

PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

on

Privacy and Data Security: Protecting Consumers in the Modern World

Before the

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

UNITED STATES SENATE

Washington, D.C.

June 29, 2011

¹ The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any other Commissioner. Commissioner William E. Kovacic dissents from this testimony to the extent that it endorses a Do Not Track mechanism. Commissioner Rosch dissents to the portions of the testimony that discuss and describe certain conclusions about the concept of Do Not Track. His views are included in an attached Separate Statement.

Information on the FTC's privacy initiatives generalmation on the F

privacy through ongoing policy initiatives, such as a recent proposed privacy framework.

This testimony begins by describing some of the uses of consumer data that affect consumers' privacy in today's economy. It then offers an overview of the Commission's recent efforts in the enforcement, education, and policy areas. While the testimony does not offer views on general privacy legislation, the Commission encourages Congress to enact data security legislation that would (1) impose data security standards on companies, and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.⁴

II. Information Flows in the Current Marketplace

For today's consumer, understanding the complex transfers of personal information that occur in the offline and online marketplaces is a daunting task. Indeed, these information flows take place in almost every conceivable consumer interaction. For example, a consumer goes to work and provides sensitive information to her employer, such as her Social Security Number, to verify her employment eligibility, and bank account number, so that she can get paid. After work, she uses an application on her smartphone to locate the closest ATM so that she can withdraw cash. She then visits her local grocery store and signs up for a loyalty card to get

⁴ The Commission has long supported data security and breach notification legislation. *See, e.g.*, Prepared Statement of the Federal Trade Commission, *Data Security*, Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Comm. on Energy and Commerce, 112th Cong., June 15, 2011, *available at* <http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf> (noting the Commission's support for data security and breach notification standards); Prepared Statement of the Federal Trade Commission, *Protecting Social Security Numbers From Identity Theft*, Before the Subcomm. on Social Security of the H. Comm. on Ways and Means, 112th Cong., April 13, 2011, *available at* <http://ftc.gov/os/testimony/110411ssn-idtheft.pdf> (same); FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), *available at* www.ftc.gov/os/2008/12/P075414ssnreport.pdf; President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), *available at* <http://www.idtheft.gov/reports/IDTReport2008.pdf>.

brokers have long gathered information about our retail purchases, and consumer reporting agencies have long made decisions about our eligibility for credit, employment, and insurance based on our past transactions. But new online business models such as online behavioral advertising, social networking, interactive gaming, and location-based services have complicated the privac

⁵ 16 C.F.R. Part 310.

⁶ 15 U.S.C. §§ 1681e-i.

⁷ 15 U.S.C. §§ 7701-7713.

soug

⁸ See <http://www.ftc.gov/os/closings/staffclosing.shtm>.

⁹ See the Commission's Safeguards Rule under the Gramm-Leach-Bliley Act, 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b), and provisions of the FCRA, 15 U.S.C. §§ 1681e, 1681w, implemented at 16 C.F.R. Part 682.

¹⁰ *Ceridian Corp.*, FTC Docket No. C-4325 (June 8, 2011) (consent order), available at www.ftc.gov/opa/2011/05/ceridianlookout.shtm.

¹¹ *Lookout Servs., Inc.*, FTC Docket No. C-4326 (June 15, 2011) (consent order), available at www.ftc.gov/opa/2011/05/ceridianlookout.shtm.

¹² See *U.S. v. Teletrack, Inc.*, No. 1:11-CV-2060 (N.D. Ga. filed June 24, 2011) (proposed consent order), available at <http://www.ftc.gov/opa/2011/06/teletrack>.

Buzz.¹⁴ The Commission charged that Google made public its Gmail users' associations with their frequent email contacts without the users' consent and in contravention of Google's privacy policy. As part of the Commission's 0B TDt0/rt

¹⁴ *Google, Inc.*, FTC File No. 102 3136 (Mar. 30, 2011) (consent order accepted for public comment), available at www.ftc.gov/opa/2011/03/google.shtm. Commissioner Rosch issued a concurring statement expressing concerns about the terms of the proposed consent agreement, available at <http://www.ftc.gov/os/caselist/1023136/110330googlebuzzstatement.pdf>.

¹⁵ This provision would apply to any data collected by Google about users of any Google product or service, including mobile and location-based data.

¹⁶ *Chitika, Inc.*, FTC Docket No. C-4324 (June 7, 2011) (consent order), available at <http://www.ftc.gov/opa/2011/03/chitika.shtm>.

data that can be associated with a1 yc(an be a)Tj33.8400 0.0n0ot oumer c

¹⁷ *US Search, Inc.*, FTC Docket No. C-4317 (Mar. 14, 2011) (consent order), *available at* <http://www.ftc.gov/opa/2010/09/ussearch.shtm>.

