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

I. Introduction

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

Privacy has been an important component of the Commission's consumer protection mission for 40 years.[2] During this time, 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 undertaken substantial efforts to promote privacy in the private sector through law enforcement, education, and policy initiatives. For example, since 2001, the Commission has brought 34 cases challenging the practices of companies that failed to adequately protec

[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.

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

[3] 15 U.S.C. §§ 6501-6508.

[4] The Commission has long supported data security and breach notification legislation. *See, e.g.*, Prepared Statement of the Federa

withdraw cash. She then visits her local grocery store and signs up for a loyalty card to get discounts on future purchases. Upon returning home, the consumer logs onto her computer and begins browsing the web and updating her social networking page. Later, her child logs on to play an online interactive game.

All of these activities clearly benefit the consumer – she gets paid, enjoys free and immediate access to information, locates places of interest, obtains discounts on purchases, stays connected with friends, and can entertain herself and her family. Her life is made easier in a myriad of ways because of information flows.

There are other implications, however, that may be less obvious. Her grocery store purchase history, web activities, and even her location information, may be collected and then sold to data brokers and other companies she does not know exist. These companies could use her information to market other products and services to her or to make decisions about her eligibility for credit, employment, or insurance. And the companies with whom she and her family interact may not maintain reasonable safeguards to protect the data they have collected.

Some consumers have no idea that this type of information collection and sharing is taking place. Others may be troubled by the collection and sharing described above. Still others may be aware of this collection and use of their personal information but view it as a worthwhile trade-off for innovative products and services, convenience, and personalization. And some consumers – some teens for example – may be aware of the sharing that takes place, but may not appreciate the risks it poses. Because of these differences in consumer understanding, and attitudes, as well as the rapid pace of change in technology, policymaking on privacy issues presents significant challenges and opportunities.

As the hypothetical described above shows, consumer privacy issues touch many aspects of our lives in both the brick-and-mortar and electronic worlds. In the offline world, data 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 privacy picture. In addition, the aggregation of data in both the online and offline worlds have in some instances led to increased opportunities for fraud. For instance, entities have used past transaction history gathered from both the online and offline world to sell "sucker lists" of consumers who may be susceptible to different types of fraud. In both the online and offline worlds, data security continues to be an issue. The FTC continues to tackle each of these issues through enforcement, education, and policy initiatives.

III. Enforcement

In the last 15 years, the Commission has brought 34 data security cases; 64 cases against companies for improperly calling consumers on the Do Not Call registry;[5] 86 cases against companies for violating the Fair Credit Reporting Act ("FCRA");[6] 97 spam cases; 15 spyware (or nuisance adware) cases; and 16 cases against companies for violating COPPA. 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

[5] 16 C.F.R. Part 310.

[6] 15 U.S.C. §§ 1681e-i.

million under the CAN-SPAM Act;[7] and $6.2 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. In addition, the Commission has brought numerous cases against companies for violating the FTC Act by making deceptive claims about the privacy protection they afford to the information they collect. And these numbers do not fully reflect the scope of the Commission's vigorous enforcement agenda, as not all investigations result in enforcement actions. When an enforcement action is not warranted, staff closes the investigation, and in some cases it issues a closing letter."[8] This testimony highlights the Commission's recent, publicly-announced enforcement efforts to address the types of privacy issues raised by the hypothetical scenario described above

First, the Commission enforces the FTC Act and several other laws that require companies to maintain reasonable safeguards for the consumer data they maintain.[9] Most recently, the Commission resolved allegations that Ceridian Corporation[10] and Lookout Services, Inc.[11] violated the FTC Act by failing to implement reasonable safeguards to protect the sensitive consumer information they maintained. The companies offered, respectively, payroll processing

---

[7] 15 U.S.C. §§ 7701-7713.

[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.

and immigration compliance services for small business employers. As a result, they both obtained, processed, and stored highly-sensitive information – including Social Security numbers – of employees. The Commission alleged that both companies failed to appropriately safeguard this information, which resulted in intruders being able to access it. The orders require the companies to implement a comprehensive data security program and obtain independent audits for 20 years.

Second, the Commission enforces the FCRA, which, among other things, prescribes that companies only sell sensitive consumer report information for "permissible purposes," and not for general marketing purposes. Just this week, the Commission announced an FCRA enforcement action against Teletrack for violating this provision. Teletrack provides consumer reporting services to payday lenders, rental purchase stores, and certain auto lenders, so that they can determine consumers' eligibility to receive credit.[12] The Commission alleged that Teletrack created a marketing database of consumers, and sold lists of consumers who had applied for payday loans to entities that did not have a permissible purpose. The Commission asserted that Teletrack's sale of these lists violated the FCRA because the lists were in fact consumer reports, which cannot be sold for marketing purposes. The Commission's agreement with Teletrack requires it to pay $1.8 million in civil penalties for FCRA violations.

Third, the Commission has been active in ensuring that companies engaged in social networking adhere to any promises to keep consumers' information private.[13] The

---

[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.shtm.

