Comments by Eric L. Howes on the Problem of Spyware in Advance of the FTC April 2004 Spyware Workshop

Mar. 29, 2004

Federal Trade Commission
Office of the Secretary
Room 159-H
600 Pennsylvania Avenue N.W.
Washington, D.C. 20580

Re: Spyware Workshop – Comment, P044509

The FTC is to be commended for hosting a workshop on the problems that spyware poses to consumers and citizens on the internet. Spyware is fast becoming the most serious threat to the privacy and security of internet users, and it is imperative that the FTC take action to protect consumers and citizens from the unscrupulous behavior of companies that use advertising software to force their commercial messages on unwilling and vulnerable consumers. These comments are submitted with the hope that they might aid the FTC's efforts to understand the threat of spyware to consumers and develop an effective response to it.

Background

I am a graduate student in the Graduate School of Library and Information Science at the University of Illinois at Urbana-Champaign. For the past twelve years I have also taught business and technical writing at the University of Illinois. More recently I have begun teaching at Parkland Community College in Champaign.

Over the past four years I have maintained a personal web site at the University of Illinois (http://www.staff.uiuc.edu/~ehowes/) to supply internet users with resources to protect their privacy and security on the internet. Among those resources are several utilities and "block lists" that allow users of Microsoft's Internet Explorer web browser to protect themselves against the flood of unwanted software and content pushed on them by aggressive advertising and marketing entities.

In recognition of my work to help internet users protect their privacy and security, Microsoft recently awarded me its MVP (Most Valued Professional) Award (http://mvp.support.microsoft.com/).

Experiences with Spyware

My experience with spyware stems not only from the time I spend helping users troubleshoot PC problems but also from the research I perform to update the tools and "block lists" used by visitors to my web site. Users, including my students, frequently ask me for help removing spyware from their computers, and I provide advice and support both online and in person. In addition to assisting users, I have also spent thousands of hours in online forums over the past few years, examining HijackThis! logs posted by users with spyware-infested systems and investigating the software and companies responsible for the problems of those users.

In working with students and online users, I have watched spyware grow from a marginal problem that once affected only a small number of users who unwittingly installed advertising supported freeware (often called "adware") to a commercial plague of aggressive "hijackware" that now afflicts the majority of the PCs of users who request help from me. During the few years that I have researched spyware for my "block lists" and other tools, the number of web sites known to distribute aggressive "hijackware" has grown from a few dozen to a few thousand; the number of companies or entities engaged in distributing spyware has grown equally fast. Most alarming to me, though, is the increasingly aggressive nature of this spyware, whose creators seem to find ever more sophisticated ways to push their software on unsuspecting users and hijack consumers' computers for commercial purposes.

The spyware that I find installed on users' PCs proves troublesome to users for three reasons. First, users who request help are simply bewildered and flummoxed by this spyware. They almost never know how it was installed on their computers and do not recall ever having agreed to the installation of such software. On the rare occasions they do remember the installation, users maintain that they did not fully understand the true functionality of the software. In many cases these users do not even recognize that spyware is installed on their computers and mistakenly attribute their PCs' problems to more traditional (and familiar) "malware" such as viruses, trojans, and worms.

Second, these spyware programs can severely degrade the stability and usability of victims' PCs and prevent consumers from using their computers and internet connections as they choose. The computers that I fix are usually sluggish and unstable, prone to errors and crashes, and are unable to connect to the internet in some cases. Even when the performance of their PCs is not degraded, these spyware victims are frequently subjected to a raft of unwelcome system changes. Users often complain that their desktops are littered with intrusive pop-up advertising, that unwanted toolbars and other widgets have been added to their browsers and desktops, and that their browsers' default home page and search engine preferences have been changed without their consent.

Third, however, these users often cannot remove the spyware from their PCs by themselves or even prevent the future installation of unwanted spyware. The vast majority of users that I help are not "computer savvy" and find even basic computer maintenance tasks challenging and intimidating. These people are typically not aware that some spyware can be removed with an uninstaller provided by the vendor. In cases where an uninstaller is not available or fails to do the job, these users face significant hurdles in attempting to use an anti-spyware application to remove the unwanted software. When these users do manage to locate and download effective anti-spyware programs, they often cannot use those anti-spyware programs properly and effectively because the problems that the anti-spyware programs identify on their computers are simply too numerous and bewildering. Still worse, spyware victims are usually unfamiliar with what they could do to prevent spyware from being installed on their computers in the future, and the preventative solutions that do exist frequently prove too complex and frustrating for these users to employ.

