From: Marty Lafferty
Posted At: Friday, March 19, 2004 4:03 PM
Posted To: spywareworkshop2004
Conversation: Spyware Workshop - Comment, P044509
Subject: Spyware Workshop - Comment, P044509

FEDERAL TRADE COMMISSION (FTC)

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

DISTRIBUTING COMPUTING INDUSTRY ASSOCIATION (DCIA)

www.dcia.info <**http://www.dcia.info/**>

Comments

A. Defining and Understanding Spyware

1. What types of software (particularly downloaded software) should be considered “spyware”?

The DCIA broadly defines “spyware” as software installed without consent that provides no benefit and, more specifically, as a pejorative term to describe software that installs itself on consumers’ personal computers without their knowledge or consent and does one or more of the following: gathers personal data about users and/or tracks their usage behavior without consent, supplies this information to undisclosed third parties for undeclared purposes, utilizes processing capabilities for unknown tasks without permission, and makes itself difficult to uninstall. The DCIA opposes “spyware.”

2. How is adware different from spyware?

The DCIA broadly defines “adware” as software installed with consent that provides a benefit and, more specifically, to describe beneficial software that enables installation and usage of valuable computer programs by consumers at no cost or at a reduced cost in exchange for receipt of online advertising. It clearly communicates its value proposition before installation and during operation, fully discloses and clearly explains its functionality, requires positive affirmation of permission before being installed, respects end-user privacy while serving ads (which may be targeted by online computer activity patterns but gather and transmit no personally identifiable information), provides easily understandable explanations of what it is doing, and is not difficult to uninstall. The DCIA supports “adware.”

B. Distribution of Spyware

1. How is spyware distributed?

Spyware can be distributed mechanically by means of disk(s) or downloaded from online networks including the Internet much as any other type of software program. By definition, its installation is accomplished, however, without the informed consent of the end-user.

2. What role does peer-to-peer file-sharing play in the distribution of spyware?

DCIA Members who are peer-to-peer (P2P) file-sharing software suppliers agree not to distribute spyware. It is possible for non-member P2P software as well as e-mail and instant-messaging applications, chat-rooms, search-engines, and even web-sites to distribute spyware, either by the suppliers themselves or by abusers of such software or sites who may disguise spyware as some other type(s) of file(s) or cloak it entirely.

3. To what extent is spyware bundled with other software, especially freeware?

It would be a rules violation for a DCIA Member to bundle spyware with any type of software, and we are not aware of any such practice by Members. On the Internet overall, however, this practice should be of concern to all responsible parties. While we are not aware of quantitative data, anecdotal evidence indicates the general incidence of spyware downloads is significant.

4. Do consumers know that spyware is being placed on their personal computers?

Under our definition, spyware is either installed without the knowledge of the user, or may be installed with knowledge of the user, if its real character and purpose are not fairly disclosed.

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

According to our understanding, spyware typically operates in conjunction with other software programs, but hides or disguises its operation from the end user, often running in the background while other tasks are performed. Its uses range from gathering personal information about users to tracking their keystrokes, and from transmitting such data to undeclared entities to utilizing personal computer processing capabilities for undisclosed activities.

C. The Effects of Spyware

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

Spyware affects the functioning of personal computers. It can interfere with their use of the Internet and operation of other programs, sometimes adversely affecting computer performance. Spyware does this by running in conjunction with and taking control of certain other software programs running on the personal computers on which it is installed, and may thus consume enough processor capacity to degrade performance noticeably. It may also cause computers to “hang” or otherwise disrupt operations either through interoperability problems with other functions and applications, or simply through poor code design.

2. Does spyware raise privacy concerns for consumers?

Yes, spyware raises privacy concerns for consumers.

a. Does spyware collect personal information about consumers?

Yes, we believe certain spyware programs collect personal information about consumers.

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

According to our understanding, the personal information spyware collects can be used for a variety of purposes, ranging from relatively unharmful purposes such as individualized marketing to very serious violations of consumer privacy including identity theft. It can be combined with data from other sources such as marketing lists or information obtained offline by private detectives. It can be transferred automatically by uploading over the Internet or stored on the personal computer to be mechanically retrieved by the party responsible for installing it.

c. Does spyware capture the keystrokes of consumers? Is keystroke information combined with data from other sources? Is it transferred or disclosed to third parties?

