Taughannock Networks

FTC Spyware Workshop
March 2004

WRITTEN COMMENTS OF DR. JOHN R. LEVINE

It is my honor and privilege to submit these comments to the Federal Trade Commision for their public workshop, entitled *Monitoring Software on Your PC: Spyware, Adware, and Other Software*. These comments are substantially identical to comments submitted to the Subcommittee on Communications of the Senate Committee on Commerce, Science, and Transportation for consideration during their hearing on S.2145, the SPY BLOCK Act, on March 23, 2004 at which I have been invited to testify.

I am a consultant and author specializing in consumer-oriented Internet topics. I am the primary author of *The Internet for Dummies*, the world's best selling book on the Internet, which has sold over seven million copies in nine editions in over two dozen languages since 1993. I am also the co-author of numerous other books including the recent *Internet Privacy for Dummies* (2002) and *Fighting Spam for Dummies* (2004). In these books, my co-authors and I educate readers regarding online marketing and advertising practices that threaten the privacy of their personal information and/or present the risk of unauthorized collection, use, and abuse, of information about their online activities.

I co-chair the Anti-Spam Research Group (ASRG) of the Internet Research Task Force under the oversight of the Internet Activities Board of the Internet Society. The ASRG is a coordinating forum to coordinate research into and development of technical measures to deal with unwanted e-mail, with broad participation of industry, academia, and independent researchers. I serve on the board of the Coalition Against Unsolicited Commercial E-mail (CAUCE), the leading grass roots anti-spam advocacy organization.

I have spoken at many professional, trade, and government fora such as the 2003 Federal Trade Commission Spam Forum and the upcoming *Enterprise Messaging Decisions* conference in Chicago, May 4-6, 2004, and the *E-mail Technology Conference* in San Francisco, June 16-18, 2004.

I serve on advisory boards related to consumer Internet issues at companies ranging from Orbitz, one of the big three on-line travel agencies based in Chicago, to Habeas, a small anti-spam certification startup in Palo Alto CA.

What is Spyware?

Spyware is a general term used to describe software that runs on consumers' personal computers and performs actions that the consumer considers undesirable or hostile. The term has been applied to a wide variety of different applications, ranging from the arguably legitimate to the egregiously fraudulent. The three most common types of spyware are the following.

- *Adware* monitors the pages fetched by a user's Web browser or other material on the consumer's computer and when it sees particular pages or terms, displays other pages containing advertisements paid for by the spyware's sponsors. So called "Browser Helper Objects" install themselves as part of the Internet Explorer web browser and change the way it works. The changes can be as simple as switching to a different home page, or as complex as redirecting web searches to the spyware vendor's search system rather than the consumer's desired system, or adding new "click here" buttons that lead to sponsors' advertisements.

  In some cases, the adware rewrites the web pages displayed by the browser, substituting ads from adware vendor for the ads originally in the page. This technique has been likened to opening newspaper boxes and pasting one's own ads on top of the ads in the papers.

- *Key loggers* record every key pressed by the computer's user and send the stream of keystrokes back to the spyware's author. More generally, "Activity Monitors" can log and report on any type of consumers' computer usage, such as e-mail send and received, web pages visited, and instant messages exchanged. The data can be used for anything from consumer preference statistics to identity theft.

- *Trojan Horses* allow the spyware author or vendor to remotely control the consumer's computer for the author's purposes. At the point, the most common purpose is probably to send spam.

  Although these are the most common current varieties of spyware, variations on these themes and new and different spyware programs are released frequently. We can expect different varieties of spyware to appear in the future.

How Is Spyware Installed on Consumers' PCs?

Spyware distribution is made possible by a combination of the weak security of Microsoft Windows and the inability of consumers to understand the many security-related warnings that their computers currently present to them.

