Prepared Statement of

The Federal Trade Commission

Before the

Committee on Commerce, Science & Transportation
Subcommittee on Trade, Tourism, and Economic Development
United States Senate

Washington, D.C.

October 5, 2005

year, the Commission has initiated five law enforcement actions addressing spyware and malware, and has ongoing investigations. Moreover, as in other areas such as spam and data security, we believe that it is essential that industry continue to develop technology to assist its customers in combatting spyware.

II. Spyware Law Enforcement

One of the FTC's first steps in responding to the spyware problem was to educate ourselves in order to develop, implement, and advocate effective policies to respond to it. In 2004, the FTC sponsored a public workshop entitled "Monitoring Software on Your PC: Spyware, Adware, and Other Software." The agency received almost 800 comments in connection with the workshop, and 34 representatives from the computer and software industries, trade associations, consumer advocacy groups and various governmental entities participated as panelists. In March 2005, the FTC released a staff report based on the information received in connection with the workshop.[3] Notwithstanding significant challenges in defining "spyware,"[4]

---

[3] The workshop agenda, transcript, panelist presentations, and public comments received by the Commission are available at http://www.ftc.gov/bcp/workshops/spyware/index.htm. The FTC Staff Report, Monitoring

the staff report recommended that the government should: (1) increase, using existing laws, criminal and civil prosecution of those who distribute spyware; and (2) increase efforts to educate consumers about the risks of spyware. The Commission is pleased to be able to describe today what we are doing to implement these recommendations.

The Commission's spyware law enforcement strategy focuses on three key questions. First, were consumers aware of the installation of the software on their computers? Second, what harm did the installation of the software cause? Third, how difficult was it for consumers to uninstall the software after it had been installed?

A. Did Consumers Know?

A common problem with spyware is that it is installed on consumers' computers without their knowledge. Some spyware distributors use so-called "drive-by" downloads to install their software on computers without even any pretense of obtaining consent. In *FTC v. Seismic Entertainment*,[5] for example, the Commission alleged that the defendants exploited a known vulnerability in the Internet Explorer web browser to download spyware to users' computers without their knowledge. The FTC alleged that this was an unfair act or practice in violation of Section 5 of the FTC Act, and a federal district court entered a preliminary injunction that prohibited the defendants from using this method to distribute their software.

In other instances, software distributors may violate Section 5 of the FTC Act by failing to disclose clearly and conspicuously to consumers the software that is being installed. In

---

[5] *FTC v. Seismic Entertainment, Inc.*, No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004).

FTC v. Odysseus Marketing, Inc.,[6] the defendants offered consumers a free software program that purported to make the consumers anonymous when using peer-to-peer file sharing programs. The Commission alleged, however, the distributors failed to disclose to consumers that this program, in turn, would install other, harmful software on their computers. The Commission recently filed a complaint in federal court alleging that this failure to disclose was deceptive in violation of Section 5 of the FTC Act, and we are awaiting a ruling on our motion for a temporary restraining order. Similarly, in the *Advertising.com, Inc.* case,[7] the respondents allegedly offered free security software, but failed to clearly and conspicuously disclose to consumers that bundled with it was software that traced consumers' Internet browsing and force-fed them pop-up advertising. The Commission recently issued a final consent order to resolve administrative complaint allegations that this failure to disclose was deceptive in violation of Section 5 of the FTC Act.

The Commission's spyware law enforcement actions reaffirm the principle that consumers have the right to decide whether to install new software on their computers. Acts and practices that undermine their ability to make this choice will be vigorously prosecuted.

B. Substantial Harm to Consumers

As the agency learned at the workshop, and through our enforcement actions and subsequent investigations, spyware can cause a broad range of injury to consumers. The harm from spyware may vary significantly in both type and severity.

---

[6] *FTC v. Odysseus Marketing, Inc.*, No. 05-CV-330 (D.N.H. filed Sept. 21, 2005).

[7] *In the Matter of Advertising.com*, FTC File No. 042 3196 (filed Sept. 12, 2005), available at http://www.ftc.gov/os/caselist/0423196/0423196.htm.