Certain types of spyware capture the keystrokes of consumers. This information can be combined with data from other sources and transferred or disclosed to third parties.

d. To what extent is spyware used for identity theft?

We have no data on the extent to which spyware is used for different purposes. This information may be known by law enforcement officials, or may be obtainable by conducting specialized research.

3. Does spyware raise security concerns for consumers? Does spyware expose personal computers to increased risk from hackers? If so, how?

Yes, spyware raises security concerns for consumers. We are informed that certain types of spyware expose personal computers to increased risk from hackers by creating backdoors and other insecure means to access data from and/or gain control of the operation of such personal computers.

a. Are 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?

First, as a trade association whose mission includes supporting the commercial development of peer-to-peer technologies, the DCIA must emphatically state that peer-to-peer (P2P) file-sharing software and spyware have no particular interrelationship. We appreciate the FTC's need to explore the spyware phenomenon – it is of concern to us as well. But there are no special or unique privacy or security risks associated with spyware disseminated through peer-to-peer file-sharing software. The means of dissemination of spyware has no direct correlation with its privacy or security risks. These are an independent function of each spyware program's design and operational parameters. In any event, consumer-use anti-spyware software is currently available on both a paid basis, and free via download from popular Internet shareware sites.

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

The privacy, security and other concerns spyware raises for consumers are different from those associated with other types of software because of spyware's attributes of being invisible at installation and during operation, because it may have malevolent purposes, and because it makes itself difficult to uninstall.

5. 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?

Spyware creates security risks for and can cause harm to businesses, in terms of violating their confidential data and abusing their computer processing capabilities, just as it can for the personal information and functioning of an individual's personal computer. In addition, the existence of spyware is a negative for the software and high technology industries in general, including the distributed computing industry, and we oppose spyware.

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

The DCIA believes that spyware, other than that which may be used by duly authorized governmental authorities for national defense and law enforcement purposes, does not benefit consumers or competition. Spyware may provide a source of revenue for software suppliers who permit it to be bundled with their applications, but this benefit is far outweighed by the potential damage spyware can cause the public at large.

D. Possible Responses to Spyware Concerns

1. What can consumers do to prevent the harms related to spyware?

Consumers need to keep spyware from being installed on their personal computers, and if it is found to be installed, to uninstall it to prevent the harms related to spyware. There are reputable software programs that can be used to detect and prevent spyware from becoming installed and to uninstall it if it has been installed, but there are also disreputable programs claiming to perform these tasks that can be harmful as well. The conventional advice, "buyer beware," applies here. Professional tech support should be sought from trusted suppliers if consumers have any questions about spyware or anti-spyware issues.

2. What can consumers do to avoid downloading unwanted spyware?

Consumers need to be careful when downloading any software from the Internet. This includes reading carefully disclosure and explanatory materials associated with software before permitting its installation and verifying such information with qualified third parties. The challenge in avoiding spyware is that it may hide, fail to disclose, or disguise its presence before installation as well during operation. Anti-virus programs and anti-spyware programs can be helpful; again with the caveat that care must be taken with these to ensure that they are reliable and effective. Professional tech support from trusted service suppliers and knowledgeable IT staff members at one's place of employment can also be helpful.

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

Parents can minimize the risk that their children will download spyware by installing anti-spyware software and by communicating with them specifically about how to avoid spyware. Depending on the age and maturity of their children, parents may even want to monitor their children's online activity and personally

screen any software downloads. DCIA Members who distribute P2P applications pledge not to disseminate spyware with their software, and parents can easily confirm which such firms are Members by visiting **www.dcia.info** <**http://www.dcia.info/**> . Also, there are programs designed for parents that can be installed manually or downloaded from the Internet to help them track what their children are doing online. As previously noted, P2P software distributed by DCIA Members is warranted to be spyware-free and DCIA Members are encouraged to display the DCIA logo on their primary web site home page.

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

Consumers can detect and remove installed spyware, but spyware typically makes it difficult to do so, and therefore anti-spyware software and/or professional technical assistance may be required. Program files that have been installed in the computer's registry must be identified and deleted, and any "tickler" reinstallation programs must be detected and deactivated.