[13] *See, e.g., Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 2, 2011) (consent order), *available at* http://www.ftc.gov/opa/2010/06/twitter.shtm (resolving allegations that social networking service Twitter deceived its customers by failing to honor their choices after offering

Commission's recent case against Google alleges that the company deceived consumers by using information collected from Gmail users to generate and populate its new social network, Google 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 proposed settlement order, Google must implement a comprehensive privacy program and conduct independent audits every other year for the next 20 years.[15] Further, Google must obtain affirmative express consent for product or service enhancements that involve new sharing of previously collected data.

Fourth, the Commission has sought to protect consumers from deceptive practices in the behavioral advertising area. In June, the Commission finalized a settlement with Chitika, Inc., an online network advertiser that acts as an intermediary between website publishers and advertisers.[16] The Commission's complaint alleged that Chitika violated the FTC Act by offering 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. The Commission's order prohibits Chitika from making future privacy misrepresentations. It also requires Chitika to

---

the opportunity to designate certain "tweets" as private).

[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.

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 requires Chitika to destroy any data that can be associated with a consumer that it collected during the time its opt-out mechanism was ineffective.

Fifth, the Commission has tried to ensure that data brokers respect consumers' choices. In March, the Commission announced a final order against US Search, a data broker that maintained an online service, which allowed consumers to search for information about others.[17] The company allowed consumers to opt out of having their information appear in search results, for a fee of $10. The Commission charged that 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.

Finally, to protect children's privacy, the Commission enforces the Children's Online Privacy Protection Act ("COPPA"). In its most recent case, against Playdom, Inc. and one of its senior executives, the Commission obtained an agreement with the operators of 20 online virtual worlds to pay $3 million to settle charges that they violated COPPA by illegally collecting and disclosing personal information from hundreds of thousands of children under age 13 without their parents' consent.[18] The defendants allegedly collected children's ages and email addresses

---

[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.

during registration and then enabled them to publicly post their full names, email addresses, instant messenger IDs, and location on personal profile pages and in online community forums. The FTC charged that the defendants' failure to provide proper notice or obtain parents' prior verifiable consent before collecting or disclosing children's personal information violated COPPA. It further charged that the defendants violated the FTC Act because their privacy policy misrepresented that the company would prohibit children under 13 from posting personal information online. In addition to the $3 million civil penalty – the largest ever for a COPPA violation – the proposed settlement permanently bars the defendants from violating COPPA and from misrepresenting their information practices regarding children.

IV. Education

The FTC conducts outreach to businesses and consumers in the area of consumer privacy. The Commission's well-known OnGuard Online website educates consumers about many online threats to consumer privacy and security, including spam, spyware, phishing, peer-to-peer ("P2P") file sharing, and social networking.[19] The Commission has also issued numerous education materials to help consumers protect themselves from identity theft and to deal with its consequences when it does occur. The FTC has distributed over 3.8 million copies of a victim recovery guide – *Take Charge: Fighting Back Against Identity Theft* – and has recorded over 3.5 million visits to the Web version. In addition, the FTC has developed education 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

[19] *See* www.onguardonline.gov. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alertaena Línea have attracted nearly 12 million unique visits.

children navigate the online world.[20] In less than one year, the Commission distributed more than 7 million copies of *Net Cetera* to schools and communities nationwide.

Business education is also an important priority for the FTC. The Commission developed a widely-distributed guide to help small and medium-sized businesses implement appropriate data security for the personal information they collect and maintain.[21]

Another way in which the Commission seeks to educate businesses is by publicizing its complaints and orders and issuing public closing letters. For example, the Commission recently sent a letter closing an investigation of Social Intelligence Corporation, a company that sold reports to employers about potential job applicants.[22] The reports included public information gathered from social networking sites. The investigation sought to determine Social Intelligence's compliance with the FCRA.[23] Although the staff decided to close the particular investigation, the public closing letter served to notify similarly situated businesses that, to the extent they collect information from social networking sites for employment determinations, they must comply with the FCRA. The letter included guidance on the obligations of such businesses under the FCRA. For example, companies must take reasonable steps to ensure the maximum possible accuracy of the information reported from social networking sites. They

---

[20] *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.

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

[22] Letter from Maneesha Mithal, Associate Director, Division of Privacy & Identity Protection to Renee Jackson, Counsel to Social Intelligence Corporation (May 9, 2011), *available at* www.ftc.gov/os/closings/110509socialintelligenceletter.pdf.

[23] FTC staff did not express an opinion on the merits of Social Intelligence's business model.

must also provide employers who use their report

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

[25] *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* www.ftc.gov/os/2010/12/101201privacyreport.pdf. Commissioners Kovacic and Rosch issued concurring statements *available at* www.ftc.gov/os/2010/12/101201privacyreport.pdf at Appendix D and Appendix E, respectively.

[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*, Hearing Before the S. Comm. on Commerce, Science and Transportation, 112th Cong. (Mar. 16, 2011), *available at* http://www.ftc.gov/os/testimony/110316consumerprivacysenate

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. 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

[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.

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 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 ke p pace with changes in technology and the

[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*

theft, how to protect children's personal data, and how to help parents and young adults who have been victims of child identity theft recover from the crime.

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.