¹⁸ *See U.S. v. Playdom, Inc.*, No. SACV11-00724 (C.D. Cal. filed May 11, 2011) (proposed consent order), *available at* <http://www.ftc.gov/opa/2011/05/playdom.shtm>.

¹⁹ See www.ong

²¹ See *Protecting Personal Information: A Guide For Business*, available at www.ftc.gov/infosecurity.

Letter from Maneesha Mit

²⁴ *See generally* FTC Exploring Privacy web page, at www.ftc.gov/bcp/workshops/privacyroundtables

²⁶ Commissioner Kovacic believes that the endorsement of a Do Not Track mechanism by staff (in the report) and the Commission (in this testimony) is premature. His concerns about the Commission Staff Report are set forth in his statement on the report. *See* FTC Staff Report, *supra* note 22, at App. D. 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. *Id.* at App. E. Commissioner Rosch continues to believe that a variety of issues need to be addressed prior to the endorsement of any particular Do Not Track mechanism. *See* Statement of Commissioner J. Thomas Rosch, Dissenting in Part, *Privacy and Data Security: Protecting Consumers in the Modern World*, Hearing Before the S. Comm. on Commerce, Science, and Transportation, 112th Cong.(June 29, 2011).

²⁷ *See, e.g.*, Prepared Statement of the Federal Trade Commission, *The State of Online Consumer Privacy*,

should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes. Finally, an effective Do Not Track system would go beyond simply opting consumers out of receiving targeted advertisements; it would opt them out of collection of behavioral data for all purposes other than product and service fulfillment and other commonly accepted practices.²⁸

Of course, any Do Not Track system should not undermine the benefits that online behavioral advertising has to offer, by funding online content and services and providing personalized advertisements that many consumers value. For this reason, any Do Not Track mechanism should be flexible. For example, it should allow companies to explain the benefits of tracking and to take the opportunity to convince consumers not to opt out of tracking. Further, a Do Not Track system could include an option that enables consumers to control the types of advertising they want to receive and the types of data they are willing to have collected about them, in addition to providing the option to opt out completely.²⁹

Industry appears to be receptive to the demand for simple choices. Recently, three of the major browsers offered by Mozilla, Microsoft, and Apple, announced the development of new choice mechanisms for online behavioral advertising that seek to provide increased transparency, greater consumer control and improved ease of use. More recently, Mozilla introduced a version

²⁸ As noted in prior Commission testimony, such a mechanism should be different from the Do Not Call program in that it should not require the creation of a “Registry” of unique identifiers, which could itself cause privacy concerns. *See Do Not Track Testimony, supra* note 27.

²⁹ For example, use of a Do Not Track browser header would enable consumer customization. The browser could send the header to some sites and not others. Moreover, a particular site could ignore the header to the extent the user has consented to tracking on that site.

of its browser that enables Do Not Track for mobile web browsing. In addition, an industry coalition of media and marketing associations, the Digital Advertising Alliance, has continued to make progress on implementation of its improved disclosure and consumer choice mechanism offered through a behavioral advertising icon.

Third, the Staff Report proposed a number of measures that companies should take to make their data practices more transparent to consumers. For instance, in addition to providing the contextual disclosures described above, companies should improve their privacy notices so that consumers, advocacy groups, regulators, and others can compare data practices and choices across companies, thus promoting competition among companies. The staff also proposed providing consumers with reasonable access to the data that companies maintain about them, 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. Staff is evaluating the 450 comments received and expects to issue a final report later this year.

In addition to issuing reports, the Commission also reviews its rules periodically to ensure that they keep pace with changes in the marketplace. The Commission is currently reviewing its rule implementing COPPA and anticipates that any proposed changes will be announced in the coming months.³⁰

Finally, the Commission hosts workshops to study and publicize more specific issues.

³⁰ See generally COPPA Rulemaking and Rule Reviews web page, available at business.ftc.gov/documents/coppa-rulemaking-and-rule-reviews.

³¹ See, e.g., Richard Power, Carnegie Mellon CyLab, *Child Identity Theft, New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers* (2011), available at www.cyblog.cylab.cmu.edu/2011/03/child-identity-theft.html; Children's Advocacy Institute, *The Fleecing of Foster Children: How We Confiscate Their Assets and Undermine Their Financial Security* (2011), available at http://www.cachildlaw.org/Misc/Fleecing_Report_Final_HR.pdf.

³² See Press Release, FTC, Department of Justice to Host Forum on Child Identity Theft (June 2, 2011), available at www.ftc.gov/opa/2011/06/childtheft.shtm.

VI. Conclusion

The Commission is committed to protecting consumers' privacy and security – both online and offline. We look forward to continuing to work with Congress on these critical issues.