PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Emerging Threats in the Online Advertising Industry

Before the

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

UNITED STATES SENATE

Washington, D.C.

May 15, 2014

I. INTRODUCTION

Chairman Levin, Ranking Member McCain, and members of the Subcommittee, I am Maneesha Mithal, Associate Director of the Division of Privacy and Identity Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's testimony on consumer protection issues involving the online advertising industry.

Online advertising offers many benefits to consumers. It helps support a diverse range of online content and services that otherwise might not be available, or that consumers would otherwise have to pay for – services such as blogging, social networking and instant access to newspapers and information from around the world. It also can be used to tailor offers for products and services most relevant to consumers' interests.

But online behavioral advertising, which entails collecting information about consumers' online activities across websites in order to serve them personalized advertising, can also raise a number of consumer protection concerns. For example, some consumers may be uncomfortable with the privacy implications of being tracked across the websites they visit, or may be unaware that this practice is even occurring. And, without adequate safeguards in place, consumer tracking data may fall into the wrong hands or be used for adverse unanticipated purposes, including transmission to other third parties. These concerns are exacerbated when the tracking involves sensitive information about, for example, children, health, or a consumer's finances. Finally, online advertising can be used to deliver spyware and other malware to cause a host of problems to consumers' computers.

---

[1] This written statement presents the views of the Federal Trade Commission. My oral statements and responses to questions are my own and do not necessarily reflect the views of the Commission or of any Commissioner.

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 neither reasonably avoidable by consumers nor 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, *Ehavioral Advertising: Tracking, Targeting, & Technology* (Nov. 1-2, 2007), *available at* http://www.ftc.gov/news-events/events-calendar/2007/11/ehavioral-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, *Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

[6] FTC Report, *Protecting Consumers in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012) ("Privacy Report"), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. Commissioner Ohlhausen and Commissioner Wright were not members of the Commission at that time and thus did not participate in the vote on the report.

[7] In the Privacy Report, the Commission articulated five essential elements of a robust do-not-track mechanism: universal, persistent, easy to find and use, effective, and that the mechanism provide control over the collection of information, not just the delivery of targeted ads. *Id.* at 53.

[8] *Chitika, Inc.*, No. C-4324 (F.T.C. June 7, 2011) (consent order), *available at*

misrepresentations. It also requires Chitika to provide consumers with an effective opt-out mechanism, link to this opt-out mechanism in its advertisements, and provide a notice on its website for consumers who may have opted out when Chitika's opt-out mechanism was ineffective. Finally, the order required Chitika to destroy any data that can be associated with a consumer that it collected during the time its opt-out mechanism was ineffective.

Online ad network ScanScout also settled FTC charges that it deceptively claimed that consumers could opt out of receiving targeted ads by changing their computer's web browser settings to block cookies.[9] In fact, ScanScout used Flash cookies, which browser settings could not block. Under the terms of the order, ScanScout is prohibited from misrepresenting the company's data collection practices and consumers' ability to control collection of their data. It also requires ScanScout to improve disclosure of its data collection practices and to provide a user-friendly mechanism that allows consumers to opt out of being tracked.

Epic Marketplace, an online ad network, settled charges that it used "history sniffing" to secretly and illegally gather data from millions of consumers about their interest in sensitive medical and financial issues ranging from fertility and incontinence to debt relief and personal bankruptcy.[10] As explained in the complaint, Epic Marketplace is a large advertising network with a presence on 45,000 websites. Consumers who visited any of the network's sites received a cookie, which stored information about their online practices including sites they visited and the ads they viewed. The cookies allowed Epic to serve consumers behaviorally targeted ads. Despite claims that it would collect information only about consumers' visits to sites in its

---

http://www.ftc.gov/enforcement/cases-proceedings/1023087/chitika-inc-matter.

[9] *ScanScout, Inc.*, No. C-4344 (F.T.C. Dec. 14, 2011) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/102-3185/scanscout-inc-matter.

[10] *Epic Marketplace, Inc.*, No. C-4389 (F.T.C. Mar. 13, 2013), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3182/epic-marketplace-inc.

