PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

THE NEED FOR PRIVACY PROTECTIONS:

PERSPECTIVES FROM THE ADMINISTRATION

AND THE FEDERAL TRADE COMMISSION

Before the

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

UNITED STATES SENATE

Washington, D.C.

May 9, 2012

I. Introduction

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee, I am Jon Leibowitz, Chairman of the Federal Trade Commission ("FTC" or "Commission").[1]

We are pleased to be testifying today alongside General Counsel Cameron Kerry of the Department of Commerce and the newest member of the FTC, Commissioner Maureen Ohlhausen. The Commission supports the privacy efforts and approach developed by the Department of Commerce, and we look forward to working with the Department of Commerce, the Administration, and Congress as they move forward in their efforts in this arena. Members of this Committee in particular have demonstrated that they understand how important it is that consumers' – and especially children and teens' – personal data be treated with care and respect.

This is a critical juncture for consumer privacy, as the marketplace continues to rapidly evolve and new approaches to privacy protection are emerging in the United States and around the world. After careful consideration, the Commission recently released the final privacy report ("Final Report"). The Final Report sets forth best practices for businesses to guide current efforts to protect consumer privacy while ensuring that companies can continue to innovate. The Commission urges industry to use this guidance to improve privacy practices and accelerate the pace of self-regulation. Importantly, we have seen promising developments by industry toward a Do Not Track mechanism and we ask the Committee to continue to encourage industry to move towards full implementation. The Report also calls on Congress to consider enacting general privacy legislation. We reiterate today our call to Congress to enact legislation requiring

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

companies to implement reasonable security measures and notify consumers in the event of cert

[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

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 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 authorized by law. For all other data practices, consumers should have the ability to make informed and meaningful choices at a relevant time and context and in a uniform and comprehensive way. The Commission advocated such an approach for online behavioral tracking – often referred to as "Do Not Track" – that is discussed in more detail below.

Finally, companies should take steps to make their data practices more transparent to consumers. For instance, companies should improve their privacy disclosures and work toward standardizing them so that consumers, advocacy groups, regulators, and others can compare data practices and choices across companies, thus promoting competition among companies. Consumers should also have reasonable access to the data that companies maintain about them, particularly for non-consumer-facing entities such as data brokers, as discussed in more detail below. The extent of access should be proportional to the volume and sensitivity of the data and to its intended use.

In addition, the Final Report makes general and specific legislative recommendations. The Report supports the development of general privacy legislation to ensure basic privacy protections across all industry sectors, and can inform Congress, should it consider such privacy

[5] Earlier this year, the Administration released its final "White Paper" on consumer privacy, recommending that Congress enact legislation to implement a Consumer Privacy Bill of Rights. *See Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012), *available at* http://

The Report's recommendations broadly address the commercial use of consumer information, both online and offline, by businesses. Below, we highlight two specific issues addressed in the Report – Do Not Track and data brokers.

A. Do Not Track

The Final Report advocates the continued implementation of a universal, one-stop mechanism to

[7] Do Not Track is intended to apply to third-party tracking of consumers because third-party tracking is inconsistent with the context of a consumer's interaction with a website; by contrast, most first-party marketing practices are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice.

[8] For example, the FTC brought an action against a company that told consumers they could opt out of tracking by exercising

Not Track privacy control for its Firefox browser that an impressive number of consumers have adopted.[10] Apple subsequently included a similar Do Not Track control in Safari.[11]

The online advertising industry, led by the Digital Advertising Alliance ("DAA"), has also led efforts by implementing a behavioral advertising opt-out program. The DAA's accomplishments are notable: it has developed a notice and choice mechanism through a standard icon in ads and on publisher sites; deployed the icon broadly, with reportedly over 900 billion impressions served each month; obtained commitments to follow the self-regulatory principles from advertisers, ad networks, and publishers that represent close to 90 percent of the online behavioral advertising market; and established an enforcement mechanism designed to ensure compliance with the principles.[12] The DAA is also working to address one of the long-standing criticisms of its approach – how to limit secondary use of collected data so that the