A Typical Case of Spyware

The most recent case in which I fixed a student's computer is a good illustration of the problems I have just summarized. One of my students came to me because her PC (less than a year old) had suddenly stopped connecting to the internet, preventing her from accessing her email, browsing the web, or using her instant messaging software. This broken internet connection proved especially troublesome because she was in the middle of a job search, and had been researching and talking with companies online in order to secure employment after graduation (just a few months away). As I questioned this student about her PC's behavior, she complained about a number of other problems including system instability, inexplicable error messages, and the mysterious appearance of pop-up advertising on her desktop. She thought her PC's problems were caused by a virus or worm of some sort.

When I finally sat down at her computer the true cause of her PC's problems became clear. Her computer was not infected with a virus or worm (a system scan with a reputable anti-virus program confirmed as much). Rather, a dozen or so different varieties of spyware were installed and running on her computer. One of those spyware programs I immediately recognized because it replaces key Windows networking files and reconfigures systems' networking settings -- a likely cause of her broken internet connection.

To remove the spyware, I first ran every vendor-supplied uninstaller that I could find. Many of the spyware programs had not shipped with an uninstaller, however. While some of the associated companies may make uninstallers available on their web sites, we could not access those web sites because the PC's internet connection was broken. Still worse, the uninstallers I did manage to find failed to remove the associated spyware programs completely. More importantly, though, even after I had run the vendor-supplied uninstallers the PC's internet connection was still broken.

This student had managed to download and install SpyBot Search & Destroy 1.2 a few days earlier (I had recommended that anti-spyware application to her class). She had failed, however, to update the program's definition databases (she didn't understand that it was necessary to do so). Moreover, she hadn't fixed any of her PC's problems because she found the long list of problems that SpyBot reported too daunting and confusing. And no wonder: when I ran SpyBot Search & Destroy, it flagged several hundred serious problems to be fixed on her PC, and that was with severely outdated definitions.

After I ran SpyBot Search & Destroy and rebooted the computer, SpyBot did manage to fix the vast majority of the PC's problems, some of which had been left behind by the vendor-supplied uninstallers. SpyBot even restored the PC's internet connection, which the vendor-supplied uninstallers had failed to do. With the internet connection restored, I then downloaded Ad-aware 6.0, new definitions for SpyBot Search & Destroy, and several programs to protect her computer from future spyware. I had to perform several more system scans with SpyBot and Ad-aware before this student's computer was finally usable. Before leaving, I installed several programs to protect her computer against future installations of spyware, though she had difficulty understanding how those programs work.

This student's encounter with spyware is all too representative of the problems that average internet users report with spyware. As I identified one spyware program after another on her computer, I asked this student if she remembered installing each program or consenting to its installation by clicking through a EULA (end user license agreement). With every single one of those programs, she insisted that she had not knowingly installed it (though she did recognize the name of one of the programs because of the pop-up advertising on her desktop).

When I found the particular program that had broken her internet connection, I even explained that program's ostensible purpose or function and described the company's business model. Not only was she unfamiliar with the program, she was positively bewildered by its functionality (and this, mind you, is a program from a company who insists that users always consent to installation of its software by clicking through a EULA at some point).

All of the spyware programs on this student's computer, I should add, were installed via the web; there were no advertising-sponsored "freeware" programs (such as P2P file sharing applications or "download managers") on her computer -- I checked.

This case of spyware is quite similar to those of most other spyware victims that I have helped online and in person. In working with such users and their PCs I have learned that:

- Spyware is usually installed on victims' computers without their full knowledge, consent, and understanding;

- Spyware is sufficiently complex and confusing that users find it difficult or impossible to keep spyware off their systems;
- Spyware frequently trashes users' computers, denies users the full enjoyment of their PCs and internet connections, and even prevents its victims from fixing the problems it caused;
- Spyware often proves too difficult to remove for normal internet users, even after users download and install anti-spyware applications;

Some spyware victims do manage to get help from more experienced users, either through an online forum or in person. Those who cannot get free assistance from experienced users, however, might need to call tech support from their OEMs or take their PCs to a computer repair shop and pay for a system repair or re-installation, either of which can prove expensive.