The allegations in the *Seismic* case describe a prime example of software causing several types of serious harm to consumers. The software allegedly changed the consumer's browser home page and default search engine, displayed an incessant stream of pop-up ads, and caused the user's computer to malfunction, slow down, or crash. But perhaps the most serious harm alleged was that the spyware secretly installed a number of additional software programs, including programs that could monitor Internet activity and capture personal information entered into online forms.

Another example of serious harm to consumers allegedly caused by spyware arose in the *Odysseus* case. According to the Commission's complaint, the defendants surreptitiously install a spyware program called "Clientman" on the computers of consumers. Clientman, in turn, installs a number of adware and other programs. It also replaces or reformats Internet search engine results, generates pop-up ads, and captures and transmits information, which may include personal information.

In the *Advertising.com* case, the Commission alleged that software bundled with free security software collected information about consumers, including the websites they visited, and then was used to send a substantial number of pop-up ads. Although the harm to an individual consumer from receiving such pop-ups ads may be less egregious than the harm in other FTC spyware cases to date, the harm to consumers in the aggregate from these pop-up ads was sufficient to warrant law enforcement action. The Commission alleged a violation of Section 5 of the FTC Act because the presence of bundled adware that collected information about consumers' computer use and led to numerous pop-up ads clearly would have been material to consumers in determining whether to install the free security software.

As stated in the FTC staff spyware report, it is the combination of lack of knowledge and consumer harm that makes certain installation of software illegal under the FTC Act.[8]

C. Uninstalling and Deleting Spyware Problems

As described above, spyware often is installed without consumers' knowledge and causes consumers substantial harm. This type of installation should not occur, but once it has, consumers should be able to uninstall or disable such software. Unfortunately, the FTC's law enforcement experience and research shows that some software distributors take improper advantage of consumers' concerns about spyware and market bogus anti-spyware tools. In addition, in the FTC's experience, some spyware programs are difficult to identify and uninstall or disable.

[9] the FTC alleged that the defendants made false claims to consumers about the existence of spyware on their machines. According to the FTC's complaint, the defendants then used these false claims to convince consumers to conduct free

---

[9] *FTC v. MaxTheater, Inc.*, No. 05-CV-0069 (E.D. Wa. filed Mar. 7, 2005), available at http://www.ftc.gov/opa/2005/03/maxtheater.htm; *FTC v. Trustsoft, Inc.*, No. H-05-1905 (S.D.Tex. filed May 31, 2005), available at http://www.ftc.gov/opa/2005/06/trustsoft.htm.

"scans" of their computers. These scans identified innocuous software as spyware, helping to persuade consumers to purchase defendants' spyware removal products at a cost of between $30 and $40. Moreover, the FTC alleged, the defendants claimed their spyware removal products could effectively uninstall many different types of known spyware programs, but the defendants' products did not perform as promised. The Commission filed actions alleging that the perpetrators of these scams violated Section 5 of the FTC Act, and the courts have entered preliminary injunctions in both cases that prohibit the claims.

III. Additional Steps to Address Spyware

Given the prevalence of spyware and the consumer harm it inflicts, the FTC has made spyware investigations and prosecutions an enforcement priority, and we will continue to file law enforcement actions against those who distribute spyware in violation of the FTC Act. The Commission would like to emphasize four additional measures that it believes would enhance its efforts to combat the dissemination of spyware.

First, the FTC supports legislation that would enhance its ability to investigate and prosecute spyware distributors that are located abroad or who try to mask their location by using foreign intermediaries to peddle their scams. Webroot, a well-known anti-spyware product distributor, recently reported that a majority of spyware programs distributed to United States consumers come from foreign distributors.[10] In the FTC's investigations, staff finds that, regardless of where spyware distributors are physically located, they often use foreign Internet service providers, web hosting companies, and domain registrars to create their websites, so that it is difficult for the agency to track down who is ultimately responsible.

