PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

The State of Online Consumer Privacy

Before the

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

UNITED STATES SENATE

Washington, D.C.

March 16, 2011

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee, I am Jon Leibowitz, Chairman of the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to present the Commission's testimony on privacy.[1]

Privacy has been an important component of the Commission's consumer protection mission for 40 years. During this time, the Commission has employed a variety of strategies to protect consumer privacy, including law enforcement, regulation, outreach to consumers and businesses, and policy initiatives.[2]

Over the years, the Commission's goal in the privacy arena has remained constant: to protect consumers' personal information and ensure that they have the confidence to take advantage of the many benefits offered by the dynamic and ever-changing marketplace. To meet this objective, the Commission has periodically re-examined its approach to privacy to ensure that it keeps pace with advances in technology and changing business practices as well as to ensure that incentives for American innovation are maintained. The latest effort in this process is a Preliminary FTC Staff Report, released in December, which proposes a framework for protecting consumer privacy in this era of rapid technological change. This proposed framework is intended to inform policymakers, including Congress, as they develop solutions, policies, and

---

[1] This written statement represents the views of the Federal Trade Commission. Commissioner Kovacic dissents. His concerns about the Commission's testimony, and the report by its staff, are set forth in his statement on the latter. In particular, he believes that the endorsement of a Do Not Track mechanism by staff (in the report) and the Commission (in this testimony) is premature.

My oral presentation and responses are my own and do not necessarily reflect the views of the Commission or of any other Commissioner.

[2] Information on the FTC's privacy initiatives generally may be found at http://business.ftc.gov/privacy-and-security.

potential laws governing privacy, and guide and motivate industry as it develops more robust

[3] 15 U.S.C. §§ 1681e-i.

[4] 15 U.S.C. §§ 7701-7713.

e-i.

Chitika, Inc., FTC F

[7] Many of the Commission's earliest consumer privacy cases similarly held companies accountable for their privacy statements and practices. *See, e.g., GeoCities, Inc.*, FTC Docket No. C-3850 (Feb. 5, 1999) (consent order) (alleging that company misrepresented the purposes for which it was collecting personal information from both children and adults); *Liberty Fin. Cos.*, FTC Docket No. C-3891 (Aug. 12, 1999) (consent order) (alleging that site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously); *FTC v. ReverseAuction.com, Inc.*, No. 00-0032 (D.D.C. Jan. 10, 2000) (consent order) (alleging that online auction site obtained consumer data from competitor site and then sent deceptive, unsolicited e-mail messages to those consumers seeking their business);

telling parents. The Commission's order prohibits the company from sharing information gathered from its monitoring software and requires the company to destroy any such information in its database of marketing information.[8]

Finally, in September, the Commission settled a case against US Search, a data broker that maintained an online service, which allowed consumers to search for information about others. The company allowed consumers to opt out of having their information appear in search results, for a fee of $10. Although 4,000 consumers paid the fee and opted out, their personal information still appeared in search results. The Commission's settlement requires US Search to disclose limitations on its opt-out offer, and to provide refunds to consumers who had previously opted out.[9]

In addition to these privacy enforcement actions, the Commission has been aggressive on the data security front to ensure that companies protect the sensitive data they collect about consumers. In Februaryed fe comp omp

[8] *FTC v. Echometrix, Inc.*, No. CV10-5516 (E.D.N.Y. Nov. 30, 2010) (consent order).

[9] *US Search, Inc.*, FTC File No. 102 3131 (Sept. 22, 2010) (consent order accepted for public comment).

[10] *SettlementOne Credit Corp.*, File No. 082 3208; *ACRAnet, Inc.*, File No. 092 3088; and *Fajilan and Associates, Inc.*, File No. 092 3089 (Feb. 3, 2011) (consent orders accepted for public comment).

hargc

the Gramm-Leach-Bliley Safeguards Rule, and Section 5 of the FTC Act. The consent orders bar the companies from violating these laws, require them to implement comprehensive information security programs, and require them to obtain independent audits, every other year for 20 years.

B. Consumer and Business Education

The FTC has done groundbreaking outreach to businesses and consumers in the area of consumer privacy. For example, the Commission's well-known OnGuard Online website educates consumers about spam, spyware, phishing, peer-to-peer ("P2P") file sharing, social networking, laptop security, and identity theft.[11] The FTC has developed additional resources specifically for children, parents, and teachers to help children stay safe online. In response to the Broadband Data Improvement Act of 2008, the FTC produced the brochure *Net Cetera: Chatting with Kids About Being Online* to give adults practical tips to help children navigate the online world.[12] The publication includes information about how parents should talk to children about online privacy, sexting, and cyberbullying. In less than one year, the Commission already has distributed more than 7 million copies of *Net Cetera* to schools and communities nationwide. The Commission also offers specific guidance to young people concerning certain types of Internet services, including, for example, social networking and video and photo sharing.[13]

---

[11] *See* http://www.onguardonline.gov/topics/social-networking-sites.aspx. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alertaena Línea have attracted nearly 12 million unique visits.

[12] *See* Press Release, FTC, OnGuardOnline.gov Off to a Fast Start with Online Child Safety Campaign (Mar. 31, 2010), *available at* http://www.ftc.gov/opa/2010/03/netcetera.shtm.

[13] *See* http://www.onguardonline.gov/topics/social-networking-sites.aspx; http://www.onguardonline.gov/topics/net-cetera-mobile-phones.aspx.

Most recently, the FTC released a consumer education publication on the safe use of wi-fi hot spots. The publication, available on the FTC and Onguard Online websites, explains that

[14] *See* http://www.onguardonline.gov/topics/hotspots.aspx.