Whether or not they manage to get help, spyware victims are denied the full use of the PCs and internet connections that they purchased. Moreover, they are forced to waste an untold number of frustrating hours repairing the damage to their PCs and restoring their systems to a fully functional state (if indeed they ever manage to do so).

Ten Myths About Spyware

As consumer outrage over spyware has grown, the spyware industry has developed a number of excuses to defend its software and behavior. Let me address the most frequently propagated excuses or myths about spyware.

Defining Spyware

1. Software that doesn't surreptitiously monitor users and collect personally sensitive data is not spyware and thus isn't of any concern.

Although the term "spyware" has proved popular with internet users, it has caused more than its share of confusion because the term implies functionality (data gathering, backdoor connectivity, etc.) that some intrusive, unwanted software may not have. We should not let a confusion over terminology, however, distract us from the real goal of protecting users from unwanted, abusive software that is installed on consumers' PCs without their full knowledge and consent.

The term "spyware" was first used to describe unwanted commercial software during the spring and summer of 2000, when consumers became aware of "adware" -- advertising sponsored "freeware" -- which often does monitor system use and report potentially sensitive data to advertisers for the purpose of targeted advertising. The term "spyware" proved to be a catchy one, and consumers were soon using it to describe or name all manner of unwanted software that engaged in unwelcome behavior -- even software that did not technically "spy" on users. In other words, the term "spyware" has become a loose, broad term used by consumers for a wide variety of unwanted, intrusive software that consumers understandably and rightfully deplore.

Some companies have argued that software that does not meet a strict, narrow definition of spyware (system monitoring, data gathering, backdoor connectivity) should be excluded from the discussion of spyware. Were we to do so, we would ignore the vast majority of problems that consumers experience with unwanted commercial software. In fact, some the more widely distributed (and despised) forms of advertising software may not meet a strict definition of spyware, however, this software usually engages in other abusive behavior such as:

- installing on PCs without users' full knowledge, consent, and understanding;
- making unwelcome modifications to users' systems and web browsers to drive users to online commercial sites and services;
- adding unwanted toolbars and other widgets to users' browsers and systems;
- displaying unsolicited advertising on users' desktops through pop-ups that interfere with consumers' everyday use of their PCs;
- preventing users from reversing the changes made to their systems and browsers;

All of these problems warrant attention from the FTC, and we should not let distributors of unwanted commercial software define their products out of the discussion by insisting on a narrow, self-serving definition of spyware -- a term with a problematic usage history. If another term or name is needed for the kinds of software that consumers are complaining about, then let us find it.* The problems that consumers face with unwanted advertising software are too serious to be dismissed on the basis of a mere definition dispute.

* Note: for a discussion of one possible replacement for the term "spyware," see my "Junkware: A New Name for Spyware," included with these comments.

2. Software that presents users with a EULA is adware, not spyware, and users elect to install such software on their systems.

Spyware companies have resorted to another similar argument over the term "spyware" to insist that their software be excluded from the discussion of problems associated with spyware. On this argument, software that requires users to click through a EULA (end user license agreement) or similar legal agreement cannot be considered spyware because users' acceptance of the terms of a EULA allegedly indicates their awareness and understanding of the software. Such software is not "spyware," it is argued, but rather "adware," a seemingly innocuous form of commercial advertising software.

There are any number of problems with this argument, not the least of which is the unwarranted assumption that users who click through license agreements are fully aware (or could even become fully aware) of the software's true purpose and functionality. All too many of the EULAs that consumers encounter with unwanted software are presented in confusing, pressured circumstances -- in the midst of several pop-ups from a web site that refuses to work unless the user installs the correct plug-in, for example.

Moreover, these EULAs often couch complex, even outrageous, terms of agreement in long, dense blocks of legalese that few consumers have any hope of understanding. Many of these EULAs point to still more EULAs from other associated parties, requiring users to track down and plow through a pile of prose so daunting that few would ever venture to attempt it.

