interfering with its operation or adding to the user's cost may not violate the CFAA.

[11] Cade Metz, "Spyware—It's lurking on your machine," *PC Magazine*, April 22, 2003. Available at: <http://www.pcmag.com/article2/0,4149,978170,00.asp>.

[12] 18 U.S.C. § 2510-21, 2701-12.

[13] 18 U.S.C. § 1030.

Additionally, as with ECPA, programs that work with the consent of the user, even if obtained in a long or confusing EULA, probably do not violate the CFAA except in especially egregious cases.

The statute that may have the most direct relevance for the most common varieties of spyware is Title 5 of the Federal Trade Commission Act, which gives the US Federal Trade Commission (FTC) the ability to take action against unfair and deceptive trade practices.[14] Both categories may apply to some of the most invasive kinds of applications discussed above.

Deception cases can be brought against companies that tell consumers they are doing one thing and then do another. These cases have been common in the privacy and security arena when companies have promised high standards in their public privacy notices but have not followed through in practice. If an unwanted application is installed without giving the user notice in the EULA or another form, or if the EULA is misleading or unclear, leading consumers to think they are downloading one program when in fact they are downloading and installing an application that does something completely different, this could likely be considered a deceptive practice.

Unfairness cases can be brought against companies that trap consumers into unwanted payments. For example, the FTC recently brought a case against D Squared Solutions, a company that took advantage of the defaults in Windows Messenger Service to repeatedly send pop-up ads to Internet users.[15] The ads requested money in exchange for an application to block future pop-ups—a sort of pop-up blackmail. In certain cases, companies promoting invasive applications that only manage to get user consent through especially long and confusing EULAs; that utilize consumer resources such as computer power or bandwidth or that capture personal information; and that are difficult to uninstall could be engaging in an unfair practice.

Despite the potential applicability of Title 5, the FTC so far has not brought any major actions against spyware makers or spyware distributing companies.

Proposed Legislation

The growth of the spyware problem has prompted several proposals for new legislation to address the privacy dimension of the issue. Representative Mary Bono (R-CA) and Senator John Edwards (D-NC) have each introduced legislation targeted specifically at spyware, while Senator Ernest Hollings (D-SC) has included a section applying to spyware in a more comprehensive bill to establish baseline privacy standards on the Internet. In addition to the three bills for which language has already been introduced, Senator Conrad Burns' (R-MT) office has indicated that he may introduce a bill targeted at spyware.

The slipperiness of the term "spyware" makes it very hard to craft a definition that is precise enough for use in legislation. For this reason, we believe it will be extremely difficult to adequately address all of the privacy concerns with spyware outside the

[14] 15 U.S.C. § 45.

[15] FTC v. D Squared Solutions, No. 032-3223 (D. Md. filed Nov. 10, 2003).

context of general privacy legislation. Rather than trying to pin down some subset of computer applications that ought to be regulated, we believe it makes more sense to articulate the basic privacy standards to which all programs should be held.

At the same time, even considering the issues associated with spyware in isolation, legislation introduced to date has been an incomplete solution to the problem insofar as it has focused primarily on the privacy dimension of spyware. Privacy legislation would not, for example, deal with software that commandeers computing resources without revealing user information, like Brilliant Digital's Altnet program. We argue that a full solution to spyware must deal with the user-control aspects of the issue—piggybacking, avoiding uninstallation, and so on. More thought needs to be given to spyware as a problem of trespass in addition to as a privacy issue.

The "Safeguard Against Privacy Invasions Act," H.R. 2929

Representative Bono, along with Representative Edolphus Towns (D-NY), introduced the "Safeguard Against Privacy Invasions Act" in the House in July 2003. The act would require that transmission of all "spyware programs" be preceded by a "clear and conspicuous request" for transmission of the program and would require notice of all personally identifiable information that is gathered and transmitted. The bill defines a "spyware program" to be "any program or software that can be used to transmit from a computer, or that has the capability of so transmitting, by means of the Internet and without any action on the part of the user of the computer, information regarding the user of the computer, regarding the use of the computer, or that is stored on the computer."

The Bono bill currently covers much more than what people typically consider to qualify as "spyware." Its definition of spyware potentially encompasses a tremendous array of programs—for example, the bill would cover most cookies, including many session cookies that are only temporarily stored in web browsers. In response to some of these concerns, Rep. Bono's office has indicated that they are working on a revised version of the bill, which will include a narrower definition of spyware and will add provisions relating to uninstallation of software and software that changes user settings without authorization.

