Monitoring Software on Your PC:
Spyware, Adware, and Other Software

Spyware Workshop
Comment P044509

Submitted to the Federal Trade Commission
by Webroot Software, Inc.

May 21, 2004

Webroot Software, Inc., was founded in 1997 to provide computer users with privacy, protection and peace of mind. Today, Webroot provides solutions and services for millions of users around the world, ranging from enterprises, Internet service providers, government agencies and higher education institutions, to small businesses and individuals.

Among its award winning products is Spy Sweeper, winner of PC Magazine's 2004 Editors' Choice award. In the April 5 issue of Business Week, Stephen Wildstrom, author of the "Technology and You" column also recommended Spy Sweeper, referring to Webroot as the "established leader" in the market.

Webroot's world headquarters is located in Boulder, Colorado, with a European headquarters in Frankfurt, Germany, and sales offices in Chicago, London, Amsterdam, and Paris. Webroot products are sold online at www.webroot.com, and at leading retailers around the world, including Best Buy, CompUSA, Circuit City, Fry's, Staples, MicroCenter and WalMart. In addition, Webroot provides a full suite of privacy and security solutions designed to help ISPs like EarthLink provide value-added products and services to their customers.

Every day, Webroot employees talk to computer users in the U.S. and Europe who are being negatively impacted by spyware that has found its way onto their computers. Given this expertise, Webroot provides the following answers to the questions included in the FTC's Federal Register notice.

Defining and Understanding Spyware

What types of software (particularly downloaded software) should be considered "spyware"? How is adware different from spyware?

In 2003, Webroot helped to found the Consortium of Anti-Spyware Technology vendors (COAST), a non-profit organization established to facilitate collaboration among spyware detectors and increase awareness of the growing spyware problem.

COAST defines spyware as: Any software program that aids in gathering information about a person or organization without their knowledge, and can relay this information back to an unauthorized third party.

“Without your knowledge” and “to an unauthorized third party” are key components of this definition. The workshop was very appropriately titled: “Computer Monitoring Software on Your PC: Spyware, Adware, and Other Software.” From a pure technology point of view, there is little difference between computer monitoring programs that serve legitimate purposes and those that put your privacy and personal information at serious risk. For example, a keylogger program like ChildSafe, a Webroot product, provides parents with the ability to monitor their childrens’ online activities by tracking what the child types on the keyboard or views on the screen. A functionally similar keylogger program installed without permission by JuJu Jioang on computers in at least 15 Kinko’s stores provided him with personal information about over 400 people, which he used to open back accounts and commit other illegal activities.

Thus, there is not a technological definition for spyware. The definition is contextual – how the program came to reside on your computer is a threshold question to defining it as spyware. Under this definition, there are several kinds of programs that can be considered spyware.

The four most common forms of spyware are:

- Back Door Trojans -- malicious programs that appear as harmless or desirable programs. Back Door Trojans deploy remote access tools, allowing hackers to gain unrestricted access to a user’s computer. Trojans can be deployed as email attachments, or bundled with another software program.
- Keyloggers -- programs that can monitor and record the user’s every keystroke. Keyloggers can be used to gather sensitive data such as username and password, private communications, credit card numbers, etc.
- System Monitors -- applications designed to monitor computer activity. These programs can capture everything that is done on a computer. Information can be received by a third-party, through remote access, or scheduled emails.
- Adware -- advertising supported software that displays some form of advertisements whenever the program is running. Once installed, these programs can download and install new software and data files – advertisements, etc. – based on user activities such as websites visited. An adware program should be considered spyware when it was installed without informed consent and sends information to unauthorized parties.

<u>Distribution of Spyware</u>

How is spyware distributed? What role does peer-to-peer file-sharing play in the distribution of spyware?