Still worse, some users may not even see the EULAs. Spyware companies often distribute their software through automated installations of ActiveX controls on web sites. These automated installations -- referred to by many users as "drive-by-downloads" -- are initiated by the web pages that users visit or the pop-ups spawned from those pages, not the users themselves. When web sites initiate program installations, users may or may not see a EULA. Whether they see a EULA is dependent not only on consumers' ability to use the meager amount of information provided Microsoft's Internet Explorer web browser, but also on the security settings for the Internet zone within Internet Explorer.

Internet Explorer provides users with information about ActiveX programs installed via "drive-by-downloads" and the software vendors responsible, however, this information is often not helpful in determining the potential risks of ActiveX programs. With the default Internet zone settings users should see an Internet Explorer dialog box requesting their agreement to the installation of a program (i.e., an ActiveX control). Though this dialog box is titled "Security Warning," it provides almost no specific information that might help users understand the programs to be installed on their computers. Nor does it contain any strong warning that might alert users to potential privacy and security problems with this program. Although, this "Security Warning" box also provides a clickable link for users to get more information about the program -- usually the EULA -- it is quite easy for users to miss that information link. If users don't click the link, they won't see the EULA.

Some "drive-by-downloads" are initiated by web pages or pop-ups that do provide more information about the ActiveX controls, however, that information is usually not helpful in assessing privacy and security risks (it's usually promotional puff and hype). Moreover, if users are inundated with multiple pop-ups from a web page, they may not correctly associate the "Security Warning" box with the pop-up that caused it and may even think the program issues from the web site they are visiting, which may be a trusted source.

Given the poor quality of information presented to users during "drive-by-downloads" as well as the confusing manner and context in which that information is often delivered, it is not at all surprising that users would think nothing of clicking through Internet Explorer warning boxes without the slightest idea that they might be allowing intrusive spyware onto their systems.*

If the security settings for the Internet zone are low enough, however, users won't even see the "Security Warning" box (let alone the EULA) -- the ActiveX controls or programs will simply install automatically. It is not uncommon for users to lower the security settings for Internet Explorer's Internet zone (the default security zone for all web sites) in order to get relief from the barrage of confirmation prompts (including the ActiveX "Security Warning" boxes) that result from surfing the web with the default Internet zone settings. Users simply do not understand that by bwering their Internet zone settings they are effectively rolling out the welcome mat for unwanted software, which can then install on their systems with no prompt or warning whatsoever.

It is difficult to imagine that spyware distributors are unaware of the problems that users experience with automated "drive-by-downloads" and complex EULAs that few people can make any sense of. When spyware distributors couple dense crops of legalese with disorienting "drive-by-downloads," the effect on confused consumers is not unlike the bewilderment created by the fast-talking door-to-door salesman who gets his foot in the door and, in a flash, is in your living room, busily vacuuming the carpet and arranging shelf space for a new set of encyclopedias.

These companies benefit enormously from such confusion, as many of them have business models that are built upon the widespread distribution of their software -- even to consumers who might not normally be interested in their programs. Spyware distributors have no business exploiting users' ignorance of computers and the law -- a deadly combination, to be sure -- only to claim that consumers' complaints ought to be ignored because users somehow "elected" to install their companies' software.

The sad fact is that we would not even be discussing the problems with spyware if spyware distributors started providing better notice to users and stopped distributing their software through means and methods that they surely know are likely to cause complaints from consumers.

* Note: for a more detailed discussion of the problems with "drive-by-downloads," see my "The Anatomy of a Drive-by-Download," included with these comments.

Distribution of Spyware

3. *If users would stop surfing porn sites and crackz/warez sites, the spyware problem would solve itself.*

When consumers visit web sites associated with pornography (porn sites) or pirated software (warez/crackz sites) they are certainly more prone to encounter unwanted, abusive spyware. Plenty of users, however, pick up spyware by visiting completely "legitimate," "mainstream" web sites or by installing apparently innocuous software from seemingly reputable sources.

If porn sites and warez/crackz sites were to disappear from the web tomorrow, we would still have a spyware problem. Indeed, spyware distributors would likely ramp up their efforts to distribute their software through more "mainstream" web sites frequented by large numbers of consumers.

