PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

The State of Online Consumer Privacy

Before the

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

UNITED STATES SENATE

Washington, D.C.

March 16, 2011

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

Privacy has been an important component of the Commission's consumer protection mission for 40 years. During this time, the Commission has employed a variety of strategies to protect consumer privacy, including law enforcement, regulation, outreach to consumers and businesses, and policy initiatives.[2]

Over the years, 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 periodically re-examined its approach to privacy to ensure that it keeps pace with advances in technology and changing business practices as well as to ensure that incentives for American innovation are maintained. The latest effort in this process is a Preliminary FTC Staff Report, released in December, which proposes a framework for protecting consumer privacy in this era of rapid technological change. This proposed framework is intended to inform policymakers, including Congress, as they develop solutions, policies, and

---

[1] This written statement represents the views of the Federal Trade Commission. Commissioner Kovacic dissents. His concerns about the Commission's testimony, and the report by its staff, are set forth in his statement on the latter. In particular, he believes that the endorsement of a Do Not Track mechanism by staff (in the report) and the Commission (in this testimony) is premature.

My oral presentation and responses are my own and do not necessarily reflect the views of the Commission or of any other Commissioner.

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

potential laws governing privacy, and guide and motivate industry as it develops more robust and effective best practices and self-regulatory guidelines.

This testimony begins by describing the Commission's recent efforts to protect consumer privacy through law enforcement, education, and policy initiatives. It then sets forth some highlights from the Staff Report on consumer privacy, and concludes with a discussion of issues related to a universal choice mechanism for behavioral tracking, commonly referred to as "Do Not Track".

I. The FTC's Efforts to Protect Consumer Privacy

A. Enforcement

The Commission continues to pursue an aggressive and bipartisan privacy enforcement agenda. In the last 15 years, it has brought 32 data security cases; 64 cases against companies for improperly calling consumers on the Do Not Call registry; 86 cases against companies for violating the Fair Credit Reporting Act ("FCRA");[3] 97 spam cases; 15 spyware (or nuisance adware) cases; and 15 cases against companies for violating the Children's Online Privacy Protection Act ("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 million under the CAN-SPAM Act,[4] and $3.2 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

[3] 15 U.S.C. §§ 1681e-i.

[4] 15 U.S.C. §§ 7701-7713.

making deceptive claims about the privacy protection they afford to the information they collect, which has the effect of undermining consumer choices on privacy. This testimony describes four such cases that the Commission has brought within the past several months.

Just this week, the Commission announced its first online behavioral advertising case against an online network advertiser, Chitika, that acts as an intermediary between website publishers and advertisers. The Commission 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.[5] The Commission's order prohibits Chitika from making future privacy misrepresentations. It also requires Chitika to 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.

Second, earlier this month, the Commission approved a final consent order in a case involving the social networking service Twitter.[6] On one level, Twitter is a traditional data security case – the FTC charged that serious lapses in the company's data security allowed hackers to obtain unauthorized administrative control of Twitter. As a result, hackers had access to private "tweets" and non-public user information and took over user accounts, including

---

[5] *Chitika, Inc.*, FTC File No. 102 3087 (Mar. 14, 2011) (consent order accepted for public comment).

[6] *Twitter, Inc.*, FTC File No. 092 3093 (Mar. 11, 2011) (consent order) (resolving allegations that Twitter deceived its customers by failing to honor their choices to designate certain "tweets" as private).

among others, those of President Obama and Rupert Murdoch. On another level, the case stands for the proposition that social networking services must honor the commitments they make to keep their users' communications private. The order prohibits misrepresentations about the extent to which Twitter protects the privacy of communications, requires Twitter to maintain reasonable security, and mandates independent, comprehensive audits of Twitter's security practices.[7]

Third, in December, the Commission announced a case against EchoMetrix, a company selling a software program called Sentry Parental Controls that enables parents to monitor their children's activities online. The Commission alleged that EchoMetrix sold certain information that it collected from children via this software to third parties for marketing purposes, without