The FTC's ability to pursue distributors of spyware, spam, and other Internet threats to consumers would be significantly improved if the Congress were to pass the US SAFE WEB Act, introduced by Chairman Smith in the Senate as S.1608. The Act makes it easier for the FTC to share information and otherwise cooperate with foreign law enforcement officials. The Internet knows no boundaries, and it is critical to improve the FTC's ability to work with the

---

[10] Webroot Software, Inc., State of Spyware Q2 2005, released Aug. 2005, at 26, available at http://www.webroot.com/land/sosreport.php.

officials of other countries to prevent online conduct that undermines consumer confidence in the Internet as a medium of communication and commerce.

Second, the Commission will continue to coordinate with its federal and state partners who are starting to bring their own law enforcement actions against spyware distributors to make law enforcement as effective as possible. At the federal level, the Department of Justice is able to prosecute criminally those who distribute spyware in certain circumstances. In August 2005, for instance, the Department announced the indictments of the creator and marketer of a spyware program called "Loverspy" and four others who used the program to break into computers and illegally intercept the electronic communications of others.[11] At the state level, state attorneys general are bringing civil law enforcement actions. Federal criminal and state law enforcement actions are a critical complement to the FTC's law enforcement actions.

Third, the FTC and others need to continue to play an active role in educating consumers about the risks of spyware and anti-spyware tools. The FTC has issued a Consumer Alert specifically on spyware, as well as four other Alerts addressing other online security issues such as viruses and peer-to-peer file sharing. The Spyware Alert lists clues that indicate spyware may have been installed and also discusses measures consumers can take to get rid of spyware or to reduce their chances of getting spyware in the first place. The Spyware Alert has been accessed over 100,000 times since it was released in October 2004, and the tips it includes have been repeated in dozens of print and broadcast media stories.

---

[11] Press Release, Department of Justice, Office of the United States Attorney, Southern District of California Carol C. Lam, News Release Summary (Aug. 26, 2005), available at http://www.usdoj.gov/usao/cas/pr/cas50826.1.pdf.

And, just last week, the Commission launched a new consumer education initiative, OnGuard Online. Over the past few months, the FTC staff has taken a broader look at its education materials and tactics related to cybersecurity, online privacy, and Internet fraud, and

Fourth and finally, the Commission believes that legislation granting the Commission authority to seek civil penalties against spyware distributors may be useful in deterring the dissemination of spyware. As described above, the Commission has challenged conduct related to spyware dissemination as unfair or deceptive acts or practices in violation of Section 5 of the FTC Act. Under Section 13(b) of the FTC Act, the Commission has the authority to file actions against those engaged in this conduct in federal district court and obtain injunctive relief, including monetary relief in the form of consumer redress or disgorgement of ill-gotten profits. However, it may be difficult in some instances for the FTC to prove the sort of financial harm to consumers needed to order consumer redress, or the ill-gotten gains necessary to order disgorgement. A civil penalty is often the most appropriate remedy in such cases, and serves as a strong deterrent.

IV. Technological Solutions

Reducing the problems associated with spyware and other malware will require the efforts of government, consumers, and industry acting both individually and in concert. As in other high-technology areas, the best and most comprehensive responses to misuse of technology will often be improved technology. At this time there are certain technologies consumers can use to help protect themselves, but none is completely effective and further developments are needed to enhance security.

The primary technological tools that consumers can use right now to protect themselves from spyware are detection programs. These programs can scan consumers' computers, inform them whether there is spyware, and offer them the option of disabling it, deleting it, or leaving it alone. To be effective, however, these programs must be updated on a regular basis. In addition,

they are inherently variable depending on what they classify as "spyware." Furthermore, they only detect spyware once it has been installed; they do not prevent its installation. Some Internet service providers have made spyware scanners and removers available to their subscribers. Firewalls also provide some protection from spyware, but, like scanners, they do not prevent spyware from being installed. Rather, they alert consumers if installed spyware attempts to send out information it has collected.

Other technological solutions at the browser and operating system level are being developed. The Commission's experience in other technological areas suggests that market forces will provide the high-tech industry with incentives to develop te