Finally, it is well known that the online porn industry serves as a kind of "test bed" for new technologies and business practices. Technologies and practices that were once the exclusive province of porn sites just a few years ago are now commonplace on the "mainstream" internet. Moreover, as any number of spyware distributors themselves have argued, spyware could very well become an attractive means for large, "mainstream" online entities to push their commercial messages on users, especially given the problems that have plagued the online advertising industry over the past few years.

4. *If users would stop installing P2P file-sharing applications, the spyware problem would solve itself.*

As with porn sites and warez/crackz sites, consumers who carelessly download and install popular P2P (peer-to-peer) file sharing applications could find that they have also installed spyware that was bundled with those host applications. The potential risk of P2P file sharing applications is a red herring, though -- at least for the purposes of our discussion of spyware. There are plenty of P2P file sharing applications that do not bundle spyware. Moreover, consumers face the threat of spyware from many other sources. P2P file sharing applications could be driven from the Net tomorrow, and consumers would still face a problem with spyware.

5. *Users can easily prevent spyware from being installed, so it's their fault when it is installed.*

There are indeed several anti-spyware software packages that allow users to prevent the installation of spyware on their systems. Some of the better ones include JavaCool's SpywareBlaster and SpywareGuard, the SpywareGuide ActiveX block list, the several custom-built HOSTS files available on the Net, and my own utilities for Internet Explorer (IE-SPYAD and Enough is Enough!). Moreover, users can customize their Internet Explorer security zone settings to "lock down" Internet Explorer and guard against the installation of unwanted spyware. These preventative approaches, however, all have problems that could make them unsuitable for many, if not most internet users.

First, many of these preventative approaches are too complex for average internet users to employ. These prevention methods often demand a familiarity with computers and a set of skills that are simply beyond what most users could be expected to acquire. Still further, they require users to master a complex set of trade-offs between privacy and security (on the one side) and convenience and usability (on the other), and the technical act of balancing of these trade-offs can challenge even the savviest of computer users. Even the simpler preventative solutions confront users with a potentially steep learning curve.

Second, most of these preventative approaches leave consumers vulnerable to new forms and versions of spyware, much as anti-virus programs leave users vulnerable to new viruses, worms, and trojans (at least until updated signature definitions are installed). Spyware distributors have become increasingly aggressive in pushing their unwanted software on users, frequently (sometimes even daily) modifying and morphing their software to bypass anti-spyware applications. Still worse, spyware distributors have been developing ever more complex and sophisticated means to foist their software on users' systems, much as spammers have resorted to ever more byzantine methods to get their unwanted bulk commercial email past spam filters. In some cases, these newer distribution methods have proved so complex that it takes dedicated anti-spyware developers days, and even weeks, to develop a response.

In such an environment, average internet users have not a chance of protecting their systems. And note that we haven't even begun to discuss spyware distributors who use deceptive or even fraudulent pop-ups (e.g., fake error boxes and system notices; prompts to install false "updates" from Microsoft, et al) as well confusing graphical interface elements (e.g., mislabeled or misleading buttons and hyperlinks, uncloseable popups, et al) to trick users into installing software. Still other spyware vendors exploit known security holes in Microsoft's software to automatically install their programs on consumers' PCs.

Finally, in a troubling turn of events, spyware distributors are increasingly and noisily complaining that anti-spyware developers interfere with the installation of their software. It is not unreasonable to expect that spyware distributors might very well resort to the court of law to ensure that consumers have no recourse whatsoever to third-party spyware-prevention methods and tools.

Effects of Spyware

6. ***Spyware isn't a significant problem because users can install anti-spyware applications to protect their PCs.***

The anti-spyware market has grown by leaps and bounds over the past few years, and consumers certainly have a number of spyware removal applications to choose from. Among the several excellent free spyware removal tools are Lavasoft's Ad-aware Personal and PepiMk's SpyBot Search & Destroy. There are also several for-pay applications such as PestPatrol and Webroot's Spy Sweeper. Big-name anti-virus vendors like McAfee and Symantec have also entered the market recently. Despite this wealth of anti-spyware scanners (which work much like more traditional anti-virus scanners), many consumers will not find these programs to be a satisfactory solution to the problem of spyware.