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

DCIA Members, including P2P software suppliers and adware suppliers, take pride in clearly, conspicuously, and completely communicating essential information to consumers before installation, during operation, and at uninstallation of their programs. Typically, the standard operating system application used to add or remove software in a personal computer (e.g. Windows' Add/Remove Software function) can be used to uninstall DCIA Member P2P software and adware programs, which are clearly labeled by name in the Add/Remove list and in the "Start" program list, just as any other reputable software program.

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

As with many issues related to rapidly evolving personal computer technologies and global connectivity via the Internet, gaining effective control over spyware sources or purveyors to prevent its harms would be difficult for any government. To the extent it can gain effective jurisdiction, the FTC can play a useful role in attacking spyware, perhaps through its unfair-or-misleading-trade-practices authority. However, as we have seen with spam, legislative and enforcement action targeting spyware may simply encourage spyware firms to locate abroad; to the extent they haven't already done so. Government can play a role in funding anti-spyware technology development and in sponsoring anti-spyware education, however, and the DCIA would encourage and support endeavors in both of these areas.

a. Can 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?

As noted in the answer to the preceding question, law enforcement activity can reduce the harms related to spyware by seeking to prosecute those responsible for its unauthorized development, distribution, and usage. The focus of these law enforcement efforts should be prioritized based on achieving the greatest benefit to the greatest number of citizens, taking into account the seriousness of harm that can be done by a particular spyware application and the relative scale of its dissemination.

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

Government-sponsored consumer education can play a role in addressing spyware. In many cases, teenagers may be more tech-savvy and already more aware of the risks of spyware than their parents, but in any case, a broad education program encompassing public schools, the personal computer industry, and the media generally could be of significant value and should be initiated. It would also be helpful, in the DCIA's view, if such education efforts clearly differentiated spyware from P2P software, and did not wrongly seek to equate or associate spyware with P2P software, but addressed spyware in the broader context of the many ways in which it can be installed on computers, including Internet surfing, online purchasing, email- and instant-message-mediated downloads, etc.

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

Government can assist industry in addressing the harms caused by spyware by bringing together major representatives of the private sector, including trade associations like the DCIA, to codify best practices to oppose the development and distribution of spyware and to warn consumers about its dangers. Government-sponsored consumer education, as previously noted, with carefully planned and clearly defined roles for industry can also be of value in this area.

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

Industry can help prevent the harms related to spyware by examining and implementing counter-measures at each step of the design, creation, dissemination, operation, and integration process of spyware with other technologies and businesses. Each sector of each affected industry can respond in ways that will be most effective in helping to prevent the further advancement or spread of spyware.

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

Technological tools can reduce consumer concerns about spyware. Anti-spyware detection and removal tools similar to anti-virus protection programs have been and can be developed and marketed with a similarly extensive impact.

6. Can industry best practices or self-regulation decrease consumer concerns about spyware? If so, how and to what extent?

Industry best practices and self-regulation can decrease consumer concerns about spyware. To have the greatest impact, consumer communications at key points in the purchasing and setting up of personal computers for use, the installation of computer programs, and the transmission of data could be examined for including safeguards and messaging to consumers regarding spyware and how to protect themselves from being affected by it.

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

Industry-sponsored efforts to educate consumers and employees can help reduce the harms related to spyware. Within each sector, specific studies can be undertaken to determine those instances where exposure or vulnerability to spyware is the greatest, and to develop appropriate communications through appropriate media to be provided in anticipation of these instances, in order to prevent spyware from being installed on their computers.

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

High-tech industry can partner with the government to address spyware. A jointly developed task force could be developed to analyze the specific areas where governmental and private sector actions could have the most impact, and make recommendations to their respective agencies and companies and trade associations.

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

Businesses can work effectively with each other to address spyware by means of government sanctioned activities, multiple company trade association initiatives, bilateral arrangements between companies, and individual actions.

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

The effect on the market for software if spyware were eliminated would be one of general improvement, because the market would be perceived to be safer and more secure, although this would be hard to quantify.

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

Presumably, the elimination or reduction of spyware would require that those software providers who currently bundle spyware with their software would need to replace that revenue, which might include charging consumers directly.

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

Not file-sharing software distributed by DCIA Members, since such software does not incorporate spyware. In the fullness of time, the elimination or reduction of spyware would benefit the free distribution of all peer-to-peer file-sharing software by removing a stigma that has been wrongly associated with some major P2P software applications by certain of its opponents, and may be keeping some consumers from installing it.

Martin C. Lafferty
Chief Executive Officer, DCIA