Prepared Statement of

The Federal Trade Commission

Before the

Committee on Commerce, Science, and Transportation

United States Senate

Washington, D.C.

June 11, 2008

I. Introduction

Chairman Pryor and members of the Committee on Commerce, Science, and Transportation, I am Eileen Harrington, Deputy Director of the Bureau of Consumer Protection of the Federal Trade Commission ("Commission" or "FTC").[1] Spyware and other malware can cause substantial harm to consumers and to the Internet as a medium of communication and commerce. Protecting consumers from such harm is a priority for the Commission, and the agency thanks this Committee for the opportunity to describe what the FTC is doing in this area and to provide input on S. 1625, the "Counter Spy Act" introduced by Senators Pryor, Boxer, and Nelson.

This written statement provides background on the Commission's active program to address concerns about spyware and other malware, which includes law enforcement actions and consumer education efforts. First, it discusses the Commission's three key principles related to spyware as illustrated by the eleven spyware-related law enforcement actions the agency has initiated to date. Second, the statement highlights the Commission's consumer education efforts on spyware. Third, the statement offers the Commission's views on the proposed legislation, S. 1625.

The Commission has a broad mandate to prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[2] Although it is often challenging to locate and apprehend the perpetrators, the FTC has successfully challenged the distribution of

---

[1]The written statement presents the views of the Federal Trade Commission. Oral statements and responses to questions reflect the views of the speaker and do not necessarily reflect the views of the Commission or any Commissioner.

[2]15 U.S.C. § 45.

spyware that causes injury to consumers online.

Spyware and other malware that is downloaded without authorization can cause a range of problems for computer users, from nuisance adware that delivers pop-up ads, to software that causes sluggish computer performance, to keystroke loggers that capture sensitive information. As described below, the Commission has an active program to address concerns about spyware and other malware, including law enforcement and consumer education. Since 2004, the Commission has initiated eleven spyware-related law enforcement actions.[3] While the problem of spyware has not been solved, our cases have had a significant effect and, based on our investigative experience, we believe the prevalence of pop-up ads generated by nuisance adware has been dramatically reduced.

II. Spyware Law Enforcement

A. FTC Cases

The Commission's spyware law enforcement actions reaffirm three key principles. The first is that a consumer's computer belongs to him or her, not to the software distributor, and it must be the consumer's choice whether or not to install software. This principle reflects the basic common-sense notion that Internet businesses are not free to help themselves to the resources of a consumer's computer. For example, in *FTC v. Seismic Entertainment Inc.,*[4] and *FTC v. Enternet Media, Inc.,*[5] the Commission alleged that the defendants unfairly downloaded

---

[3]Detailed information regarding each of these law enforcement actions is available at http://www.ftc.gov/bcp/edu/microsites/spyware/law_enfor.htm.

[4]*FTC v. Seismic Entertainment, Inc.*, No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Mar. 22, 2006), *available at* http://www.ftc.gov/os/caselist/0423142/0423142.shtm.

[5]*FTC v. Enternet Media, Inc.*, CV 05-7777 CAS (C.D. Cal., Aug. 22, 2006), *available at* http://www.ftc.gov/os/caselist/0523135/0523135.shtm.

spyware to users' computers without the users' knowledge, in violation of Section 5 of the FTC Act. Stipulated permanent injunctions were entered against the defendants in both matters, and defendants were ordered to disgorge more than $6 million, combined.

The second principle is that buried disclosures of material information necessary to correct an otherwise misleading impression are not sufficient, just as they have never been sufficient in more traditional areas of commerce. Specifically, burying material information in an End User License Agreement will not shield a spyware purveyor from Section 5 liability. This principle was illustrated in *FTC v. Odysseus Marketing, Inc.*[6] and *Advertising.com, Inc.*[7] In these two cases, the Commission's complaint alleged (among other violations) that the defendants failed to disclose adequately that the free software they were offering was bundled with harmful software programs. The orders entered in both cases require the defendants to disclose properly the effects of software programs that they offer in the future.

The third principle is that, if a distributor puts a program on a computer that the consumer does not want, the consumer should be able to uninstall or disable it. This principle is underscored by cases against Zango, Inc.[8] and DirectRevenue LLC.[9] These companies allegedly provided advertising programs, or adware, that monitored consumers' Internet use and displayed

---

[6] *FTC v. Odysseus Marketing, Inc.*, No. 05-CV-330 (D.N.H. Oct. 24, 2006) (stipulated permanent injunction), *available at* http://www.ftc.gov/os/caselist/0423205/0423205.shtm.