---

[7] Many of the Commission's earliest consumer privacy cases similarly held companies accountable for their privacy statements and practices. *See, e.g., GeoCities, Inc.*, FTC Docket No. C-3850 (Feb. 5, 1999) (consent order) (alleging that company misrepresented the purposes for which it was collecting personal information from both children and adults); *Liberty Fin. Cos.*, FTC Docket No. C-3891 (Aug. 12, 1999) (consent order) (alleging that site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously); *FTC v. ReverseAuction.com, Inc.*, No. 00-0032 (D.D.C. Jan. 10, 2000) (consent order) (alleging that online auction site obtained consumer data from competitor site and then sent deceptive, unsolicited e-mail messages to those consumers seeking their business); *FTC v. Toysmart.com LLC*, 00-CV-11341-RGS (D. Mass. filed July 10, 2000) (alleging site attempted to sell personal customer information, despite the representation in its privacy policy that such information would never be disclosed to a third party); *FTC v. Rennert,* No. CV-S-00-0861-JBR (D. Nev. July 24, 2000) (consent order) (alleging that defendants misrepresented their security practices and how they would use consumer information); *Educ. Research Ctr. of Am., Inc.; Student Marketing Grp., Inc.*, FTC Docket No. C-4079 (May 6, 2003) (consent order) (alleging that personal data collected from students for educational purposes was sold to commercial marketers); *The Nat'l Research Ctr. for College & Univ. Admissions*, FTC Docket No. C-4071 (Jun. 28, 2003) (consent order) (same); *Gateway Learning Corp.,* FTC Docket No. C-4120 (Sept. 10, 2004) (consent order) (alleging that company rented customer information to list brokers in violation of its privacy policy); *Vision I Props., LLC,* FTC Docket No. C-4135 (Apr. 19, 2005) (consent order) (alleging that a service provider disclosed customer information in violation of merchant privacy policies). *Sears Holdings Mgmt. Corp.*, FTC Docket No. C-4264 (Aug. 31, 2009) (consent order).

telling parents. The Commission's order prohibits the company from sharing information gathered from its monitoring software and requires the company to destroy any such information in its database of marketing information.[8]

Finally, in September, the Commission settled a case against US Search, a data broker that maintained an online service, which allowed consumers to search for information about others. The company allowed consumers to opt out of having their information appear in search results, for a fee of $10. 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.[9]

In addition to these privacy enforcement actions, the Commission has been aggressive on the data security front to ensure that companies protect the sensitive data they collect about consumers. In February 2011, three companies that resell consumers' credit reports agreed to settle FTC charges that they did not take reasonable steps to protect consumers' personal information, which allowed computer hackers to access more than 1,800 credit reports via their clients' computer networks. These are the first cases the FTC has brought against credit report resellers for their failure to ensure that the companies to whom they provide consumer reports maintain reasonable security.[10] The Commission alleged that the resellers violated the FCRA,

---

[8] *FTC v. Echometrix, Inc.*, No. CV10-5516 (E.D.N.Y. Nov. 30, 2010) (consent order).

[9] *US Search, Inc.*, FTC File No. 102 3131 (Sept. 22, 2010) (consent order accepted for public comment).

[10] *SettlementOne Credit Corp.,* File No. 082 3208; *ACRAnet, Inc.,* File No. 092 3088; and *Fajilan and Associates, Inc.*, File No. 092 3089 (Feb. 3, 2011) (consent orders accepted for public comment).

the Gramm-Leach-Bliley Safeguards Rule, and Section 5 of the FTC Act. The consent orders bar the companies from violating these laws, require them to implement comprehensive information security programs, and require them to obtain independent audits, every other year for 20 years.

