# SEMINAR REPORT

# ON

# SPYWARE

# CONTENTS

# INTRODUCTION

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;

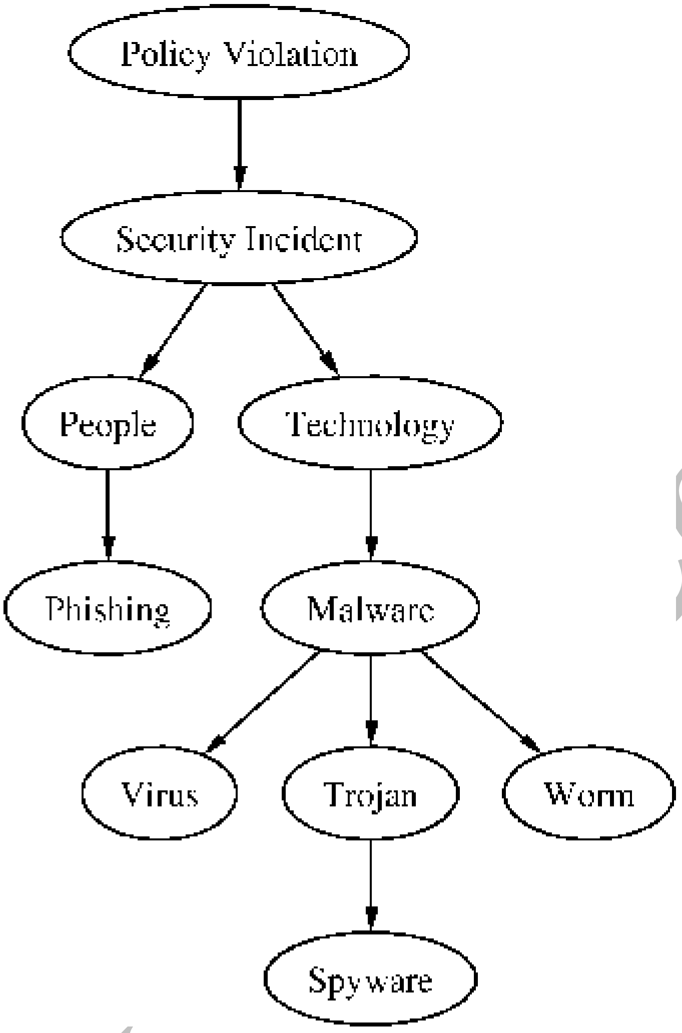
- describe other kinds of software that have often (and we think, mistakenly) been lumped together with spyware;
- investigate the connection between spyware and peer-to-peer software;
- evaluate policy and other solutions to the spyware problem;
- and provide tips for users about what they can do today 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.

Software to observe user behavior to collect information under users' noses is often called spyware. These systems have become central to a heated debate regarding online privacy, prompting the U.S. Congress to consider several bills. In addition, the very nature of such systems--the collection of data that would not otherwise be available outside of corporate firewalls--raises questions about how companies can remain compliant with privacy-oriented regulation like the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Financial Modernization Act of 1999 (GLBA).

## What is Spyware?

In its most simple form, spyware is software designed to collect information from computer system users without their knowledge. Typically, spyware can be classified as a type of trojan horse, which is a type of technology-based security incident, allowing for information security policy violation. Figure 1 shows where spyware fits within the broader context of policy enforcement.



## Features of spyware?

Over the past few years, a new class of software has emerged that's up to no good. It goes by many names: spyware, adware, foistware, malware, eulaware, or even crapware. For simplicity we'll just call them all spyware. Here are some of the "features" you get from spyware. Some spyware may only use one or two of these tactics, while others do quite a bit more.

- **Deceptive functionality.** Spyware often uses a classic "trojan horse" tactic--like a virus. It offers to synchronize your PC's clock or keep track of forms, but it is also doing other hidden things while you browse.
- **Home page hijacking.** Did you ever find that your home page was changed, or discover

new sites in Favorites that you didn't add? It might be spyware.

