BillP Studios

32 Sunnyside Rd.
Scotia, NY 12302
518.372.3990
Spyware@BillP.com

Home of WinPatrol
http://www.WinPatrol.com

To: SpywareWorkshop2004
Subject: Spyware Workshop Comments
Date: April 14th, 2004

Introduction

As someone developing software products in the PC industry for over 20 years I've seen many changes. I've worked at Gateway Inc, Microsoft Inc. Capital Cities/ABC/Disney, Epson America and many other companies pioneering new, innovative ways for the consumer to benefit from their personal computer.

In the late 1980's while managing software development at the service now known as America Online, I never imagined the scale of either the benefits or the dangers to individuals in a connected world. Our goal then was to permit anyone, any age, regardless of their expertise, access to a wide variety of online content. At the time, as a closed system our members could be protected.

America Online and the Internet are no longer closed and an even larger consumer market with very little experience now has access to a connected world. This large market has been ripe pickings for less than ethical individuals looking to make big bucks off the ignorance of others. The newest Internet boom may be fueled by investments in companies whose concern for consumers is less than admirable.

In this document, I'll help the reader distinguish between acceptable software behavior and methodology, as opposed to tricks used to intentionally mislead and take advantage of the consumer. I hope to get past the insignificant use of terminology and specifically define the behavior that is undesirable and intrusive to the public. I will also suggest changes to currently proposed legislation so that it's capable of preventing objectionable software from making future court challenges.

Terminology

There has been considerable debate over the definitions and differences between *Adware* and *Spyware*. Lately, *Spyware* has become a popular term for any program which has been installed on a computer without the user's knowledge or understanding and is often difficult to remove. However, many Adware creators say the term should only be used to describe programs like 'key loggers', which are used by parents or spouses to monitor computer activities or programs created by hackers to collect user ID's and passwords. The common ground appears to be that any program which tracks a consumers actions including web navigation or purchase habits are spying as well.

I sincerely hope this single debate does not monopolize the upcoming Spyware Workshop. There is little value in the FTC defining terminology when important consumer protections need to be addressed. It really doesn't matter if it's called Spyware, Adware, Malware or "Mysteryware". In the end, consumers will continue to use the term they want. The focus of the FTC would be better spent addressing and defining the behavior and characteristics of these programs.

At best, these insidious programs frustrate and confuse users, misdirecting them away from their intended web destination. At worst, they incorrectly reconfigure network connections, destroy files or slow computer speed to a crawl. The loss in productivity can not be measured and very often, our customers usually refer to this type of software in terminology that isn't appropriate to print.

Behavior

Last year's focus was on curbing the annoyance of 'spam.' This year, a more serious issue is exploding and we have observed three program behaviors that have become excessive and harmful to consumers:

1) **Programs installed in a deceptive manner.**
   Consumers are often mislead into clicking 'Yes' and agreeing to install software which is neither required nor wanted. Some sites require a download confirmation before users are allowed to continue. Often, some legitimate downloads are accompanied by 'hidden' software intended for an entirely unrelated purpose.

   Companies claim that the "user makes a conscious decision to download our software." While it is true that the user did press the 'Yes' button, they rarely know or understand the full extent of their action. The secrets are hidden within a lengthy EULA (End-User License Agreement), which between the legal language and size of the document, are rarely viewed or understood.

2) **"Always-on" Programs installed to Autostart.**

Most consumers have limited memory and CPU usage, yet many programs are auto configured in such a way that they will run at all times. These programs are not launched when the consumer needs them. Instead, they are positioned in such a way so as to automatically launch every time the computer restarts. With some of these programs, consumers are not given the option (during installation) to decide if they want it added to the list of applications that always run, and remain running, until the computer is shut down.

This also applies to application parasites that are loaded as 'helpers' for applications such as the Internet Explorer browser. Many programs allow for 3rd party companies to create Plug-Ins or Skins but many times these add-ons are installed without notifying the user of their use.

3) **Programs that cannot be removed.**

Anyone with enough knowledge to create a program for Microsoft® Windows will also be aware of Microsoft's recommendations for making the removal of a program necessary. Microsoft has even made additional interfaces available to make Install and Uninstall an easy process for programmers to implement.

Many of the programs our customers struggle with have been purposely created to prevent removal. Frequently, these programs come in pairs and one will automatically reinstall or restart its partner program as soon as it detects the other is missing.

Resolve

The proposed SPYBLOCK Act S.2145 is an important step in being able to prosecute companies and individuals who exploit consumers and take control over their property. The FTC should make sure that this law and any other means of enforcement does not allow companies to walk a fine line between legal and illegal based on flawed semantics or terminology used when creating public policy.

Affirmative consent is defined in S.2145 as "*consent expressed through action by the user of a computer other than default action specified by the installation sequence and independent from any other consent solicited from the user during the installation process.*" In the real world a user may give what is defined as "affirmative consent" yet has no understanding of the impact and implications of their consent. This definition needs to be expanded to reflect that the user "understands within reason" what they are agreeing to and is providing "**informed** affirmative consent". The public should not be forced or expected to read through multiple pages of legal commentary.

Most computer users understand the concept of "running" or "launching" computer software known as a "program". Typically, they launch a requested program or a program automatically loads when a document is requested. When they have completed their activities they close the document or exit the program. Far too often, when installing

new programs users are not made aware that portions of the program will be installed to automatically start and remain in an “always ready” state. When portions of programs are started automatically at boot time it reduces the computing power and resources available to the user. This activity has become so common an entire software category has evolved to help users deal with this predicament. This behavior is most common among spyware and other malicious programs yet is not addressed in any way by SPYBLOCK Act S.2145.

The Windows Control Panel Applet, Add/Remove programs has become well known by computer users. It’s an industry standard for the Windows market but has never been a requirement. While I would hope that any legitimate company would implement this feature I would also recommend the FTC insist that programs can be removed by users using other methods without a struggle.

It should be possible for a user to end a program using the Windows Task Manager without a secondary partner task or program reactivating it. It should be possible for a user to change the Auto Start option without a program rewriting the change. Any program that exhibits this resistance for removal should be suspect. While S.2145 addresses the need for an Uninstall program it does not provide a remedy for programs that refuse to cease operation on request or use methods to resist removal.

In Closing

Our company, BillP Studios provides a free program called WinPatrol which helps users gain back control of their own machines. This program has been available since 1997 and its existence is spread mostly by word of mouth. Few company resources were ever devoted to maintaining or supporting WinPatrol. In the past year, the influx of Spyware has grown so much that we’re now known more for our WinPatrol product than anything else.

We have created a PLUS version of our software which helps to fund support and continued development. WinPatrol PLUS includes information to help educate users to what programs are running on their machines. Our goal was never to be the business of Spyware prevention. The response from our customers make it clear that we’ll continue in this business sector for some time. We actually have plenty of other things to do if the FTC can put an end to the need for programs like Ad-aware, Spybot and WinPatrol.

I don’t care if you call it Adware, Spyware or Mysteryware. You must implement a way to find and prosecute the benefactors of programs that infiltrate computers just because consumers are not experts in computer security.

Sincerely,
Bill Pytlovany