[7] *In the Matter of Advertising.com, Inc.*, FTC Dkt. No. C-4147 (Sept. 12, 2005) (consent order), *available at* http://www.ftc.gov/os/caselist/0423196/0423196.shtm.

[8] *In the Matter of Zango, Inc. f/k/a 180 Solutions, Inc.*, FTC Dkt. No. C-4186 (Mar. 7, 2007), *available at* http://www.ftc.gov/os/caselist/0523130/index.shtm.

[9] *In the Matter of DirectRevenue LLC*, FTC Dkt. No. C-4194 (June 26, 2007), *available at* http://www.ftc.gov/os/caselist/0523131/index.shtm.

frequent, targeted pop-up ads – over 6.9 billion pop-ups by Zango alone. According to the Commission's complaints, the companies deliberately made these adware programs difficult for consumers to identify, locate, and remove from their computers, thus thwarting consumer efforts to end the intrusive pop-ups. Among other relief, the consent orders require Zango and DirectRevenue to provide a readily identifiable means to uninstall any adware that is installed in the future, as well as to disgorge $3 million and $1.5 million, respectively.

Similarly, in *FTC v. Digital Enterprises, Inc.*,[10] the Commission alleged that the defendants installed software onto consumers' computers that repeatedly launched text and video pop-ups that consumers could not close or minimize. These pop-ups demanded payment for access to the defendants' purported entertainment web sites. Among other relief, the September 2007 stipulated permanent injunction requires the defendants to provide a way for consumers to remove the software, bars future downloads without consumer consent, and requires the defendants to pay more than $500,000 for consumer redress.

In addition, the agency's law enforcement efforts have alerted the Commission to novel spyware-related consumer protection issues such as the marketing of bogus anti-spyware programs. For example, in *FTC v. MaxTheater, Inc.*[11] and *FTC v. Trustsoft*, *Inc.*,[12] the FTC alleged that the defendants made false claims to consumers about the existence of spyware on their machines and then used these false claims to convince consumers to conduct free "scans"

---

[10]*FTC v. Digital Enterprises, Inc. d/b/a Movieland.com*, CV06-4923 (C.D. Cal. Sept. 5, 2007), available at http://www.ftc.gov/os/caselist/0623008/index.shtm.

[11]*FTC v. MaxTheater, Inc.*, No. 05-CV-0069 (E.D. Wa. Dec. 6, 2005), *available at* http://www.ftc.gov/os/caselist/0423213/0423213.shtm.

[12]*FTC v. Trustsoft*, *Inc.*, No. H-05-1905 (S.D. Tex. Nov. 30, 2005), *available at* http://www.ftc.gov/os/caselist/0523059/0523059.shtm.

of their computers. These scans would identify innocuous software as spyware, helping to persuade consumers to purchase the 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. In both cases, courts entered stipulated permanent injunctions prohibiting the claims and requiring the defendants to disgorge a total of nearly $2 million.

B. Cooperation with Department of Justice and State Law Enforcement

As in so many other areas, cooperation among law enforcement agencies is vital to successful law enforcement in the spyware arena. Many of the worst abuses connected with spyware are criminal,[13] and, in appropriate cases, the Commission coordinates closely with the Department of Justice. For example, in *FTC v. ERG Ventures, LLC*,[14] the FTC's complaint alleged that the defendants secretly downloaded multiple malevolent software programs, including spyware, onto millions of computers without consumers' consent. The defendants also allegedly tricked consumers into downloading harmful software by hiding the malicious programs within seemingly innocuous free software. The U.S. Attorney's Office for the District

---

[13] *See, e.g.*, Department of Justice, Computer Crime & Intellectual Property Section, Computer Crime News Releases, *available at* http://www.usdoj.gov/criminal/cybercrime/ccnews.html.

[14] *FTC v. ERG Ventures, LLC*, 3:06-CV-00578-LRH-VPC (D. Nev. Oct. 3, 2007), *available at* http://www.ftc.gov/os/caselist/0623192/index.shtm. Pursuant to the stipulated order entered by the court in the FTC action, the defendants must disgorge $330,000. A permanent injunction also bars the defendants from downloading software onto consumers' computers without disclosing its function and obtaining consumers' consent prior to installation, bars them from downloading software that interferes with consumers' computer use, and bars false or misleading claims.

of Columbia launched a parallel criminal investigation, and executed search warrants simultaneously with the filing of the FTC's civil case.[15]

The Commission also coordinates with state partners who bring their own law enforcement actions against spyware distributors. The FTC has established a federal-state spyware law enforcement task force to discuss issues and trends in spyware law enforcement. The task force consists of representatives from agencies such as the Department of Justice and state attorneys general. Federal criminal and state law enforcement actions are a critical complement to the FTC's law enforcement actions.

