**PREPARED STATEMENT OF**

**THE FEDERAL TRADE COMMISSION**

**on**

**Internet Privacy: The Views of the FTC, the FCC, and NTIA**

**Before the**

**COMMITTEE ON ENERGY AND COMMERCE**

**SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE**

**and**

**SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY**

**UNITED STATES HOUSE OF REPRESENTATIVES**

**Washington, D.C.**

**July 14, 2011**

## I. Introduction

Chairman Bono-Mack, Chairman Walden, Ranking Member Butterfield, Ranking Member Eshoo, and members of the Subcommittees, I am Edith Ramirez, 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 part 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 protect consumers' personal information; more than 100 spam and spyware cases; and 16 cases for violation of the Children's Online Privacy Protection Act ("COPPA").[3] The

---

[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 J. Thomas Rosch dissents to the portions of the testimony that discuss and describe certain conclusions about the concept of Do Not Track. Commissioner Rosch also has some reservations about the proposals in the preliminary staff privacy report. *See* attached statement, Statement of Commissioner J. Thomas Rosch, Dissenting in Part, *Internet Privacy: The Views of the FTC, FCC, and NTIA*, Before the Subcomm. on Commerce, Manufacturing, and Trade and Subcomm. on Communications and Technology of the H. Comm. on Energy and Commerce, 112th Cong., July 14, 2011 (hereinafter "Rosch 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.

Commission also has distributed millions of copies of educational materials for consumers and businesses to address ongoing threats to security and privacy. And the FTC examines the implications of new technologies and business practices on consumer 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 today. It then offers an overview of the Commission's recent enforcement, education, and policy efforts. While the testimony does not offer views on general privacy legislation, the Commission continues to encourage 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 offline and online 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

---

[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.

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 discounts on future purchases. Upon returning home, the consumer logs onto her computer and begins browsing the web and updates her social networking profile. Later, her twelve-year old grabs her smartphone and plays games on a mobile app.

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 myriad 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.

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, 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; 16 cases against companies for violating COPPA; 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

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

[6] 15 U.S.C. §§ 1681e-i.

Call cases; $21 million in civil penalties under the FCRA; $5.7 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.

And these activities 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, 16 C.F.R. Part 314, implementing provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801(b), and the Commission's Disposal Rule, 16 C.F.R. Part 682, implementing provisions of the FCRA, 15 U.S.C. §§ 1681e, 1681w.

[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. Last month, the Commission announced an FCRA enforcement action against Teletrack, Inc., which 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 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. Last month, 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.

Finally, the Commission has sought 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.

## 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.[18]

---

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

Last month, the FTC issued a new consumer education guide called "Understanding Mobile Apps: Questions and Answers." The guide provides consumers 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.[19] The FTC issued the guide to help consumers better understand the privacy and security implications of using mobile apps before downloading them.

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.[20] 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 children navigate the online world.[21] In less than one year, the Commission distributed more than 7 million copies of *Net Cetera* to schools and communities nationwide.

---

[19] *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.

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

[21] *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.

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.[22]

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.[23] The reports included public information gathered from social networking sites. The investigation sought to determine Social Intelligence's compliance with the FCRA.[24] 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 must also provide employers who use their reports with information about the employers' obligation to notify job applicants if they were denied employment on the basis of these reports, and to provide such applicants with information about their rights under the FCRA.

---

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

[23] 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.

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

## V. Policy Initiatives

The Commission reviews its rules periodically to ensure that they keep pace with changes in the marketplace.[25] The Commission is currently reviewing its rule implementing COPPA and anticipates that any proposed changes will be announced in the coming months.[26]

In addition to reviewing rules, the Commission's policy initiatives also include public workshops, reports, and policy reviews to examine the implications of new technologies and business practices on consumer privacy. For example, in December 2009, February 2010, and March 2010, the FTC convened three public roundtables to explore consumer privacy issues, including the issues facing the hypothetical consumer discussed in Section II above.[27] The roundtables examined the effectiveness of current privacy approaches in addressing the challenges of the rapidly evolving market for consumer information, including consideration of the risks and benefits of consumer information collection and use; consumer expectations

---

[25] For example, the Commission recently announced plans to enhance the agency's longstanding program to review rules and guides in order to increase transparency and public participation and reduce burden on business. *See, e.g.*, Prepared Statement of the Federal Trade Commission, *The FTC's Regulatory Reform Program: Twenty Years of Systematic Retrospective Rule Reviews & New Prospective Initiatives to Increase Public Participation and Reduce Burdens on Business*, Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce, 112th Cong., July 7, 2011, *available at* http://www.ftc.gov/os/testimony/110707regreview.pdf; Notice Announcing Ten-Year Regulatory Review Schedule and Review of the Federal Trade Commission's Regulatory Review Program (July 7, 2011), *available at* http://www.ftc.gov/os/fedreg/2011/07/110707regulatoryreviewfrn.pdf. More information about the Commission's efforts can be found on the Regulatory Review web page, http://www.ftc.gov/ftc/regreview/index.shtml.

[26] *See generally* COPPA Rulemaking and Rule Reviews web page, business.ftc.gov/documents/coppa-rulemaking-and-rule-reviews.

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

surrounding various information management practices; and the adequacy of existing legal and self-regulatory regimes to address privacy interests. At the roundtables, stakeholders across the board emphasized the need to improve the transparency of businesses' data practices, simplify the ability of consumers to exercise choices about how their information is collected and used, and ensure that businesses take privacy-protective measures as they develop and implement systems that involve consumer information.[28] At the same time, the roundtable commenters and participants urged regulators to be cautious about restricting the exchange and use of consumer data in order to preserve the substantial consumer benefits made possible through the flow of information.

