PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Ey0.004yr ( )8<52.Y-2.3 -4.5 -2.3 Td ( )Tj EMC /P MCID 8 >>BDC 0.00MCID ((T

I. INTRODUCTION

Chairman Levin, Ranking Member McCain, and members of the

As the nation's consumer protection agency, the FTC is committed to protecting consumers in the online marketplace. The Commission is primarily a civil law enforcement agency, and its main operative statute is Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in or affecting commerce.[2] A company acts deceptively if it makes materially misleading statements or omissions.[3] A company engages in unfair acts or practices if its practices cause or are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.[4] The Commission uses its enforcement authority under Section 5 to take action against online advertising companies and others engaged in unfair or deceptive practices. It also educates consumers and businesses about the online environment and encourages industry self regulation.

This testimony will discuss the Commission's work to address three consumer protection issues affecting the online advertising industry: privacy, malware, and data security. It will then provide some recommendations for next steps in this area.

II. CONSUMER PROTECTION ISSUES AFFECTING THE ONLINE ADVERTISING INDUSTRY

A. PRIVACY

Since online privacy first emerged as a significant issue in the mid-1990s, it has been one of the Commission's highest consumer protection priorities. The Commission has worked to address privacy issues in the online marketplace, particularly those raised by online advertising networks, through consumer and business education, law enforcement, and policy initiatives.

---

[2] 15 U.S.C. § 45(a). The Commission also enforces numerous specific statutes.

[3] See Federal Trade Commission Policy Statement on Deception, appended to Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984).

[4] See 15 U.S.C. § 45(n); Federal Trade Commission Policy Statement on Unfairness, appended to Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984) ("FTC Unfairness Statement").

Throughout the last decade, the FTC has examined the privacy implications of online behavioral advertising through a number of workshops and reports.[5] In March of 2012, the Commission released its Privacy Report, which set forth best practices for businesses – including the online advertising industry – to protect consumer privacy while ensuring that companies can continue to innovate.[6] The report called on companies to provide simpler and more streamlined choices to consumers about their data, through a robust universal choice mechanism for online behavioral advertising.[7]

The Commission has also engaged in a number of privacy enforcement actions involving the online advertising industry. For example, in its first online behavioral advertising case, the Commission alleged that online advertising network Chitika violated the FTC Act's prohibition on deceptive practices when it offered consumers the ability to opt out of the collection of information to be used for targeted advertising – without telling them that the opt-out lasted only ten days.[8] The Commission's order prohibits Chitika from making future privacy

---

[5] See, e.g., FTC Press Release, Staff Proposes Online Behavioral Advertising Policy Principles (Dec. 20, 2007), available at http://www.ftc.gov/news-events/press-releases/2007/12/ftc-staff-proposes-online-behavioral-advertising-privacy; FTC Town Hall, Behavioral Advertising: Tracking, Targeting, & Technology (Nov. 1-2, 2007), available at http://www.ftc.gov/news-events/events-calendar/2007/11/behavioral-advertising-tracking-targeting-technology; FTC Workshop, Protecting Consumers in the Next Tech-Ade (Nov. 6-9, 2006), available at http://www.ftc.gov/news-events/events-calendar/2006/11/protecting-consumers-next-tech-ade; FTC Staff Report,

network, Epic was employing "history-sniffing" technology that allowed it to collect data about sites outside its network that consumers had visited, including sites relating to personal health conditions and finances. The FTC alleged that the history sniffing was deceptive and allowed Epic to determine whether a consumer had visited any of more than 54,000 domains, including pages relating to fertility issues, impotence, menopause, incontinence, disability insurance, credit repair, debt relief, and personal bankruptcy. The order imposed similar relief to the other cases in this area.

Finally, in 2012 Google agreed to pay a record $22.5 million civil penalty to settle charges that it misrepresented to Safari browser users that it would not place tracking cookies or serve targeted ads to them,[11] violating an earlier privacy order with the Commission.[12] In its complaint, the FTC alleged that for several months, Google placed a certain advertising tracking cookie on the computers of Safari users who visited sites within Google's DoubleClick advertising network, although Google had previously told these users they would automatically be opted out of such tracking, as a result of the Safari browser default settings. Despite these promises, the FTC alleged that Google circumvented the default settings

B. SPYWARE AND OTHER MALWARE

Spyware and other malware can cause substantial harm to consumers and to the Internet as a medium of communication and commerce. When downloaded without authorization, including through online ads, spyware and other malware can cause a range of problems for computer users, from nuisance adware that delivers unwanted pop-ups, to software that causes sluggish computer performance, to keystroke loggers that capture sensitive information.