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 placed advertising tracking cookies on consumers' computers, in many cases by circumventing the Safari browser's default cookie-blocking setting.[13] According to the complaint, Google's misrepresentations violated an earlier FTC order, which barred Google from – among other things – misrepresenting the extent to which consumers can exercise control over the collection of their information.

---

[11] *United States v. Google, Inc.*, No. 512-cv-04177-HRL (N.D. Cal. Nov. 16, 2012), *available at* http://www.ftc.gov/enforcement/cases-proceedings/google-inc.

[12] *Google, Inc.*, No. C-4336 (F.T.C. Oct. 13, 2011), *available at* http://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter.

[13] Google used an exception to the browser's default setting to place a temporary cookie from the DoubleClick domain. Because of the particular operation of the Safari browser, that initial temporary cookie opened the door to all cookies from the DoubleClick domain, including the Google advertising tracking cookie that Google had represented would be blocked from Safari browsers.

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 pop-up ads, 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-conspy-co-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 *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-CV-330 (D.N.H. 2006), *available at* http://www.ftc.gov/enforcement/cases-proceedings/042-3205-x050069/odysseus-marketing-inc-walter-rines.

[18] *Advertising.com, Inc.*, No. C-4147 (F.T.C. Sept. 12, 2005) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/042-3196/advertisingcom-inc-et-al-matter.

[19] *Zango, Inc. f/k/a 180 Solutions, Inc.*, No. C-4186 (F.T.C. Mar. 7, 2007) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/052-3130/zango-inc-fka-180solutions-inc-et-al-matter.

[20] *DirectRevenue LLC*, No. C-4194 (F.T.C. June 26, 2007) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/052-3131/directrevenue-llc-et-al.

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.

In addition to engaging in law enforcement, the FTC has made consumer education on malware issues a priority. The Commission sponsors OnGuard Online, a website designed to educate consumers about basic computer security. [21] OnGuard Online and its Spanish-language counterpart, Alerta en Línea,[22] average more than 2.2 million unique visits per year. The comprehensive web site has general information on online safety, as well as sections with detailed information on a range of topics, including spyware. And, the FTC also has created a number of articles, videos, and games available to consumers on both its website[23] and OnGuard Online to describe the threats associated with spyware and malware as well as provide consumers with information about how to avoid and detect such malicious software.

C. DATA SECURITY

While taking action against the purveyors of malware is important, it is also critical to ensure that companies are taking reasonable steps to ensure that they are not inadvertently enabling third parties to place malware on consumers' computers. To this end, online advertising networks should maintain reasonable safeguards to ensure that they are not displaying advertisements containing malware that can slow down consumers' computers, expose them to unwanted content such as pop-up ads, and gain unauthorized access to their personal information.

---

[21] *See* http://www.onguardonline.gov.

[22] *See* http://www.alertaenlinea.gov.

[23] *See generally* http://www.consumer.ftc.gov.

The Commission has undertaken substantial efforts for over a decade to promote strong data security practices in the private sector in order to prevent hackers and purveyors of malware from harming consumers. In addition to enforcing Section 5 of the FTC Act, discussed above, the Commission enforces several specific statutes and rules that impose obligations upon businesses to protect consumer data. The Commission's Safeguards Rule, which implements the Gramm-Leach-Bliley Act, for example, provides data security requirements for non-bank financial institutions.[24] The Fair Credit Reporting Act requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,[25] and imposes safe disposal obligations on entities that maintain consumer report information.[26] The Children's Online Privacy Protection Act requires reasonable security for children's information collected online.[27] Reasonableness is the foundation of the data security provisions of each of these laws.

The FTC conducts its data security investigations to determine whether a company's data security measures are reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities. The Commission's 53 settlements with businesses that it charged with failing to provide reasonable protections for consumers' personal information have halted harmful data security practices; required companies to provide strong protections for consumer data; and raised awareness about the risks to data, the need for reasonable and appropriate security, and the types of security failures that raise concerns.[28]

---

[24] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).

[25] 15 U.S.C. § 1681e.

[26] *Id.* at § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

[27] 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312 ("COPPA Rule").