First, as was the case with spyware prevention methods, these scanning programs are much too complex for many consumers to use properly and effectively. The root of this difficulty stems from the complex nature of the spyware problems that these anti-spyware applications flag for users. So daunting are the scan results from anti-spyware applications, that it is not uncommon to find users who have installed and run an anti-spyware application on their computers only to balk at fixing problems because they are too intimidated to do so.

Second, because of the complex and fast-changing nature of spyware, consumers will often have to resort to several anti-spyware applications to clean their systems properly. Despite the excellent quality of the better known applications, no single one of them will do the job by itself. Thus, consumers must learn to use not one but several new applications. Some of these spyware removal applications may be highly specialized, such as Merijn's CoolWebShredder or Javacool's RapidBlaster Killer. These specialized tools are designed to remove particular types of spyware and are frequently updated to keep pace with the applications they target.

What's worse, even a combination of standard anti-spyware scanners may not be able to fix all of the spyware problems on consumers' PCs, especially when dealing with very new and sophisticated types of spyware. In such cases, users may have to download HijackThis! (a free program that logs key system settings) and post a HijackThis! log to an online forum for experts to review. All too many users will simply be unable to go through such a long and difficult journey to remove unwanted spyware from their systems.

Third, some spyware applications now block the download of anti-spyware utilities and deny users access to anti-spyware resources on the Net where they could get help. There have also been a small number of spyware applications that have maliciously uninstalled anti-spyware tools on users' hard drives or sabotaged them to prevent their use. Average consumers unfortunate enough to be victimized by one of these vicious spyware applications are utterly at the mercy of spyware vendors because they are denied the tools and resources to establish control over their own computer systems.

Fourth, anti-spyware scanners have many of the same shortcomings as spyware-prevention methods. The protection they offer always lags, to some extent, behind the newer spyware threats that appear on the Net almost daily. Given that some spyware applications are known to break users' internet connections or even block access to anti-spyware resources on the Net, consumers can easily fall prey to new forms of spyware that their anti-spyware scanners do not recognize, only to be denied access to the updates or online assistance that would allow them to remove that unwanted spyware.

Fifth, anti-spyware scanners only fix problems after the toll has been exacted on users' PCs and the damage done. No anti-spyware scanner can give back to users the lost, frustrating hours during which they were denied the use of their computers and forced to clean up after intrusive, unwanted software.

Sixth, we should also note that the uninstallers provided by spyware vendors themselves are not a viable solution either -- at least not in their current forms. As discussed earlier, not only do many spyware applications lack uninstallers, but the vendor-supplied uninstallers that do exist often fail to remove the associated applications completely. Consumers must have access to those uninstallers if they are to use them, however. Many uninstallers are offered only on vendors' web sites and are not included with the installed applications. As consumers often will not be able to identify the source of unwanted software on their systems, they won't be able to locate and access the vendors' web sites to download the uninstallers (which are frequently tucked away in obscure corners of those sites). And as was the case with the student I helped recently, uninstallers available on vendors' web sites do no good at all when spyware breaks the user's internet connection. Given the hoops that some spyware vendors force users to jump through in order to uninstall their applications, it is difficult to come to any other conclusion but that these vendors go out of their way to deliberately discourage and even prevent users from removing their unwanted applications.

Finally, as we noted earlier when discussing spyware-prevention methods, spyware distributors are becoming more aggressive in going after anti-spyware vendors, complaining loudly about the interference with their software, and even threatening legal action against anti-spyware vendors. Given such a hostile environment, it is an open question whether anti-spyware vendors will continue to be able to provide users with effective spyware detection, protection, and removal.

Anti-spyware vendors offer critical resources for consumers who are cleaning up their systems after a bout with spyware. As welcome as these resources are, they are no substitute for strong consumer protection against the more abusive and dangerous practices of the spyware industry.

7. ***Spyware is just another form of advertising that helps support free content on the Net; anti-spyware applications that block or remove spyware undermine the implicit contract between internet surfers and the web sites they choose to visit for free.***

What is surprising and frustrating about this argument is that it flies in the face of so many of the other excuses offered for spyware distributors and commercial advertisers more generally. The commercial advertising industry has long argued that consumers need no federal legislation to protect their privacy on the Net because consumers have access to software applications to protect themselves. Private market solutions, we have been told over and over, are far preferable to intrusive governmental mandates. On this earlier argument, privacy and security software gives consumers choices and thus negates the need for governmental intervention in the marketplace.