MS Windows generally makes it very easy to install software remotely onto a consumer's PC. While this facility is useful in a corporate environment where an IT department manages computers all over the

company, hostile parties can also use it to install spyware without the consumer understanding what's happening. In some cases, whenever a consumer visits a spyware vendor's web page, programming in the web page automatically installs the spyware. In other cases the spyware is installed as part of a program that performs a desirable function unrelated to the spyware features.

Sometimes, the consumer is presented with a warning screen asking whether to install the new program. The warning screen is nearly identical to the warning screens that appear when a web page needs a benign application such as one to display "flash" animations. Consumers see such warnings so often, and have so little information with which to evaluate any particular installation request, that they rarely reject an installation request. In many other cases, security weaknesses in Windows make it possible to install spyware without the consumer's knowledge or consent.

Some computer manufacturers are now shipping PCs with spyware pre-installed. This means that users will have to go to extra time and expense to remove the spyware from their new computers to bring it to a normal usable state.

Is All Software that Communicates with Remote Computers Spyware?

No. In some cases, consumers deliberately install software with remote communication features to participate in a large-scale computing project or a multi-player game or other activity. For example, many of my computers run a program from the volunteer-run distributed.net that solves large mathematical and cryptographic problems. Another well-known project called Seti@Home, coordinated at the University of California at Berkeley, uses consumers' computers to analyze data from radio telescopes, looking for evidence of intelligent signals from outer space. In both of these cases, the consumer runs the program because he or she actively wants to participate in the projects, the programs make no changes to the computer's configuration (other than an optional screen saver with Seti@Home) and the programs return no data about the consumer other than an optional e-mail address or "handle" if he or she wants to be counted in the statistics that the projects publish.

Another common situation is straightforward advertisement supported software. For example, the popular Eudora e-mail program and Opera web browser are distributed in free versions that display small advertisements in clearly labelled windows within the application. The ads do not interfere with the normal operation of the program. The consumer is clearly informed that if he or she purchases a paid registration for the program, the ads will go away.

Any legislation related to spyware should be crafted so as not to interfere with legitimate applications such as these.

How Do Consumers Feel about Spyware?

They hate it. Although spyware has never been my primary area of activity, in my role as online postmaster for CAUCE, I get mail almost daily from consumers complaining about spyware and asking what they can do about it. On the *Internet Privacy for Dummies* web site at http://www.privacyfordummies.com, a page about dealing with spyware is the most frequently visited on the entire site.

A small anti-spyware industry has arisen with programs like Adaware, from http://www.lavasoftusa.com, and Spybot Search and Destroy, from http://www.safer-networking.org, that detect and remove spyware from consumers' computers. Companies now routinely recommend that their employees install and use one of these programs on a regular basis to clean off any spyware that may have installed itself.

Spyware is frequently written so as to be difficult or impossible to remove from consumers' computers. It rarely comes with an uninstall program, as is standard with other PC software, or it comes with an uninstaller that doesn't actually remove the spyware. Some of the more egregious spyware attempts to delete anti-spyware programs such as Adaware and Spybot from computers, and to reconfigure web browsers to make it impossible to reach anti-spyware web sites or to install anti-spyware software from those sites.

Consumers clearly perceive spyware as an illegitimate use of their computers, and spyware is rarely if ever installed with the informed consent of the computer's owner.

What Policy Problems Does Spyware Present?

Spyware presents two separate policy issues, consumer protection and privacy.

The consumer protection issue is that consumers don't provide consent when spyware is installed on their computers, they don't understand what the spyware on their computer is doing, and when they become aware of its presence, they invariably want to get rid of it. In principle, this issue could be addressed by better disclosure at the time the spyware is downloaded, installed, or activated. But in practice, I am skeptical that disclosure would be effective. The behavior of spyware is often quite complex, and a disclosure of that behavior equally complex, to the point that many consumers would see the disclosure but wouldn't understand its implications and would be unable to make an informed decision whether to accept it or not.