[15] *See Protecting Personal Information: A Guide For Business*, *available at* http://www.ftc.gov/infosecurity.

[16] *See generally* http://business.ftc.gov/privacy-and-security.

[17] FTC Town Hall, *Ehavioral Advertising: Tracking, Targeting, & Technology* (Nov. 1-2, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml.

See

[22] *See A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses a*

A. The Proposed Framework

The proposed framework included three main concepts. First, FTC staff proposed that companies should adopt a "privacy by design" approach by building privacy protections into their everyday business practices. Such protections include providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer in use, and implementing reasonable procedures to promote data accuracy. Companies also should implement and enforce procedurally sound privacy practices throughout their organizations, including, for example, assigning personnel to oversee privacy issues, training

particularly for non-consumer-facing entities such as data brokers. Because of the significant costs associated with access, the Staff Report noted that the extent of access should be proportional to both the sensitivity of the data and its intended use. In addition, the Staff Report stated that companies must provide prominent disclosures and obtain affirmative consent before using data in a materially different manner than claimed when the data was collected.

Finally, the Staff Report proposed that stakeholders implement Do Not Track mechanisms to effectuate consumers' choices with respect to the collection and use of their information.[24]

[24] *See FTC Staff Report, supra note 22. See also* Rosch concurring statement, *id.*, in which Commissioner Rosch supported a Do Not Track mechanism only if it were "technically feasible" and implemented in a fashion that provides informed consumer choice regarding all the attributes of such a mechanism. To clarify, Commissioner Rosch continues to believe that a variety of questions need to be answered prior to the endorsement of any particular Do Not Track mechanism.

[25] Consumer survey evidence, by itself, has limitations. For instance, the way questions are presented may affect survey results. Also, while survey evidence may reveal a consumer's stated attitudes about privacy, survey evidence does not necessarily reveal what actions a consumer will take in real-world situations. The Commission does not endorse the reliability or methodology of any surveys discussed herein.

[26] *See, e.g.*, *Transcript of December 7, 2009, FTC Privacy Roundtable*, Remarks of Alan Westin of Columbia University, at 93-94, *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec2009_Tra00 0.0000 TD(embe)Tj

Jessica Vascellaro, *Websites Rein in Tracking Tools*, W

[32] *See* W3C Blog, Do Not Track at W3C, http://www.w3.org/QA/2011/02/do_not_track_at_w3c.html (Feb. 24, 2011).

[33] *See* Do Not Track: A Universal Third-Party Web Tracking Opt Out (Mar. 7, 2011), *available at* http://tools.ietf.org/html/draft-mayer-do-not-track-00; *see also* http://firstpersoncookie.wordpress.com/2011/03/09/mozilla-makes-joint-submission-to-ietf-on-dnt/.

[34] *See* Press Release, Interactive Advertising Bureau, Major Marketing Media Trade Groups Launch Program to Give Consumers Enhanced Control over Collection and Use of Web Viewing Data for Online Behavioral Advertising (Oct. 4, 2010), *available at* http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-100410; Tony Romm and Kim Hart, Political Intel: FTC Chairman on Self-Regulatory Ad Effort, POLITICO Forums,

grew dramatically at the end of last year.[36] In addition, Google has developed a browser add-on that can be used to block targeted advertisements from companies that participate in the Digital Advertising Alliance.[37]

These recent industry efforts to improve consumer control are promising, but they are still in the embryonic stage, and their effectiveness remains to be seen. As industry continues to explore technical options and implement self-regulatory programs, and Congress continues to examine Do Not Track, several issues should be considered. First, any Do Not Track system should be implemented universally, so that consumers do not have to repeatedly opt out of tracking on different sites. Second, the choice mechanism should be easy to find, easy to understand, and easy to use. Third, any choices offered should be persistent and should not be deleted if, for example, consumers clear their cookies or update their browsers. Fourth, a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes.[38]

---

[36] *See Written Comment of the Direct Marketing Assoc. Responding to Preliminary Staff Report*, cmt. #00449, at 21.

[37] *See* Google Chrome Web Store, Keep My Opt-Outs, *available at* https://chrome.google.com/webstore/detail/hhnjdplhmcnkiecampfdgfjilccfpfoe; *see also* Google Public Policy Blog, Keep your opt-outs http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html (Jan. 24, 2011).

[38] For example, consumers may believe they have opted out of tracking if they block third-party cookies on their browsers; yet they may still be tracked through Flash cookies or other mechanisms.

A Flash cookie, or a Flash local shared object, is a data file that is stored on a consumer's computer by a website that uses Adobe's Flash player technology. Like a regular http cookie, a Flash cookie can store information about a consumer's online activities. Unlike regular cookies, Flash cookies are stored in an area not controlled by the browser. Thus, when a consumer deletes or clears the cookies from his browser using tools provided through the browser, this may not delete Flash cookies stored on his computer.

Finally, it is important to emphasize what is meant by “tracking” as stakeholders

Recently, a researcher released a software tool that demonstrates several technical mechanisms in addition to Flash cookies that websites can use to persistently track consumers, even if they have attempted to prevent such tracking through existing tools. *See* http://samy.pl/evercookie; *see also* Tanzina Vega, *New Web Code Draws Concerns Over Privacy Risks*, N.Y. TIMES, Oct. 10, 2010, *available at* http://www.nytimes.com/2010/10/11/business/media/11privacy.html.

III. Conclusion

Thank you for the opportunity to provide the Commission's views. We look forward to continuing this important dialogue with Congress and this Committee.