As we noted above, the anti-spyware market has indeed exploded in response to consumer complaints about spyware (even if problems with anti-spyware tools remain). Confronted with a free market solution to the problem of spyware, however, the spyware industry now suggests, incredibly enough, that such private solutions are illegitimate and perhaps even illegal. Where the commercial advertising industry once headed off privacy legislation by pointing to the choices offered consumers in the free market of software tools, the spyware industry (a part of the larger commercial advertising industry) now appears to insist that consumers ought to be denied the use of such tools.

No solution to the problem of spyware, it would seem, is acceptable to the spyware industry. It argues that its software ought not be subjected to governmental regulation because that software does not meet a narrow, self-serving definition of spyware; it argues that consumers "elect" to install its software, only to insist that consumer complaints be ignored; it blames consumers for being ignorant and careless in maintaining their systems, only to insist that consumers have enough privacy protection by virtue of the many anti-spyware applications on the market. After all this, however, the spyware industry then hints that those very same free market solutions and choices might themselves be illegitimate.

What lies at the end of this sorry litany of excuses and protests is an arrogant, offensive, and even dangerous assumption: namely, that consumers are ethically (and perhaps even legally) obligated to submit themselves and their systems to intrusive advertising software; that consumers' computer systems ought to be open for hijacking and use by commercial advertisers; that internet users and citizens are obligated above all else to become passive eyeballs for whatever online advertisers choose to put in front of them; and that, finally, consumers and citizens ought to have no choice or say in the matter. Were we to accept such a proposition, we would effectively reject any hope that the internet, with all of its portent and promise, might become (or even remain) a vital communications medium for citizens. Instead, it would degenerate into merely another passive medium in which disempowered consumers -- not engaged and active citizens -- are subjected to the whims of dominant commercial interests. I would hope that the FTC would see clear to avoid this outcome by protecting internet users from the more unscrupulous demands and tactics of commercial advertisers.

8. ***The spyware "controversy" has been concocted by greedy anti-spyware companies to cash in on users' fears and paranoia.***

This myth or excuse can be only be described as amusing. Presumably the spyware industry would have us believe that internet users would be perfectly happy with broken PCs, hijacked browsers, and pop-up infested desktops, if only the anti-spyware industry would just be quiet about it. We would also have to believe that the millions of users who have downloaded anti-spyware applications and have flocked to anti-spyware sites for help and advice are simply deluded -- that the problems are all in their heads, and that anti-spyware vendors planted those nefarious delusions in what would surely count as one of the more stunningly successful propaganda or public relations campaigns of the past hundred years. Such is the heady, noxious stuff of self-serving fantasy, and anyone who has actually worked with users whose PCs have been trashed by intrusive spyware will surely recognize that the spyware industry is simply blowing smoke.

But not completely. In a strange twist of circumstances, the spyware industry does have a point -- but not quite the point it thought it had. There are indeed unscrupulous anti-spyware vendors on the Net who resort to high pressure sales tactics and who prey on users' fears and cash in on their paranoia by springing cheap scares (e.g., opening users' CD-ROM trays, "exposing" the contents of their C-drives, et al) on gullible web surfers. Not surprisingly, many of the anti-spyware applications from such vendors turn out to be so much snake-oil. Prone to "false positives" and yet seriously deficient in detecting real spyware threats, these "rent-a-coder" anti-spyware applications flag non-existent problems on users' computers and then demand payment to fix them -- a classic con game.

These rogue anti-spyware applications, however, do not emanate from the well-known anti-spyware vendors, advocates, and activists who have earned users' trust over the past four years. Rather, they often issue from elements of the advertising and marketing industry itself including, incredibly enough, companies that are known to distribute spyware. These rogue applications even fool users by trading on the trusted names of legitimate anti-spyware programs (e.g., "spybot") in their advertising through Google's "Ad Words."