[28] *See* Commission Statement Marking the FTC's 50th Data Security Settlement, Jan. 31, 2014, *available*

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-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 that despite its claims regarding reasonable security, Snapchat failed to adequately secure the Find Friends feature, which led to significant misuse and unauthorized disclosure of consumers' personal information. For example, the complaint alleges that numerous consumers complained that they had sent snaps to someone who impersonated a friend. In fact, because Snapchat failed to verify users' phone numbers during registration, these consumers were actually sending their personal snaps to complete strangers who had registered with phone numbers that did not belong to them. Moreover, in December 2013, Snapchat's failures allowed attackers to compile a database of 4.6 million Snapchat usernames and phone numbers, which could have subjected consumers to costly spam, phishing and other unsolicited communications.

---

at http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[29] *Snapchat, Inc.*, No. 132-3078 (F.T.C. May 8, 2014) (proposed consent agreement), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter.

The FTC also recently entered into settlements with Credit Karma, Inc.[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 times. Fandango's mobile app allows consumers to purchase movie tickets and has over 18.5 million downloads. According to the complaints, despite claims that the companies provided reasonable security to consumers' data, Credit Karma and Fandango did not securely transmit consumers' sensitive personal information through their mobile apps. In particular, the apps failed to authenticate and secure the connections used to transmit this data, and left consumers' information vulnerable to exposure – including Social Security numbers, birthdates, and credit report information in the Credit Karma app, and credit card information in the Fandango app. The Commission's settlements prohibit Credit Karma and Fandango from making misrepresentations about privacy and security, and require the companies to implement comprehensive information security programs and undergo independent audits for the next 20 years.

Finally, the FTC announced a case against TRENDnet, Inc., which involved a video camera designed to allow consumers to monitor their homes remotely.[32] The complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring. Although TRENDnet claimed that the cameras were "secure," they had faulty software that left them open to online viewing, and in some instances listening, by anyone with a

---

[30] *Credit Karma, Inc.*, No. 132-3091 (F.T.C. Mar. 28, 2014) (proposed consent agreement), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc.

[31] *Fandango, LLC*, No. 132-3089 (F.T.C. Mar. 28, 2014) (proposed consent agreement), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc.

[32] *TRENDnet, Inc.*, No. C-4426(F.T.C. Jan. 16, 2014) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.

camera's Internet address. This resulted in hackers posting 700 consumers' live video feeds on the Internet. Under the FTC settlement, TRENDnet must maintain a comprehensive security program, obtain outside audits, notify consumers about the security issues and the availability of software updates to correct them, and provide affected customers with free technical support for the next two years.

In each of its 53 data security cases, the Commission has examined a company's practices as a whole and challenged alleged data security failures that were multiple and systemic. Through these settlements, the Commission has made clear that reasonable and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; that the Commission does not require perfect security; and that the mere fact that a breach occurred does not mean that a company has violated the law. These principles apply equally to advertising networks. Just because malware has been installed does not mean that the advertising network has violated Section 5. Rather, the Commission would look to whether the advertising network took reasonable steps to prevent third parties from using online ads to deliver malware.

III. RECOMMENDATIONS FOR NEXT STEPS

The Commission shares this Committee's concerns about the use of online advertisements to deliver malware onto consumers' computers, which implicates each of the areas discussed in this testimony – consumer privacy, malware, and data security. We encourage several additional steps to protect consumers in this area.

The first is more widespread consumer education about how consumers can protect their computers against malware. The FTC materials discussed in this testimony are available at www.OnguardOnline.gov and www.ftc.gov. We encourage businesses, advocacy organizations,

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 longstanding, 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] *See generally* http://www.trustinads.org.

[34] *See generally* Online Trust Alliance, *Advertising & Content Publishing Supply Chain Integrity* (Apr. 1, 2014), *available at* https://otalliance.org/resources/malvertising.html.

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. Providing 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

Thank you for the opportunity to provide the Commission's testimony on consumer protection issues involving the online advertising industry. We look forward to continuing to work with the Subcommittee and Congress on this important issue.