Staff issued a preliminary privacy report in December 2010 ("Staff Report"),[29] which discusses the major themes that emerged from these roundtables, including the ubiquitous collection and use of consumer data; the extent to which consumers are able to understand and to make informed choices about the collection and use of their data; the importance of privacy to

---

[28] *See generally 3rd Roundtable*, *Panel 4: Lessons Learned and Looking Forward* at 242, *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_March2010_Transcript.pdf (industry and consumer representatives suggesting the need to simplify consumer choice and improve transparency); *Written Comment of Centre for Information Policy & Leadership at Hunton & Williams LLP*, cmt. #544506-00059, *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf (industry group comment on improving transparency, choice, and accountability on privacy); Leslie Harris, *Written Comment of Center for Democracy & Technology*, cmt. #544506-00067, *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00067.pdf (urging companies to adopt privacy by design).

[29] *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.

many consumers; the significant benefits enabled by the increasing flow of information; and the blurring of the distinction between personally identifiable information and supposedly anonymous or de-identified information.[30] The Staff Report proposed a new framework to guide policymakers and industry as they consider further steps to improve consumer privacy protection.

### 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. The Staff Report also urges companies to implement and to enforce procedurally sound privacy practices throughout their organizations, including, for example, assigning personnel to oversee privacy issues, training employees on privacy issues, and conducting privacy reviews when developing new products and services. Such concepts are not new, but the Staff Report indicated that the time has come for industry to implement them systematically. Implementation can be scaled, however, to each company's business operations. For example, the Staff Report recommended that companies that collect and use small amounts of nonsensitive consumer data should not have to devote the same level of resources to implementing privacy programs as companies that collect vast amounts of consumer data or data of a sensitive nature.

---

[30] *Id.* at 22-38.

Second, the FTC staff proposed that companies provide simpler and more streamlined choices to consumers about their data practices. Under this approach, consumer choice would not be necessary for a limited set of "commonly accepted" data practices, thus allowing clearer, more meaningful choice with respect to practices of greater concern. This component of the proposed framework is premised on the notion that consumers reasonably expect companies to engage in certain practices, such as product and service fulfillment, internal operations such as assessing the quality of services offered, fraud prevention, legal compliance, and first-party marketing. Some of these practices, such as a retailer's collection of a consumer's address solely to deliver a product the consumer ordered, are obvious from the context of the transaction, and therefore, consumers' consent to them can be inferred. Others are sufficiently accepted or necessary for public policy reasons that companies need not request consent to engage in them. The Staff Report suggested that by clarifying those practices for which consumer consent is unnecessary, companies will be able to streamline their communications with consumers, which will reduce the burden and confusion on consumers and businesses alike.

For data practices that are not "commonly accepted," the Staff Report proposed that consumers should have the ability to make informed and meaningful choices. To be most effective, choices should be clearly and concisely described and offered at a time and in a context in which the consumer is making a decision about his or her data. Depending upon the particular business model, this may entail a "just-in-time" approach, in which the company seeks consent at the point a consumer enters his personal data or before he accepts a product or service. One way to facilitate consumer choice is to provide it in a uniform and comprehensive way. Such an approach has been proposed for behavioral advertising, whereby consumers would be able to choose whether to allow the collection and use of data regarding their online

searching and browsing activities. This idea – often referred to as "Do Not Track" – is discussed further below.

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 Report 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. 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 undertake a broad effort to educate consumers about commercial data practices and the choices available to them. Increasing consumer understanding of the commercial collection and use of their information is important to both empowering consumers to make informed choices regarding their privacy and facilitating competition on privacy across companies. In addition to proposing these broad principles, the staff sought comment from all interested parties to help guide further development and refinement of the proposed framework. Close to 450 comments were received and the staff expects to issue a final report this year.

### B. Do Not Track

As noted above, the Staff Report included a recommendation to implement Do Not Track – a universal, one-stop choice mechanism for online behavioral tracking, including behavioral advertising.[31] Following the release of the Staff Report, the Commission has testified that any Do Not Track system should include certain attributes.[32] 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. Finally, an effective Do Not Track system would go beyond simply opting consumers out of receiving targeted

---

[31] 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 29, 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 believes that a variety of issues need to be addressed prior to the endorsement of any particular Do Not Track mechanism. *See* Rosch Statement, *supra* note 1.

[32] *See, e.g.*, Prepared Statement of the Federal Trade Commission, *The State of Online Consumer Privacy*, Before the S. Comm. on Commerce, Science and Transportation, 112th Cong., Mar. 16, 2011, *available at* http://www.ftc.gov/os/testimony/110316consumerprivacysenate.pdf; Prepared Statement of the Federal Trade Commission, *Do Not Track*, Before the Subcomm. on Commerce, Trade and Consumer Protection of the H. Comm. on Energy and Commerce, 111th Cong., Dec. 2, 2010, *available at* www.ftc.gov/os/testimony/101202donottrack.pdf (hereinafter "Do Not Track Testimony").

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.[33]

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.[34]

Industry appears to be receptive to the demand for simple choices. Within the last six months, 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. 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

---

[33] 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 32.

[34] 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.

Alliance, has continued to make progress on implementation of its improved disclosure and consumer choice mechanism offered through a behavioral advertising icon.

## 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.