Thus, it is true in some sense that the spyware problem was concocted by anti-spyware vendors. Not only have some rogue anti-spyware vendors distributed the very types of software they promise to clean off users' computers, but unscrupulous elements of the advertising industry have rushed in to the market to exploit users' fears. Legitimate, trusted anti-spyware vendors such as those I mentioned earlier, however, have played no part in this charade. In some cases, they have even been the victims.

Solutions to Spyware

9. Once users are educated about spyware, the spyware problem will solve itself.

If there has been one common theme throughout this discussion of "spyware myths," it has been that normal, average, everyday, non-tech-savvy internet users are at the mercy of aggressive spyware distributors who do everything in their power to foist unwanted software on these vulnerable consumers.

Rather than rehash the many relevant points once again, let me point to an interesting, and ultimately depressing, experiment in computer user education that has been going on for some ten years. I am, of course, referring to the problems of traditional malware -- viruses, trojans, and worms -- as well as the inability of normal computer users to learn safe computer behavior or even to use anti-virus applications properly and effectively to defend their PCs. Anti-virus applications have been around since the late 1980's, and viruses and worms slightly longer than that. Of all the privacy and security problems that face consumers, traditional malware is the most familiar to them. Moreover, of all the myriad privacy and security applications on the market, anti-virus programs have achieved the highest levels of market penetration and consumer adoption.

One would think that after ten plus years of ongoing efforts to educate computer users about the threat of malware and the proper use of anti-virus applications we could expect results -- perhaps only modest evidence of small steps towards improved security, but tangible results nonetheless. As the unprecedented wave of viruses and worms over the past year should have demonstrated, such is not the case. Some five years after the first mass email worm rocketed around the internet, many users are all too willing to open unknown attachments. And over ten years after anti-virus applications were introduced to the consumer market, many computer users still do not understand that they must update their anti-virus application's virus definitions; nor do they even know how to perform a manual scan of their hard drives. (Anyone who works with average computer users should be able to confirm the truth of these grim assessments.)

I am an educator by profession and choice. If anyone regards education optimistically, it is I. Indeed I already spend a good deal of my time attempting to educate users about spyware problems. As noted just above, however, this ongoing experiment in computer user education is both highly suggestive and extremely depressing in what it tells us. We would be wise to heed the lessons here and resist the urge to place too much faith (or find too many excuses) in the prospect that users might solve the spyware problem themselves by simply getting educated about it.

10. Once the industry develops a "self-regulation" plan, the spyware problem will solve itself.

As noted earlier, the problem of spyware is but the most recent stage of a longer struggle over the best ways to protect consumers' privacy online. At earlier stages in this struggle, the internet advertising industry (along with other online commercial interests) rejected federal regulation and insisted that a "self-regulatory" market solution would be far preferable and even more effective as a means for protecting consumer privacy. After successfully fending off most privacy legislation, the advertising industry turned to the task of crafting a plan for "self-regulation." What the industry came up with, however, has been something less than a smashing success. Faced with serious consumer complaints about privacy violations, the industry essentially declared, "Let them eat privacy policies!" Even the addition of a meager supplementary diet of P3P compact policies and third-party trustmarks has done little to satisfy or assuage consumers' privacy concerns.

When we consider the threat of spyware, the problems with industry "self-regulation" remain the same. It is simply not realistic to expect that an industry would suddenly learn the virtues of self-restraint when that industry stands to benefit enormously from the widest and most intrusive distribution of its software possible. That this same industry is now making noises to the effect that consumers are obligated to accept its advertising software and that anti-spyware applications are illegitimate intrusions into the marketplace should be still further cause to doubt the ability of this industry to regulate itself.

Conclusion

As this has been a long discussion, I will keep my concluding remarks brief. The FTC now confronts a problem that is quickly becoming the most significant threat to the ability of consumers and citizens to use their computers and the internet in a private and secure manner. It also faces an industry which is largely unrepentant about what it does and the way it does it -- an industry arrogant enough to suggest that consumer complaints are largely a figment of the imagination and that internet users have no choice but to accept its unwanted, intrusive offerings. I sincerely hope that the FTC would see through such bluster and excuse-making and find a way to offer citizens and consumers the protection they need.

Respectfully submitted,

Eric L. Howes