PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

BALANCING PRIVACY AND INNOVATION:

DOES THE PRESIDENT'S PROPOSAL TIP THE SCALE?

Before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

March 29, 2012

I. Introduction

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

I am pleased to be testifying today alongside Administrator Lawrence Strickling of the National Telecommunications and Information Administration. The Commission supports the recent efforts and approach developed by the Department of Commerce regarding privacy issues. The FTC looks forward to working together with the Department of Commerce and the

[1] The views expressed in this statement represent the views of the Commission, with Commissioner J. Thomas Rosch dissenting. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any other Commissioner.

[2] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf. Commissioner Rosch dissented from the issuance of the Final Privacy Report. He agrees that consumers ought to be given a broader range of choices and applauded the Report's call for targeted legislation regarding data brokers and data security. However, Commissioner Rosch has four major concerns about the privacy framework because he believes that: 1) in contravention of our promises to Congress, it is based on "unfairness" rather than deception; 2) the current state of "Do Not Track" still leaves unanswered many important questions; 3) "opt-in" will necessarily be selected as the de facto method of consumer choice for a wide swath of entities; and 4) although characterized as only "best practices," the Report's recommendations may be construed as federal requirements. *See*

targeted legislation that would provide consumers with access to information about them held by

data brok

---

[5] The Commission supports legislation similar to that contained in several of the data security bills introduced in the 112th Congress. *See* Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Congress (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011).

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

[7] 15 U.S.C. §§ 6501-6508
0000 TD (ss.)Tj ea)Tj 15.00 Tf (See)Tj 2.j 12.9600 0.0000 TD (

This testimony begins by describing the Commission's final privacy report. It then offers an overview of other recent policy efforts in the areas of privacy and data security and concludes by noting the Commission's recent enforcement and education efforts.

II. Privacy Report

Earlier this week, the FTC released its final privacy report ("Final Report"), setting forth best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. To the extent these best practices exceed existing legal requirements, they are not intended to serve as a template for law enforcement or regulations under laws currently enforced by the FTC.

The Final Report continues to support the three main principles laid out in the preliminary staff report.[8] *First*, 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

---

[8] In December 2010, the Commission issued a preliminary staff report to address the privacy issues associated with new technologies and business models. *See A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. Commissioners Kovacic and Rosch issued concurring statements available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf at Appendix D and Appendix E, respectively. The preliminary staff report set forth a proposed framework to guide policymakers and other stakeholders regarding best practices for consumer privacy and included a number of questions for public comment. The Commission received over 450 public comments from various stakeholders in response to the preliminary report. These comments informed the Commission as it refined the framework to best protect consumer privacy and innovation in today's dynamic and rapidly-changing marketplace.

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.

Choice, companies should provide simpler and more streamlined choices to consumers about their data practices. Companies do not need to provide choice before collecting and using consumers' data for practices that are consistent with the context of the transaction, the company's relationship with the consumer, or as required or specifically

Do Not Track is intended to apply to third-party

[10] For example, the FTC recently brought an action against a company that told consumers they could opt out of tracking by exercising choices through their browsers; however, the company used Flash cookies for such tracking, which consumers could not opt out of through their browsers. *In the Matter of* , FTC Docket No. C-4344 (Dec. 21, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023185/111221scanscoutdo.pdf

Such a mechanism should be different f

The Mozilla Blog

approach – how to limit secondary use of collected data so that the consumer opt-out extends beyond simply blocking targeted ads and to the collection of information for other purposes. The DAA has released new principles that include limitations on the collection of tracking data and prohibitions on the use or transfer of the data for employment, credit, insurance, or health care eligibility purposes.[17] Just as important, the DAA recently moved to address some persistence and usability criticisms of its icon-based opt out by committing to honor the tracking choices consumers make through their browser settings.[18]

At the same time, the World Wide Web Consortium ("W3C"), an Internet standards-setting body has gathered a broad range of stakeholders to create an international, industry-wide standard for Do Not Track, including DAA member companies; other U.S. and international companies; industry groups; and public interest organizations. The W3C group has done admirable work to flesh out how to make a Do Not Track system practical in both desktop and mobile settings as reflected in two public working drafts of its standards.[19] Some important issues remain, and the Commission encourages all of the stakeholders to work within the W3C group to resolve these issues.

While work remains to be done on Do Not Track, the Commission believes that the developments to date are significant and provide an effective path forward. The advertising

---

[17] Digital Advertising Alliance, *About Self-Regulatory Principles for Multi-Site Data* (Nov. 2011), *available at* http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

[18] Press Release, Digital Advertising Alliance, *DAA Commitment to Honor Browser-Based Choices* (Feb. 22, 2012), *available at* http://www.aboutads.info/resource/download/DAA.Commitment.pdf.