B. Consumer and Business Education

The FTC has done groundbreaking outreach to businesses and consumers in the area of consumer privacy. For example, the Commission's well-known OnGuard Online website educates consumers about spam, spyware, phishing, peer-to-peer ("P2P") file sharing, social networking, laptop security, and identity theft.[11] The FTC has developed additional 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.[12] The publication includes information about how parents should talk to children about online privacy, sexting, and cyberbullying. In less than one year, the Commission already has distributed more than 7 million copies of *Net Cetera* to schools and communities nationwide. The Commission also offers specific guidance to young people concerning certain types of Internet services, including, for example, social networking and video and photo sharing.[13]

---

[11] *See* http://www.onguardonline.gov/topics/social-networking-sites.aspx. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alertaena Línea have attracted nearly 12 million unique visits.

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

[13] *See* http://www.onguardonline.gov/topics/social-networking-sites.aspx; http://www.onguardonline.gov/topics/net-cetera-mobile-phones.aspx.

Most recently, the FTC released a consumer education publication on the safe use of wi-fi hot spots.[14] The publication, available on the FTC and Onguard Online websites, explains that when using wireless networks, consumers should convey personal information only if it is encrypted – either through an encrypted website or a secure network. The piece notes that an encrypted website is one whose URL begins with "https", rather than "http"; it further notes that in order to be secure, a wi-fi network must be password-protected.

Business education is also an important priority for the FTC. For example, 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.[15] The FTC also develops business education materials to respond to specific emerging issues, such as a recent brochure on security risks associated with P2P file-sharing software.[16]

C. Policy and Rulemaking Initiatives

The Commission's efforts with respect to privacy include public workshops and reports to examine the implications of new technologies on consumer privacy. For example, in November 2007, the Commission held a two-day Town Hall event to discuss the privacy implications of online behavioral advertising.[17] Based upon the Town Hall discussions, staff released for public comment a set of proposed principles to encourage industry members to

---

[14] *See* http://www.onguardonline.gov/topics/hotspots.aspx.

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

[16] *See generally* http://business.ftc.gov/privacy-and-security.

[17] FTC Town Hall, *Ehavioral Advertising: Tracking, Targeting, & Technology* (Nov. 1-2, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml.

improve their behavioral advertising practices.[18] Thereafter, in February 2009, staff released a report ("OBA Report") setting forth the following revised principles based on the comments received: (1) transparency and consumer control; (2) reasonable security and limited retention for consumer data; (3) affirmative express consent for material retroactive changes to privacy policies; and (4) affirmative express consent for the use of sensitive data.[19]

The Commission also reviews its rules periodically to ensure that they are appropriately updated in light of changes in the marketplace. For example, the Commission is currently reviewing its rule implementing the COPPA and anticipates completing that review in the coming months.[20]

II. Privacy Roundtables and Report

The Commission also recently conducted a series of public roundtables on consumer privacy,[21] which took place in December 2009, and January and March 2010. The roundtables served to explore the effectiveness of current privacy approaches in addressing the challenges of the rapidly evolving market for consumer information, including consideration of the risks and

---

[18] *See* FTC Staff, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles* (Dec. 20, 2007), *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf.

[19] *See FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising* (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf, at 33-37, 46. The revisions primarily concerned the principles' scope and application to specific business models. *Id*. at 20-30.

[20] *See* http://business.ftc.gov/documents/coppa-rulemaking-and-rule-reviews; Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 17 Fed. Reg. 17089 (Apr. 5, 2010), *available at* http://www.ftc.gov/os/fedreg/2010/april/P104503coppa-rule.pdf.

[21] *See* Press Release, FTC, FTC to Host Public Roundtables to Address Evolving Privacy Issues (Sept. 15, 2009), *available at* http://www.ftc.gov/opa/2009/09/privacyrt.shtm.

benefits of consumer information collection and use; consumer expectations surrounding various information management practices; and the adequacy of existing legal and self-regulatory regimes to address privacy interests. Staff issued a preliminary privacy report in December 2010,[22] which discusses the major themes that emerged from these roundtables, including the ubiquitous collection and use of consumer data; consumers' lack of understanding and ability to make informed choices about the collection and use of their data; the importance of privacy to 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.[23]

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. 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. Based on these comments, the preliminary staff privacy report proposed a new framework to guide policymakers and industry as they consider further steps to improve consumer privacy protection.