Furthermore, adware that shows its own advertisements in connection with web pages that a computer's user has requested causes severe consumer confusion. The consumer cannot easily tell what ads are part of the web page, and what ads may have been added or replaced by the spyware. Consumers incorrectly assume that advertisements are provided or endorsed by the author of the web page, rather than by the spyware vendor. If the advertisements are inappropriate or offensive, the consumer blames the web page author, rather than the spyware vendor that actually provided the advertisements. In some cases, the advertisements inserted by adware are for sexually oriented materials, although the spyware vendor has no way of knowing the age of the computer's user.

I am aware of at least one group of lawsuits filed by mainstream advertisers against Claria, formerly Gator, a vendor of adware that is typically installed with peer-to-peer applications such as Kazaa, due to its advertisement insertion practices.

The privacy issue is that spyware often collects personal information about the users of computers on which it is installed. This is an issue for any computer user, and is doubly so for users under the age of 13 who can't consent to collection of information about themselves.

One could argue that in principle this problem could also be addressed by better disclosure, but I believe there are public policy reasons that it's not a good idea to let people sell their privacy rights. The law has long forbidden certain kinds of consumer transactions (selling parts of one's own body, for example) as contrary to the public interest, even if the consumer wishes to enter into such a transaction voluntarily and with full notice. I believe that there are sound reasons to treat the sale of one's privacy as contrary to public policy. The value of one's privacy is great, and the amounts offered in exchange for it are rarely large. Once one's privacy is traded away, it is difficult or impossible to regain, and the implications of giving it up are frequently far greater than what a consumer would foresee.

Since spyware can and often does collect information about all of a computer user's activities on the computer, and software cannot tell private from non-private information on a computer, the opportunities for abuse are vast. For example, consumers often apply for mortgages, bank accounts, brokerage accounts, and other financial accounts online. If spyware sends the information from one of these applications back to the spyware vendor, the vendor has everything necessary to commit identity theft. Consumers often use e-mail or instant messages to communicate privately with friends and relatives, or with trusted personal advisors such as lawyers, accountants, and doctors. If spyware collects the contents of those messages, which is technically easy to do, the possibilities for abuse range from medical fraud ("our apricot seeds will cure your cancer better than old fashioned chemother-

apy'') to blackmail.

Many consumers underestimate the damage from privacy invasions on the assumption that if they conduct their lives in a legal and ethical fashion, they have nothing to hide. The reality is that some areas of everyone's life are private, and the damage from invading those private areas is real, substantial, and very difficult to cure.

Comments on S.2145

The United States Senate is considering a bill, the SPY BLOCK Act, S.2145, that would regulate spyware.

S.2145 as currently written is a well-crafted attempt to deal with spyware problems by mandating disclosure and minimal good software practices. I have two reservations about the bill in its current form.

The first is that I am not confident that disclosure is the most effective way to deal with spyware problems. In view of the universal distaste of consumers for spyware, and their invariable desire to get rid of it when they find it installed on their computers, it would make far more sense to ban spyware outright, or to provide a simple way, analogous to the telemarketer do-not-call system, that a consumer could provide one-time permanent notice that spyware is unwelcome on his or her computer, rather than having to wade through notices and disclosures every time a spyware vendor wants to sneak something onto the consumer's PC.

My other concern is for enforcement. The current draft leaves enforcement primarily to the FTC and to state Attorneys General without providing any new funding for enforcement. In view of the large number of spyware authors and vendors, and the budget pressures on all enforcement agencies, it seems unlikely that they will be able to take action against any but the largest violators. One of the reasons that the existing do-not-call system is so effective against telemarketers is that the law specifies statutory damages for consumers who are the victims of illegal telemarketing calls, and allows consumers who are sufficiently motivated to sue for modest but meaningful amounts. A similar provision to let consumers recover for spyware violations would make an anti-spyware law far more effective without requiring new funding for the FTC or other agencies.

I thank Ray Everett-Church, Esq., for his assistance in preparing these remarks.

Revision date: 2004/03/19 21:18:23