[19] *See* Press Release, W3C, *W3C Tracking Protocol Specification Advances* (Nov. 14, 2011), *available at* http://www.w3.org/2011/11/dnt-pr.html.en.

industry, through the DAA, has committed to deploy browser-based technologies for consumer control over online tracking, alongside its ubiquitous icon program. The W3C process, thanks in part to the ongoing participation of DAA member companies, has made substantial progress toward specifying a consensus consumer choice system for tracking that is practical and technically feasible.[20] The Commission anticipates continued progress in this area as the DAA members and other key stakeholders continue discussions within the W3C process to work to reach consensus on a Do Not Track system in the coming months.

B. Data Brokers

The Final Report recommends that companies provide consumers with reasonable access to the data maintained about them. The extent of such access should be proportionate to the sensitivity of the data and the nature of its use.

The Final Report addresses the particular importance of consumers' ability to access information that data brokers have about them. Data brokers are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information for a variety of purposes, including verifying an individual's identity, differentiating one consumer's records from another's, marketing products, and preventing financial fraud. Such entities often have a wealth of information about

[20] A system practical for both businesses and consumers would include, for users who choose to enable Do Not Track, significant controls on the collection and use of tracking data by third parties, with limited exceptions such as security and frequency capping. As noted above, first party sharing with third parties is not consistent with the context of the interaction and would be subject to choice. Do Not Track is one way for users to express this choice.

consumers without interacting directly with them. Consumers are often unaware of the existence of these entities, as well as the purposes for which they collect and use data.[21]

The Commission has monitored data brokers since the 1990s, hosting workshops, drafting reports, and testifying before Congress about the privacy implications of data brokers' practices.[22] Following a Commission workshop, data brokers created the Individual References Services Group (IRSG).[23] 00 cm 2a9l000T33TD /F2000 0.0000 TD (s)Tj 4.6800 0.0000 TD (Gr)Tj 15.600

---

[21] As noted above, first-party sharing with third parties is not consistent with the context of the interaction and would be subject to choice.

[22] *See, e.g.*, Prepared Statement of the FTC, *[illegible]*, 109th Cong. (Mar. 10, 2005), [illegible] http://www.ftc.gov/os/testimony/050310idtheft.pdf; [illegible] FTC Workshop, *[illegible]* (Mar. 13, 2001), [illegible] http://www.ftc.gov/bcp/workshops/infomktplace/index.shtml; FTC Workshop, *[illegible]* (June 18, 2003), [illegible] http://www.ftc.gov/bcp/workshops/infoflows/030618agenda.shtm.

[23] *[illegible]* FTC, *[illegible]* (1997), [illegible] http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm.

[24] *[illegible]* Prepared Statement of the FTC, *[illegible]*, 109th Cong. (Mar. 15, 2005), [illegible] http://www.ftc.gov/os/2005/03/050315protectingconsumerdata.pdf.

[25] *See, e.g.*, Prepared Statement of the FTC, *Legislative Hearing on H.R. 2221, the Data Accuracy and Protection Act, and H.R. 1319, the*

could exercise such options. This website would improve transparency and enhance consumer control over the data practices of companies that maintain and share data about them for marketing purposes. It could also provide consumer-facing entities such as retailers a means for ensuring that the information brokers from which they purchase consumer information have instituted appropriate transparency and control mechanisms. Indeed, the consumer-facing entities could provide consumers with a link to the centralized website, after having made sure that the data brokers from which they buy data participate in such a system. The Commission staff intends to discuss with relevant companies how this mechanism could be developed and implemented voluntarily, to increase the transparency and give consumers tools to opt out.[28]

III. Other Policy Initiatives

In addition to conducting policy reviews, such as through the Final Report, the

[28] The current website of the Direct Marketing Association (DMA) offers an instructive model for such a mechanism. The DMA – which consists of data brokers, retailers, and others – currently offers a service through which consumers can opt out of receiving marketing solicitations via particular channels, such as direct mail, from DMA member companies. *See* DMAChoice, http://www.dmachoice.org/dma/member/home.action.

[29] FTC Staff Report, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012) at http://www.ftc.gov/opa/2012/02/mobileapps_kids.shtm

n u(107Di00.00000 1.00000 03ln06i 11 10rlb00 2sei 28.2000 0.008h00 c116.8800 0.0000 TD (dc800 1

[30] News reports indicate that some companies, like Apple, are already working to limit certain types of data collection via apps. *See, e.g.*, Kim-Mai Cutler, *Amid Privacy Concerns, Apple Has Started Rejecting Apps That Access UDIDs*, TechCrunch (Mar. 24, 2012), http://techcrunch.com/2012/03/24/apple-udids/.

[31] FTC Workshop, *Dot Com Disclosures* (May 30, 2012), *available at* http://www.ftc.gov/opa/2012/02/dotcom.shtm.