---

[10] The Mozilla Blog, *Mozilla Firefox 4 Beta, Now Including "Do Not Track" Capabilities* (Feb. 8, 2011), blog.mozilla.com/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities/; Alex Fowler, *Do Not Track Adoption in Firefox Mobile is 3x Higher than Desktop*, MOZILLA PRIVACY BLOG (Nov. 2, 2011), http://blog.mozilla.com/privacy/2011/11/02/do-not-track-adoption-in-firefox-mobile-is-3x-higher-than-desktop/.

[11] Nick Wingfield, *Apple Adds Do-Not-Track Tool to New Browser*, WALL ST. J., Apr. 13, 2011, *available at* http://online.wsj.com/article/SB10001424052748703551304576261272308358858.html. Google has taken a slightly different approach – providing consumers with a browser extension that opts them out of most behavioral advertising on a persistent basis. Sean Harvey & Rajas Moonka, *Keep Your Opt Outs*, GOOGLE PUBLIC POLICY BLOG (Jan. 24, 2011), http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html.

[12] Peter Kosmala, *Yes, Johnny Can Benefit From Transparency & Control*, SELF-REGULATORY PROGRAM FOR ONLINE BEHAVIORAL ADVERTISING, http://www.aboutads.info/blog/yes-johnny-can-benefit-transparency-and-control (Nov. 3, 2011); *see also* Press Release, Digital Advertising Alliance, *White House, DOC and FTC Commend DAA's Self-Regulatory Program to Protect Consumers Online Privacy* (Feb. 23, 2012), *available at* http://www.aboutads.info/resource/download/DAA%20White%20House%20Event.pdf.

consumer opt-out extends beyond simply blocking targeted ads and to the collection of information for other purposes. The DAA has released 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.[13] The DAA is now working to fully implement these principles. 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.[14]

At the same time, the World Wide Web Consortium ("W3C"), an Internet standards-setting body, has convened 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.[15] Some important issues remain, and the Commission encourages all of the stakeholders to work within the W3C group to resolve these issues.

---

[13] 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.

[14] Press Release, Digital Advertising Alliance, *DAA Position on Browser Based Choice Mechanism* (Feb. 22, 2012), *available at* http://www.aboutads.info/resource/download/DAA.Commitment.pdf.

[15] *See* Press Release, W3C, *Two Drafts Published by the Tracking Protection Working Group* (Mar. 13, 2012), *available at* http://www.w3.org/News/2012#entry-9389; Press Release, W3C, *W3C Announces First Draft of Standard for Online Privacy* (Nov. 14, 2011), *available at* http://www.w3.org/2011/11/dnt-pr.html.en.

[16] 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 for functions such as security and frequency capping. As noted above, a website's sharing of behavioral information with third parties is not consistent with the context of the consumer's interaction with the website and would be subject to choice. Do Not Track is one wa

[17] As noted above, in connection with online tracking, it is generally inconsistent with the context of the interaction for a consumer-facing entity to share the consumer's data with a third party. Accordingly, such transfers of personal information would be subject to choice.

[18] *See, e.g.*, Prepared Statement of the FTC, *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information*: *Hearing Before the S. Comm. on Banking, Housin*

ChoicePoint – led to renewed scrutiny of the practices of data brokers,[20] there have been no meaningful broad-based efforts to implement self-regulation in this area in recent years.

To improve the transparency of the practices of data brokers, the Final Report proposes that data brokers, like all companies, provide consumers with reasonable access to the data they maintain. Because most data brokers are invisible to consumers, however, the Commission makes two additional recommendations as to these entities.