III. Education

In addition to engaging in law enforcement, the FTC has made consumer education a priority. In September 2005, the Commission and a partnership of other federal agencies and the technology industry launched a multimedia, interactive consumer education initiative, OnGuard Online, along with a Spanish-language version, AlertaenLinea. The OnGuardOnline.gov site now attracts over 350,000 unique visits each month, and many organizations have adapted the OnGuard Online materials for their own security training. The comprehensive web site has general information on online safety, as well as sections with specific information on a range of topics, including spyware. The spyware module includes up-to-date information, as well as interactive features like quizzes and videos. As part of the OnGuard Online initiative, the FTC also has distributed a million copies of the brochure and two million copies of the bookmark, "Stop Think Click: 7 Practices for Safer Computing," with information on spyware and other

[15] *See* FTC News Release, *Court Shuts Down Media Motor Spyware Operation* (Nov. 13, 2006), *available at* http://www.ftc.gov/opa/2006/11/mediamotor.shtm.

computer safety topics. The FTC also has issued a Consumer Alert on spyware, as well as Alerts addressing other online security issues such as viruses and peer-to-peer file sharing.[16]

IV. Legislative Steps to Address Spyware

Although the FTC has successfully challenged conduct related to spyware dissemination under Section 5, legislation authorizing the Commission to seek civil penalties in spyware cases could add a potent remedy to those otherwise available to the Commission. Currently, under Section 13(b) of the FTC Act, the Commission has the authority to file actions in federal district court and to obtain injunctive relief and equitable monetary relief in the form of consumer redress or disgorgement. It has been the agency's experience in spyware cases, however, that restitution or disgorgement may not be appropriate or sufficient remedies because consumers often have not purchased a product or service from the defendants, the harm to consumers may be difficult to quantify, or the defendants' profits may be slim or difficult to calculate with certainty. In such cases, a civil penalty may be the most appropriate remedy and serve as a strong deterrent. Accordingly, the Commission is pleased that S. 1625 provides the Commission this valuable law enforcement tool.

Last June, FTC staff provided this Committee with technical comments to S. 1625. Of the various suggestions respectfully made by staff, one important aspect of the bill relating to both injunctive relief and civil penalties stands out. Under general consumer protection

---

[16] *See. e.g.*, *P2P File-Sharing: Evaluate the Risks* (Feb. 2008), *available at* http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt128.shtm; *Botnets and Hackers and Spam (Oh, My!)* (June 2007), *available at* http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt132.shtm; *Spyware* (July 2005), *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/spywarealrt.shtm; *Detect, Protect, Dis-infect: Consumers Online Face Wide Choices in Security Products* (Sept. 2004), *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/idsalrt.shtm; *see generally* http://www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm.

principles and traditional Section 5 jurisprudence, the Commission need not show knowledge or intent in order to obtain injunctive relief: that is, for stopping the violative conduct itself. But, several sections of S. 1625 impose an overarching knowledge or intent threshold for enforcement that could create an additional – and often very challenging – evidentiary burden for the FTC in obtaining injunctions in civil cases. Moreover, Section 5(m)(1) of the FTC Act already requires the Commission to prove knowledge in any action where civil penalties are sought. Eliminating the knowledge or intent threshold from the bill would not change the Commission's elevated burden regarding civil penalties, while maintaining the ordinary burden for obtaining injunctive relief.[17] The agency looks forward to working with the Committee regarding the knowledge and intent aspects of the legislation, as well as any of the other important considerations raised by staff's technical comments.

V. Conclusion

The FTC will continue its aggressive law enforcement and innovative consumer education programs in the spyware arena. The FTC thanks this Committee for focusing attention on this important issue, and for the opportunity to discuss the Commission's law enforcement program.

[17]Indeed, removing the knowledge or intent requirements from S. 1625 would be consistent, for example, with the approach in the CAN-SPAM Act. *See* 15 U.S.C. § 7706(e) (granting the FTC authority to seek cease-and-desist orders and injunctive relief without alleging or proving knowledge). Spam raises similar enforcement issues to spyware regarding quantifying consumer injury and defendants' profits.