Spyware may arrive bundled with freeware or shareware, through peer-to-peer downloads, attached to or embedded in email or instant messenger communications, as an ActiveX installation, or it may be placed on your computer accidentally or deliberately by someone with access to it. Peer-to-peer file sharing is another way that spyware can be distributed; however, like the other distribution means (email and web-browsing) peer-to-peer file sharing has many other legitimate uses beyond distributing spyware. The many ways that spyware can be distributed, contribute to the dramatic rise in spyware over recent years.

EarthLink and Webroot Software collaborated in the first quarter of 2004 to offer a free SpyAudit. On April 15, 2004 the companies jointly released the findings for January 1, 2004 through March 31, 2004. During that timeframe, 1,062,756 spyware scans were run, identifying a total of 29,540,618 instances of spyware, meaning roughly 28 instances of spyware per PC. Of particular concern, were the large number of System Monitors and Trojans found which accounted for 369,478 of all the spyware instances found.

To what extent is spyware bundled with other software, especially freeware? Do consumers know that spyware is being placed on their personal computers?

Bundling spyware with freeware is one way that spyware distributors are able to legitimize the download. Some argue that spyware is installed with the user's knowledge (although often the user may not understand exactly what s/he has done). Most of the time it is installed surreptitiously as part of another program installation. Even if the bundling of software and information tracking practices are disclosed to the consumer through the End User License Agreement (EULA), such disclosures are rarely clear and conspicuous. Even when they exist, notices often fail to provide users with a real understanding of what information will be collected, who is collecting it and how they plan to use the information collected.

How does spyware operate once it has been placed on a personal computer?

Because spyware comes in many different forms, there are numerous ways it can behave once installed on a computer. A few of the more egregious behaviors are:

> Home Page Hijacking – a user's homepage is continually reset without their permission. If the user attempts to change their homepage back, the spyware will simply hijack it again.
>
> Search Page Hijacking – Internet Explorer uses internal search methods that can be hijacked, redirecting a user's searches to paid advertising results pages.
>
> Host File Hijacking – Websites can be redirected to hijacked sites (for instance a user will type www.google.com and instead be taken to a completely different site). Sometimes host file hijack sites are designed to look like the authentic site, but are populated with paid advertising information.
>
> Re-Infection of the above – If spyware is removed and the spyware has added a run key to the users system, the computer is reinfected when the user reboots the system.

Does spyware affect the functioning of personal computers?

In many cases, spyware can have a serious negative affect on system performance of your PC. Any program on your system is already using system resources, bandwidth and memory. So a spyware program that is on your system without your consent may be using more than you knew about and intended to use. Some programs may also have thread jumpers that reprioritize the current running processesin an attempt to have their program running at a stronger, more stable thread.

The Effects of Spyware

Does spyware interfere with use of the Internet or programs on personal computers? If so, how?

If a hijacker is present on a system, a user will not be able to run proper search queries. The user will not be able to modify their personal computers Internet Explorer settings without removing of the infection.

Spyware can block access to websites by interfering with normal browser functionality.

Certain types of adware with present undesired advertising in the form of pop ups. These programs present new targets for the spread of viruses, in the same way that other network-enabled applications may be exploited by hackers.

Some forms of spyware programs install a hidden dialer, which leaves an open portal for a remote access controller to make telephone calls to unwanted 900 numbers.

Does spyware raise privacy concerns for consumers?

Spyware raises serious concerns about consumers' privacy. Even in its more benign forms, it can collect and share information about your browsing and on-line searching habits that you would prefer to keep private. In its more insidious forms, spyware can be used to aid identity and intellectual property thieves.

Does spyware collect personal information about consumers?

As included in the spyware definition we provided, spyware relays information "back to an unauthorized third party." What information has been collected, who it is being sent to, and for what purpose, is unknown to the user.

How is the personal information spyware collects used? Is it combined with data from other sources? Is it transferred or disclosed to third-parties?

How personal information is used varies widely from program to program. It can be used to track a consumer's buying or surfing habits, or in a more malicious form, can be used to capture personally identifiable information in order to steal a consumer's identity, or access their bank account or credit card account. Data collected by spyware can be combined with data from other sources, and spyware does transfer or disclose information to third parties.