The Commission has long supported legislation that would give access rights to consumers for information held by data brokers.[21] For example, Senator Pryor and Chairman Rockefeller's S.1207 includes provisions to establish a procedure for consumers to access information held by data brokers.[22] The Commission continues to support legislation in this area to improve transparency of the industry's practices.[23]

---

[20] *See* Prepared Statement of the FTC, *Protecting Consumers' Data: Policy Issues Raised by ChoicePoint*: *Hearing before H. Comm. on Energy & Commerce, Subcomm. on Commerce, Trade, and Consumer Protection, Comm. on Energy & Commerce*, 109th Cong. (Mar. 15, 2005), *available at* http://www.ftc.gov/os/2005/03/050315protectingconsumerdata.pdf.

[21] *See, e.g.*, Prepared Statement of the FTC, *Legislative Hearing on H.R. 2221, the Data Accountability and Protection Act, and H.R. 1319, the Informed P2P User Act: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Trade, and Consumer Protection*, 111th Cong. (May 5, 2009), *available at* http://www.ftc.gov/os/2009/05/P064504peertopeertestimony.pdf.

[22] Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011); *see also* Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Congress (2011).

[23] *See, e.g.*, Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong. (May 4, 2011), *available at* http://www.ftc.gov/opa/2011/05/pdf/110504datasecurityhouse.pdf; Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong.(June 15, 2011), *available at* http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf; Prepared Statement of the FTC,

Protecting Consumers in the Modern World: Hearing Before the S. Comm. on Commerce,

share it, and with whom. The report recommends that all members of the children's app ecosystem – the stores, developers and third parties providing services – should play an active role in providing key information to parents.[27] The report also encourages app developers to provide information about data practices simply and succinctly. The Commission has already reached out to work with industry to provide parents with the information they need, and some industry participants have taken positive steps to improve disclosures going forward.

To discuss how members of the mobile and online ecosystems can best disclose their data practices to consumers, the Commission will host a public workshop later this month.[28] The workshop will address the technological advancements and marketing developments since the FTC first issued its online advertising disclosure guidelines known as "Dot Com Disclosures,"[29] including the advent of smartphones and tablets. The workshop will examine whether and how to revise the Dot Com Disclosures in the current online and mobile advertising environment and will include a specific panel on mobile privacy disclosures.[30]

---

[27] 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 UDID*, TECHCRUNCH (Mar. 24, 2012), http://techcrunch.com/2012/03/24/apple-udids/.

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

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

[30] In addition to examining mobile disclosures, the Commission continues to examine other privacy and security issues associated with the mobile ecosystem. *See, e.g.*, FTC Workshop, *Paper, Plastic ... or Mobile?: An FTC Workshop on Mobile Payments* (Apr. 26, 2012), *available at* http://www.ftc.gov/bcp/workshops/mobilepayments/.

The Commission’s Notice of Proposed Ru

[38] *Google, Inc.*, Docket No. C-4336 (Oct. 13, 2011) (final decision and consent order), *available at* http://www.ftc.gov/opa/2011/10/buzz.shue000 0.0400 cm000 TD(tc)TmET1.0q1.00000 0.00000 0.

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

[41] *See* www.onguardonline.gov. Since its launch in 2005, OnGuard Online and its Spanish-language

with information about mobile apps, including what apps are, the types of data they can collect and share, and why some apps collect geolocation information.[42]

The Commission has also issued numerous education materials1.00000 0.00000 0.00000 meneA.00ns

[42] *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.

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

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

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

[46] *See Peer-to-Peer File Sharing: A Guide for Business, available at* http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm

violating the FCRA, but encouraged them to review their apps and their policies and procedures to ensure they comply with the Act.

VI. Conclusion

These policy, enforcement, and education efforts demonstrate the Commission's continued commitment to protecting consumers' privacy and security – both online and offline. As noted above, the Commission encourages Congress to develop general privacy legislation and to adopt targeted legislation addressing data brokers. We appreciate the leadership of Chairman Rockefeller and this Committee on these issues and look forward to continuing to work with Congress, the Administration, industry and other critical stakeholders on these issues in the future.