- **Loss of privacy.** Some spyware keeps track of the web sites you visit and sends that information back to the spyware vendor. Do you want to tell everyone?
- ***More* advertising.** Did you install a popup stopper but you are still getting popups? The ads you are getting may not be from the web site you are on, but from spyware.
- ***Stolen* advertising.** Instead of showing the ads that should appear on a web site, some spyware substitutes its own ads which can rob a web site of revenue.
- **Broken web sites.** Spyware sometimes changes the actual content on a web page, and in the process it "breaks" the page. The page may not look correct, or you may get Javascript errors.
- **Reduced performance.** Spyware uses up system resources, CPU time, memory, disk space, and Internet bandwidth, making your system slower.
- **System instability.** Most spyware isn't very well tested or debugged, and there is no way to report bugs or obtain tech support. The result can be system crashes, hangs, or other strange behavior.
- **Security risks.** Some spyware has a built-in update feature that lets the spyware maker download and install new code to your system without your knowledge or approval.

## HOW SPYWARE WORKS

There’s not a specified single format that these menaces apply to infiltrate your computer. Spyware usually attacks your machine when you, quite unknowingly commit yourself into doing what technically speaking is not the wisest thing to do. Something like when you click on a pop-up window. The main jobs of these applications are often to use scam-like means so that you unknowingly install them, from messages containing counterfeit system alert inducing you to click a certain button. Here the button referring to a "cancel" maybe a fake one too, as they really intend to do the opposite.

There are quite a few known ways that spyware may attack your computer. To start with, Piggybacked software installation process will install spyware as a part of their standard installation system. You have to read the installation list closely to notice that you're getting more than the file-sharing application you want. This is generally and especially true for the software versions marked as “free”. This software is supposed to be your free gift and you intend to buy it in place of the original one. So it is evident that whatever you feel absolutely free is in fact not, instead it is bugged with elements such as a menace like spyware.

When we come to Drive-by download process of spyware installation is when a Web site or pop-up window automatically attempts to download and install spyware on your machine.

The Browser add-ons are that software that is camouflaged as to provide improvement to the user’s Web browser. Sometimes it works as a Trojan horse in form of an additional toolbar or search box. More often than not, they actually do what they are supposed to do or promised to do. But it is not that it will stop there only. They actually also include elements of spyware as part of the deal. Sometimes still, they are nothing more than disguised spyware themselves.

Another interesting process that spyware manages to get into your system is Masquerading as an anti-spyware. This type of software convinces you that it's a tool to detect and remove spyware. It in fact tells you that your system is free from any unwanted material while all the way it is installing the same menace into your computer.

Once inside your computer Spyware can do any number of things on your computer. To start with, and in the most minimal sense, most spyware runs as an application in the monitor background as soon as you start your computer up, this process hogs up the RAM and processor power. As per its application function it would generate endless pop-up ads as a result making your Web browser unfeasible to use as it would become so staggeringly slow. It also resets your browser's home page to exhibit an ad every time you open it.

Some spyware also redirects your Web searches, controlling the results you see and making your search engine basically ineffective. It can also alter the dynamically linked libraries that are used to connect to the Internet, thus affecting connectivity. This is very difficult to make out. Then there are certain types of spyware that can alter your Internet background so that when connected through dial-up service, it becomes much more expensive thereby hiking your telephone bill to the zenith.

Some spyware even changes the basic settings of your firewall, thus inviting in more unwanted pieces of software as a more menacing result. If you think that's enough variety of vicious spyware, hold your breath. There are even some forms that are intelligent enough to know when you try to eradicate them in the Windows registry and interrupt your efforts to do so.

These are programs that in reality actually act as spying bugs. These are designed like a ghost to take the weight off its feet and park itself cozily on your desktop and capture delicate private information like usernames and passwords. Think of that! They are mainly programmed to show you bundles of pop-up ads and fake search results there by claiming credit for displaying that ad. So, each time you click the ad button they act as a counting procedure as if the user is interested in the product that the spyware is meant to promote without you acquaintance. You are actually helping the product with an extra hit giving it an extra mileage in the trading sector.