Does spyware capture the key strokes of consumers? Is key stroke information combined with data from other sources? Is it transferred or disclosed to third parties? To what extent is spyware used for identity theft?

Key loggers are one kind of spyware what can capture the key strokes of consumers without their knowledge. The data collected can by combine with other collected data, and transferred to unknown third parties.   These programs can be used to facilitate identity theft, as was the case in 15 Kinko's stores. In that case, the perpetrator was caught and tried.

Does spyware raise security concerns for consumers?

Given the ways that spyware can be used to invade your privacy and facilitate identity theft, it raises some serious security concerns for consumers.

Does spyware expose personal computers to increased risk from hackers? If so, how?

Yes. According to Jim Rapoza, in his Dec. 1, 2003 Eweek article. "Spyware Needs to Go," "the main function of Adware and spyware is to take information from a system and send it to an external source. For legitimate programs that do this, such as Web servers, standard security practice is to lock them down as much as possible and keep their patches up-to-date. But how can you secure and patch a program that you don't even know is on your system? Spyware programs are a ripe target for crackers and malicious coders looking for holes into systems."

Spyware can open new hacker exploits into the end user's computer. For example, a user is running an Adware program. This program may have a port open on the system that is listening. A hacker could use a buffer overflow attack or another known exploit and gain access to a computer through the previously installed adware program.

Is there special or unique consumer privacy or security risks associated with spyware disseminated through peer-to-peer file-sharing software? If so, what are these risks?

The difference is those end users think they are downloading a certain program for use and do not know they are downloading these malicious programs to their systems.

To what extent are the privacy, security, and other concerns spyware raises for consumers different from those associated with other types of software?

Right now a difference between spyware and other types of software is that many consumers and businesses are still not aware of the risks that spyware presents. Many computer users are finding they do not have the right tools to fight spyware on their system. Anti-virus software does not offer protection from spyware because spyware is not viral. Since it can attach itself to legitimate downloads, spyware can often pass unchallenged through firewalls. Some forms of spyware intertwine themselves with files essential to system operation or with desirable applications, so it cannot be safely removed by simply deleting files with a system-cleaning tool.

Does spyware create security risks for or cause harm to businesses, including harm to the reputation of software companies and others in the high-technology industries?

Just as spyware poses serious risks for consumers, it also poses a serious threat to companies' intellectual property and other assets.

Does spyware benefit consumers or competition? If so, what are the nature and extent of these benefits?

While there are computer-monitoring programs that have positive benefits for consumers and competition, by our definition of spyware, there is not a consumer or competition benefit to spyware. Consumers and businesses should retain control over what computer programs come to reside on their PCs.

Possible Responses to Spyware Concerns

What can consumers do to prevent the harms related to spyware? What can consumers do to avoid downloading unwanted spyware?

It is always important that consumers take time to be educated about the technology they use in their home. With the advent of the Internet, your network connection can be an open window to the world. Consumers should take proper precautions:

- Firewalls, anti-virus, anti-spyware programs need to be installed and regularly updated.
- Spend time to read End User License Agreements (EULAs) before installing anything on your computers.
- Make sure your browser settings are set at a higher level of security.
- Delete email from unknown sources without opening it.
- Turn off the preview pane to delete messages without opening them.
- Keep current by reading industry trade magazines and visiting web sites, like the FTC's, that provide consumer protection information.

What can parents do to minimize the risk that their children will download spyware, especially spyware disseminated via peer-to-peer file-sharing software?

It is especially important for parents with children on-line to invest time in educating themselves about the risks involved. It is important that parents speak with children about spyware and other vulnerabilities that come from the network connection

Can consumers detect and remove installed spyware? If so, how difficult is it to do so?

Many computer users are finding they do not have the right tools to fight spyware on their system. Anti-virus software does not offer protection from spyware because spyware is not viral. Since it can attach itself to legitimate downloads, spyware can often pass unchallenged through firewalls. Some forms of spyware intertwine themselves with files essential to system operation or with desirable applications, so it cannot be safely removed by simply deleting files with a system-cleaning tool.