The "Spyware Control and Privacy Protection Act of 2000," S. 3180

An earlier bill, Senator Edwards' "Spyware Control and Privacy Protection Act," suffers from similar problems. The Edwards bill, like the Bono bill, would create notice and consent requirements. Edwards' version would apply to "[a]ny computer software made available to the public, whether by sale or without charge, that includes a capability to collect information about the user of such computer software, the hardware on which such computer software is used, or the manner in which such computer software is used, and to disclose such information to any person other than the user of such computer software." The bill would exclude software that only collects information for authorization/registration, technical support, or legal monitoring of employees. Even so, the definition potentially encompasses a wide array of network applications, including web browsers and software update utilities. Edwards' bill was originally introduced in 2000, and has not been reintroduced in subsequent sessions of Congress.

The "Online Personal Privacy Act," S. 2201

Senator Hollings' "Online Personal Privacy Act," passed by the Senate Commerce Committee in the 107th Congress, but not reintroduced this year, is more ambitious than the Bono or Edwards bills. The legislation would set a baseline privacy standard for all online transactions. The notice and consent requirements that the bill would place on spyware are, in broad strokes, similar to those laid out in the Edwards and Bono bills. However, the Hollings bill more fully specifies and elaborates on those requirements as befits its larger intended scope. By creating different standards for different types of information, it creates appropriate levels of protection for different collections of information. While CDT believes that several provisions of the Hollings legislation still need revision, we think it represents a much more promising approach to the spyware issue.

In summary, based on the current proposals, CDT believes that attempts to regulate spyware as an isolated issue are likely to be both over-inclusive and under-inclusive, ending up as broad privacy legislation while failing to cover some kinds of spyware. We think that baseline privacy legislation should be undertaken consciously as a full project, of which spyware should be one necessary component, as it is in the Hollings bill.

Even if baseline privacy legislation is passed to deal with the privacy aspects of the spyware issue, the broader control problems still remain. Good legislation has not yet been proposed that would deal with the control aspects of the spyware problem, but regulation may yet have to be part of a solution to this broader issue as well as to the narrow question of privacy.

7. Other Ways to Combat Spyware

Technology measures, self-regulation and user education will also be critical components of any spyware solution. Companies must do a better job of helping users understand and control what their computers and Internet connections are being used for, and users must become better educated about how to protect themselves from spyware.

A variety of technologies to help deal with these invasive applications and related privacy issues are in various stages of development. Several applications exist that will search a hard-drive for spyware applications and then attempt to delete them. These include AdAware, Spybot Search and Destroy, Spyware Eliminator, and BPS Spyware/Adware Remover. In addition, several groups are working on ways to detect and quarantine spyware programs before they are even installed.

Increasingly, standards such as the Platform for Privacy Preferences (P3P) may also play an important role in aiding transparency on the Internet and providing users with more control over their computers and their personal information. P3P is a specification developed by the World Wide Web Consortium (W3C) to allow websites to publish standard, machine-readable statements of their privacy policies for easy access by a user's browser. Standards like P3P will facilitate privacy best practices that will help users distinguish legitimate software from spyware.

For now, there are several specific things users can do to help deal with these invasive applications:

- Run one of the spyware detection and removal utilities. Especially if a computer demonstrates noticeable slowdowns, instability, or odd behaviors, including changed settings, there is a good chance it is infected with spyware. Consider repeating the process occasionally.
- Be wary of installing free, ad-supported applications unless they are from a trusted party, particularly if the advertising component is provided by a third party.
- Read up on new software and read its licensing agreements before installing it. If the information you find is confusing, send the company email asking detailed questions. Users should be able to feel comfortable about any software they install.
- Check for and read privacy policies posted on company websites, and be extremely wary if no readily accessible policy exists.
- Do not accept downloads from pop-up windows or from unknown websites.

In particular, reading up on applications from independent sources such as computer magazines and Web sites before downloading them is a simple but especially important and effective measure for combating spyware.

In addition, users should always take basic security precautions to protect themselves from spyware and snoopware. Simple measures include keeping different strong passwords (passwords should not be names, or found in the dictionary and should contain numbers or symbols) and changing passwords frequently. When using a public computer at an Internet café or a library, it is probably a good idea to avoid accessing sensitive information such as bank accounts. Those users who must use public Internet sites to access sensitive information should be especially vigilant.

While no surefire strategy for avoiding spyware exists, and many of the anti-spyware technologies are in their infancy, these steps represent basic care that users can take now to guard their privacy and help maintain control over what applications are installed on their computers.

Conclusion

Spyware represents a serious threat to users' control over their computers and their Internet connections. The increasing attention paid to the spyware issue, from articles in the popular press to bills introduced in Congress, is a positive trend.

But spyware is a complicated problem, and it will require a multifaceted solution. Congress has a role to play by passing baseline Internet privacy legislation that includes appropriate spyware provisions. At the same time, we cannot assume that legislation alone can address all of the concerns raised by spyware. Industry self-regulation and better technology tools are also essential to give users control over their digital lives.

For further information, contact:
Ari Schwartz, Associate Director
Alan Davidson, Associate Director
Michael Steffen, Policy Analyst
1634 I Street NW, Suite 1100
Washington, DC 20006
202.637.9800