[32] FTC, *Dot Com Disclosures* (2000), *available at* http://www.ftc.gov/os/2000/05/0005dotcomstaffreport.pdf

[33] FTC Workshop, *Face Facts: A Forum on Facial Recognition Technology* (Dec. 8, 2011), *available at* http://www.ftc.gov/bcp/workshops/facefacts/

discuss an array of current and future uses and benefits, and explore potential privacy and security concerns. Since then, Commission staff sought comments on the issues raised during the workshop and will issue a report in the coming months.

Third, as discussed in the Final Report, the FTC intends to examine the practices of large platforms such as Internet browser companies, mobile operating system providers, Internet Service Providers, and large social media platforms that can collect data from numerous sources to build extensive profiles about consumers. Commission staff will host a workshop in the second half of 2012 to examine questions about the scope of such data collection practices, the potential uses of the collected data, and related issues.

Finally, the Commission is undertaking a comprehensive review of the COPPA Rule in light of rapidly evolving technology and changes in the way children use and access the Internet.[34] In September 2011, the Commission proposed modifications to the Rule intended to update the Rule to meet changes in technology, assist operators in their compliance obligations, strengthen protections over children's data, and provide greater oversight of COPPA safe harbor programs.[35] For example, the Commission proposed adding geolocation information and cookies used for behavioral advertising to the definition of "personal information," which would have the

---

[34] *See* Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 75 Fed. Reg. 17,089 (Apr. 5, 2010), *available at* http://www.ftc.gov/os/fedreg/2010/april/P104503coppa-rule.pdf.

[35] The Commission's Notice of Proposed Rulemaking can be found at 76 Fed. Reg. 59,804 (Sept. 15, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-27/pdf/2011-24314.pdf

received over 350 comments on its proposed amendments to the COPPA Rule, which are being reviewed by FTC staff.

IV. Enforcement

In addition to its engagement on the policy front, enforcement remains a top priority for the agency. In the last 15 years, the Commission has brought 36 data security cases; almost 80 cases against companies for improperly calling consumers on the Do Not Call registry;[36] 86 cases against companies for violating the Fair Credit Reporting Act ("FCRA");[37] 97 spam cases; 15 spyware or nuisance adware cases; 18 COPPA cases; and numerous cases against companies for violating the FTC Act by making deceptive claims about the privacy and security protections they afford to consumer data. Where the FTC has authority to seek civil penalties, it has aggressively done so. It has obtained $60 million in civil penalties in Do Not Call cases; $21 million in civil penalties under the FCRA; $5.7 million under the CAN-SPAM Act;[38] and $6.6 million under COPPA. Where the Commission does not have authority to seek civil penalties, as in the data security and spyware areas, it has sought such authority from Congress.

Two recent privacy cases – against Internet giants Google and Facebook – will benefit more than one billion consumers worldwide. The Commission charged Google with deceiving consumers by taking previously private information – the frequent contacts of Gmail users – and making it public in order to generate and populate a new social network, Google Buzz.[39] This,

---

[36] 16 C.F.R. Part 310.

[37] 15 U.S.C. §§ 1681e-i.

[38] 15 U.S.C. §§ 7701-7713.

[39] *See, e.g.*, In the Matter of Google Inc., Docket No. C-4336 (Oct. 13, 2011) (final decision and consent order), *available at* http://www.ftc.gov/opa/2011/10/buzz.shtm.

[40] *In the Matter of* Lululemon Athletica Inc., Matter No. 0923184 (Nov. 29, 2011) (proposed consent agreement),

affirmative express consent before sharing their information in a way that exceeds their privacy settings; and requires it to implement a comprehensive privacy program and obtain outside audits. In addition, Facebook must ensure that it will stop providing access to a user's information after she deletes her account.

Further, the Commission continues to be active on the data security and children's privacy front. Just this week, it announced a settlement with RockYou, a company that allowed consumers to upload and store photos and slideshows.[41] Consumers who registered with RockYou were required to provide their

[41] *See U.S. v. RockYou, Inc.*, No. CV 12 1487 (N.D. Cal. filed Mar. 26, 2012) (consent decree).

to-peer ("P2P") file sharing and socia

[42] *See* www.onguardonline.gov. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alerta en Línea have attracted more than 25 million visits.

[43] *See* Press Release, FTC, *Facts from the FTC: What You Should Know About Mobile Apps* (June 28, 2011), *available at* http://www.ftc.gov/opa/2011/06/mobileapps.shtm.

[44] *See Take Charge: Fighting Back Against Identity Theft*, *at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

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

FTC's Business Center website, which averages one million unique visitors each month.[50] The Commission also hosts a Business Center blog,[51] which frequently features consumer privacy and data security topics; presently, approximately 3,500 attorney

[50] *See generally* http://business.ftc.gov/. The Privacy and Data Security portal is the most popular destination for visitors to the Business Center.

[51] *See generally* http://business.ftc.gov/blog.