P e a ed S a e e f

T e Fede a T ade C l l

Bef e e

C l ee C e ce, Sc é ce, a d T a a l

U ed S a e Se a e

Wa l , D.C.

J e 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

[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. S , , a e La, E f ce e .

A. FTC Ca e

The Commission's spyware law enforcement actions reaffirm three key principles. The Commi2gia.00u3my ru4nd,.

[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

[illegible]

[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.

[10]*FTC v. Digital Enterprises, Inc. d/b/a Movieland.com*, CV06-4923 (C.D. Cal. Sept. 5,

of their computers. These scans would identify innocuous software (v)12s s3(omp)1ed btwasuo (lp3(nti)1oadi

[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.

See FTC News Release,

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. Le 'la 'le S. e .. Add e S , , a e

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. Cntly, under Section 13(b) of the FTC Act, the Commissiuthority 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 JTC staff provided this Coml 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; *Sp]T]/ywd*(Jul 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.

[17]Indeed, removing the knowledge or intent requirements from S. 1625 would be