Do you think that's all they do? Spyware is also used to embezzle affiliate credits. The sites, like Amazon.com and Ebay.com which are basically shopping sites, put forward credit to those Web sites that effectively express transfer of hits to their pages containing their commodities. Certain spyware applications incarcerate your requests to view sites like Amazon and Ebay and then take the credit for transferring you there.

## Who are the main purveyors of spyware?

The biggest culprits in spreading spyware are the popular peer-to-peer programs available today. Bearshare, Kazaa, Imesh, Limewire - all of these products install multiple advertising spyware applications. It's gotten so bad that I now assume all p2p programs bundle spyware unless I've tested them personally.

I've even started a list of p2p programs that I've tested and proven to be spyware-free. I am the only person allowed to post to this list. If someone wants a program added to this list, I have to test it first and log the installation activity before I'll add it. Tragically, this list has very few products on it. If nothing else, that should tell you how bad the problem is.

## Hardware spyware

Nowadays spyware can even be found accompanying hardware you buy and install in your system. Yes, the software you install with hardware purchased from certain manufacturers (some even well-known) may include spyware agents.

## Spyware categories

- **Adware networks**

The backbone for big time spyware are ad serving networks that pay publishers of games, utilities and music/video players per download, to include their ad serving programs.

- **Stalking horses**

A number of programs that enable the adware networks to function on desktops are bundled in many popular programs and often (not always!) presented in installation disclosure screens as desirable add-ons to their Trojan horse hosts. All collect information.

- **Trojan horses**

The popular Internet downloads usually come with the ad serving network basic software and at least one stalking horse.

- **Backdoor Santas**

Stand-alone programs that incorporate similar approaches have no links to ad serving networks and collect information from users.

- **Cookies**

Netscape Navigator and Internet Explorer will still send out existing cookies even after disabling cookies in the browser settings. You must manually delete any/all cookie files on your system to eliminate being tracked by third-party ad networks or spyware or adware providers.

## Threats Affect Online Behavior

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.

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.

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.

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.** 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 clickthroughs, 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.

## 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.

## 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 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. 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.

## Legal Responses to Spyware

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. Cade Metz, "Spyware—It's lurking on your machine,". 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 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 qualifying 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 tom 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.

## Why don't most antivirus utilities block spyware?

The short answer is *"spyware is not a virus."* Webopedia defines a virus as "A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes." Spyware takes advantage of the fact that people click I Agree to most software licenses without actually reading them. So *technically*, spyware is loaded with your knowledge and permission if you read the license, so it's not a virus. Of course, if your teenager uses the computer and installs spyware without *your* permission, that's *your* problem too. Here are some examples of spyware tricks. This tricky use of software agreements puts the antivirus companies in a tough situation. It is possible that you really did agree for some of this software to be on your system. If antivirus utilities flag these borderline programs as viruses and remove them, the antivirus companies could find themselves in a legal battle with spyware makers who claim they were given permission to install.

## How do I get rid of spyware?

You can either remove each program manually, or use a utility to automatically remove all spyware. For the automatic route we recommend Pest Patrol and Spyware Doctor because it does the best job of finding and removing all spyware. To use a manual removal method, you first need to determine what types of spyware have infested your system. Our quick scan can find some of the most common spyware (but see below for an important note). Each piece of spyware requires different removal procedures. Sometimes the spyware maker has an uninstaller at their site, but usually there will be some additional steps required before you have completely eliminated it. (This can include editing the Windows registry and/or deleting files, so it is *not* something that we recommend for novice users!) In some cases we provide links to manual removal procedures in your spyware scan results. If not, you can ask in the Spyware section of the PC Pitstop Forums or use Google to search for removal instructions using the name of the spyware. Please note: Although our online spyware scan will find the most common types of spyware, it's not meant to be a replacement for a commercial product to defend you against spyware and viruses. We've kept this test small and simple so that we can quickly find the most common spyware threats. If our scan detects several different types of spyware on your system, it's possible that there is even more spyware that we did not detect.