Programs like Webroot's Spy Sweeper, winner of PC Magazine's 2004 Editors' Choice award, provide an effective, easy-to-use means of fighting spyware. The magazine's objective review of 14 spyware detection products found: "Spy Sweeper is the most effective standalone tool for detecting, removing and blocking spyware."

Can consumers detect and remove peer-to-peer file-sharing software? If so, how difficult is it to do?

Peer-to-peer file-sharing programs typically function as any other program would, either coming with their own un-installation program or with the ability to be removed through the standard Window's Add/Remove Programs function.

What can government do to prevent the harms related to spyware?

Webroot is on the front lines fighting spyware, but Congress and the Federal Trade Commission (FTC) have critical roles to play on this issue to increase public awareness, develop and reinforce clear rules, and actively enforce the law.

C*an law enforcement action reduce the harms related to spyware? If so, how, to what extent, and by whom? What should be the focus of these law enforcement efforts?*

Many spyware scenarios likely fall under current theft and anti-fraud statutes. Active enforcement against the most blatant abuses of the technology to aid in crimes will help to send a message that these laws to apply equally in the Internet context as they do when a phone or personal contact is used.

Can government-sponsored consumer education play a role in addressing spyware?

Government could play a particularly strong role in consumer education about spyware. Increased talk about the problem by elected officials would raise awareness and educated consumers will at least help to lower some of the risks.

Is there a special need for the government to educate teenagers and their parents about the risks of spyware, especially spyware disseminated through peer-to-peer file-sharing software?

Educational programs supported by the Department of Education or other governmental organizations to provide teenagers and their parents with more information about spyware and other risks associated with Internet use would be very valuable. Webroot would welcome an opportunity to help with any such programs.

What can government do to assist industry in addressing the harms caused by spyware?

In spite of great technology, companies like Webroot cannot fight this battle alone. Clear definitions about the kind of notice and consent that software distributors should provide to and receive from consumers are essential. Ensuring that law enforcement organizations have sufficient resources to pursue these kinds of cases is also essential.

What can industry do to prevent the harms related to spyware?

Industry has a critical role to play in educating consumers about spyware. Leading legitimate companies can work together to help establish the rules that all companies should abide by when offering software to consumers.

Can technological tools reduce consumer concerns about spyware? If so, how and to what extent?

Certainly technological tools can reduce a consumer concerns about spyware. Tools like Spy Sweeper help consumers stay in control of their computer environment. The challenge is that there is significant economic incentive on the side of the spyware producers, and so this becomes a technological arms race.

Can industry-sponsored efforts to educate consumers and employees help to reduce the harms related to spyware?

Greater consumer and employee awareness would likely help to slow the rate at which spyware is proliferating.

Can high-tech industry partner with the government to address spyware?

We would certainly hope that the high-tech industry and government will partner to address spyware, and we look forward to being a part of that effort.

How can businesses work effectively with each other to address spyware?

The Consortium of Anti-Spyware Technology vendors, the Consumer Software Working Group and other efforts by businesses to work together can increase consumer education, help to identify the elements of a certification program, and highlight industry best practices. The Government's involvement provides an incentive for businesses to work on these things.

What would be the effect on the market for software if spyware were eliminated or reduced?

Unless spyware was 100% eliminated then companied providing "Free" software that is currently bundled with spyware would need to find a new model to maintain financial viability. Or discontinue their services.

Would the elimination or reduction of spyware affect the price of software that is currently bundled with spyware?

Software manufacturers that bundle their software with spyware today and would not be able to be bundled their software with spyware tomorrow, may have to charge for their software programs.

Would the elimination or reduction of spyware affect the free distribution of peer-to-peer file-sharing software?

They may have to find a new business model to keep the software free or peer-to-peer sharing network may migrate to an open source community.

Webroot Contacts:

Christine Stevenson
Christine Owens