The Commission has sought to address concerns about spyware and other malware through law enforcement and consumer education. Since 2004, the Commission has initiated a number of malware-related law enforcement actions, which 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.,[14] and FTC v. Enternet Media, Inc.,[15] the Commission alleged that the defendants unfairly downloaded spyware to users' computers without the users' knowledge, in violation of Section 5 of the FTC Act. And, in its case against CyberSpy Software LLC, the FTC alleged that the defendants unfairly sold keylogging software to others that could be downloaded to users' computers without their knowledge or consent.[16]

---

[14] FTC v. Seismic Entertainment Productions, Inc., et al., No. 04-377-JD (D.N.H. 2006), available at http://www.ftc.gov/enforcement/cases-proceedings/042-3142-x05-0013/seismic-entertainment-productions-inc-et-al.

[15] FTC v. Enternet Media Inc. et al., No. CV 05-777 CAS(C.D. Cal. 2006), available at http://www.ftc.gov/enforcement/cases-proceedings/052-3135-x06-0003/enternet-media-inc-conspycozy-inc-et-al.

[16] FTC v. CyberSpy Software, LLC, No. 6:08-cv-1872-ORL-31GJK (M.D. Fla. 2010), available at http://www.ftc.gov/enforcement/cases-proceedings/082-3160/cyberspy-software-llc-trace-r-spence

The second principle is that buried disclosures of material information necessary to correct an otherwise misleading impression are not sufficient in connection with software downloads, 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 malware purveyor from Section 5 liability. This principle was illustrated in the FTC v. Odysseus Marketing, Inc.[17] and Advertising.com, Inc.[18] In these two cases, the Commission alleged (among other violations) that the companies failed to disclose adequately that the free software they were offering was bundled with harmful software programs.

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 the FTC's cases against Zango, Inc.[19] and DirectRevenue LLC.[20] These companies allegedly provided advertising programs, or adware, that monitored consumers' Internet use and displayed 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

[17] FTC v. Odysseus Marketing, Inc., No. 05-

In its most recent data security case, the FTC announced a settlement with Snapchat, Inc., a company that markets a popular mobile application ("app") that allows consumers to send and receive photo and video messages known as "snaps."[29] According to the complaint, Snapchat misrepresented that its app provided a private, short-lived messaging service, claiming that once the consumer's set timer for a viewed snap expired, the snap "disappears forever." Snapchat's app has a "Find Friends" feature that allows consumers to find and communicate with friends who use the Snapchat service. However, unbeknownst to users, the Find Friends feature collected the names and phone numbers of all contacts in a user's mobile device address book and had major security flaws. The complaint alleges that Snapchat violated Section 5 by misrepresenting the disappearing nature of messages sent through its app and the amount of personal information that its app would collect for the Find Friends feature.

The complaint also charges

The FTC also recently entered into settlements with Credit Karma[30] and Fandango, LLC.[31] to resolve allegations that the companies misrepresented the security of their mobile apps. Credit Karma's mobile app allows consumers to monitor and access their credit scores, credit reports, and other credit report and financial data, and has been downloaded over one million

and other government agencies at the state, local, and federal levels to use these materials and tailor them to their particular constituencies and concerns.

The second is continued industry self-regulation to ensure that ad networks are taking reasonable steps to prevent the use of their systems to display malicious ads to consumers. Just last week, Facebook, Google and Twitter publicly unveiled TrustInAds.org, a new organization aimed at protecting people from malicious online advertisements.[33] The companies report that they will bring awareness to consumers about online ad-related scams and deceptive activities, collaborate to identify trends, and share their knowledge with policymakers and consumer advocates. In addition, the Online Trust Alliance has published guidelines for companies in this area, along with a risk evaluation tool.[34] The Commission applauds these groups for taking steps to address this issue.

Finally, the Commission continues to reiterate its long-standing, bipartisan call for enactment of a strong federal data security and breach notification law. Reasonable and appropriate security practices are critical to preventing data breaches and protecting consumers from identity theft and other harm. Despite the threats posed by data breaches, many companies continue to underinvest in data security. For example, the Commission's settlements have shown that some companies fail to take even the most basic security precautions, such as updating antivirus software or requiring network administrators to use strong passwords. With reports of data breaches on the rise, and with a significant number of Americans suffering from identity theft, having a strong and uniform national data security requirement would reinforce the requirement under the FTC Act that companies must implement reasonable measures to ensure

[33]

that consumers' personal information is protected. Although most states have breach notification laws in place, having a strong and consistent national breach notification requirement would simplify compliance by businesses while ensuring that all consumers are protected.

Among other things, such legislation would supplement the Commission's existing data security authority by authorizing the Commission to seek civil penalties in appropriate circumstances against companies that do not reasonably protect consumers' data. The Commission with authority to seek civil penalties in these cases would help deter unlawful conduct, including using malware to gain access to consumers' personal information – such as through keystroke loggers. Such legislation could provide the Commission with an important consumer protection tool.

VI. CONCLUSION