## How SurfControl Stops Spyware SurfControl Prevents Spyware from Reaching the Desktop

The SurfControl Enterprise Protection Suite™ integrates best-in-class Web, E-mail and End Point security solutions to protect against ever-changing spyware threats that increasingly exploit multiple threat vulnerability points. SurfControl's unified approach simplifies protection across these multiple threat entry points. (e.g., Web browsing, e-mail, IM, P2P, portable media, mobile workers). This multi-layered solution is highly relevant as blended attacks find new ways to render conventional anti-spyware security measures obsolete.

SurfControl's Enterprise Protection Suite shields organizations against emerging threats by using Adaptive Threat Intelligence from its Global Threat Experts. These researchers continuously analyze and research Internet threats and provide automatic security updates to protect customers.

Enterprise Protection Suite Consists of three key anti-spyware defense layers:

- Web Threat Protection (SurfControl Web Filter, SurfControl Mobile Filter)
- E-mail Threat Protection (SurfControl E-mail Filter, SurfControl RiskFilter)

Two of the most popular tools for fighting spyware are Ad-Aware Personal SE and SpywareBlaster. They should be used in conjunction with each other, and they are both free with frequent free updates.

Ad-Aware Personal SE will scan your computer for existing spyware and alert you to what it finds. You can quarantine suspected spyware bugs so they can no longer function. It is very important to read the manual as removing spyware can lead to system or software problems if done incorrectly.

After running Ad-Aware Personal SE to quarantine or remove the spyware, run SpywareBlaster to prevent new spyware from being installed in the first place.

## Mitigation (means shanty)

There are two primary methods to deal with spyware: the first is to look to the host (computer that could have spyware installed) and the second is to look at the network.

## Host-Based Solutions

The host-based solution will provide several valuable options. The best of which is *prevention*. By using systems that are not vulnerable to the kinds of attacks that spyware--particularly thee nasty variety not discussed here--one will gain a measure of protection; the vulnerabilities in ActiveX, for example, that enable such problems are simply not present in other operating systems like MacOS, Linux, and FreeBSD. Note that not all spyware works by ActiveX controls, however--the Pharmatrak system worked for any Web-based system; users of these systems would (and, indeed, did) have information about them collected. Another host-based option is to create a standard “build” of the desktop system for users that includes not only the operating system and applications, but also defense mechanisms such as anti-malware packages. A significantly less effective mechanism is spyware “removal.” While this might appear to be a more attractive solution than prevention in some cases (because there is no need to justify the expense of an anti-spyware package on the grounds that such a threat might materialize in the future), it should be noted that any software running on a system that has been compromised might not be able to behave as advertised. In particular, malware that changes operating system libraries could cause a “removal” program to do more damage than harm to the system in question. The safest option in the event of a system compromise is to throw away the compromised installation and to replace it with one that can be trusted--which takes us back to the standard build option mentioned earlier.

## Network-Based Solutions

Another option is to take a network-based view of the system. That is, to configure intrusion detection systems, firewalls, and other policy enforcement mechanisms to prevent spyware packages from working. The first means of doing this would be to identify unsafe content (e.g., ActiveX controls) flowing from an untrusted zone (e.g., the Internet) into a trusted zone (e.g., an internal network) and blocking the download. Another means would be to identify attempts of spyware to “phone home,” effectively preventing them from being able to report their activity, but not preventing the spyware from hitting the user's system in the first place. A third mechanism would be to enforce a policy that refuses connectivity from trusted systems to unknown sites or to allow downloads of unidentifiable content.

## Blocking

- **ZoneAlarm**
  A personal dynamic firewall that allows you to block spyware communication. With Stealth mode enabled, the firewall renders your computer invisible to the Internet and to

potential intruders. Mind you, we find that ZoneAlarm itself wants to know too many details about its users. 1.5Mb.

- **Outpost**

  A personal firewall that supports plug-ins. Includes intrusion detection, ad blocking, content filtering, e-mail guard and privacy control.

Spyware-Guide.com provides a Spyware Block List File which blocks all known "bad" ActiveX controls from running inside Internet Explorer by setting the "Kill bit".

## 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.

# REFERENCES

[1] www.google.co.in

[2] www.ask.com

[3] Spyware\Interhack Introduction to Spyware.htm

[4] www.pewinternet.org

[5] www.cdt.org