---

[22] *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.

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

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. Companies also should implement and 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 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.

Second, the Commission 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 reflects the concept that consumers reasonably expect companies to engage in certain practices namely, 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," 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 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 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 through February 18, 2011. Close to 450 comments were received and staff expects to issue a final report this year.

B. Do Not Track

As noted above, the Staff Report included a recommendation to implement a universal choice mechanism for behavioral tracking, including behavioral advertising, often referred to as "Do Not Track."[24] Although behavioral tracking benefits consumers by helping support online content and services and allowing personalized advertising that many consumers value, the

---

[24] *See FTC Staff Report, supra note 22. See also* Rosch concurring statement, *id.*, in which 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. To clarify, Commissioner Rosch continues to believe that a variety of questions need to be answered prior to the endorsement of any particular Do Not Track mechanism.

practice remains largely invisible to most consumers. Some surveys[25] show that certain consumers who are aware of the practice are uncomfortable with it.[26] A recent USA Today/ Gallup poll found that 47% of consumers would like to choose which advertisers may deliver them targeted advertisements and 37% would like to receive no targeted advertisements at all.[27] In another poll, 80% of consumers supported a Do Not Track option.[28] In addition, according to a recent Wall Street Journal article, because of concerns that third-party tracking may be

---

[25] Consumer survey evidence, by itself, has limitations. For instance, the way questions are presented may affect survey results. Also, while survey evidence may reveal a consumer's stated attitudes about privacy, survey evidence does not necessarily reveal what actions a consumer will take in real-world situations. The Commission does not endorse the reliability or methodology of any surveys discussed herein.

[26] *See, e.g.*, *Transcript of December 7, 2009, FTC Privacy Roundtable,* Remarks of Alan Westin of Columbia University, at 93-94*, available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec2009_Transcript.pdf; *Written Comment of Berkeley Center for Law & Technology, Americans Reject Tailored Advertising and Three Activities that Enable It*, cmt. #544506-00113, *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00113.pdf; *Written Comment of Craig Wills, Personalized Approach to Web Privacy Awareness, Attitudes and Actions*, cmt. #544506-00119, *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00119.pdf; *Written Comment of Alan Westin*, *How Online Users Feel About Behavioral Marketing and How Adoption of Privacy and Security Policies Could Affect Their Feelings*, cmt. #544506-00052, *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00052.pdf; *see also Poll: Consumers Concerned About Internet Privacy*, Consumers Union, *available at* http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html.

[27] *See U.S. Internet Users Ready to Limit Online Tracking for Ads* (Dec. 21, 2010), *available at* http://www.gallup.com/poll/145337/internet-users-ready-limit-online-tracking-ads.aspx.

[28] *See* News Release, Consumer Watchdog, Americans Favor Broad Range Of Online Privacy Protections for Consumers (Jul. 27, 2010), *available at* http://www.consumerwatchdog.org/newsrelease/consumer-watchdog-poll-finds-concern-about-googles-wi-spy-snooping.

intrusive, some websites are increasing their scrutiny of such third-party tracking on their sites.[29]

In light of the concerns expressed about online tracking, the Staff Report recommended a Do Not Track mechanism. A robust, effective Do Not Track system would ensure that consumers can opt out once, rather than having to exercise choices on a company-by-company or transaction-by-transaction basis. Such a universal mechanism could be accomplished through legislation or potentially through robust, enforceable self-regulation.

The FTC repeatedly has called on stakeholders to develop and implement better tools to allow consumers to control the collection and use of their online browsing data.[30] Industry participants have begun to respond to this call. Two major browser vendors, Microsoft and Mozilla, have recently 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.[31] Just as important, the World Wide Web Consortium (W3C) has accepted a submission by Microsoft to consider a technical standard for a universal choice mechanism. The W3C announced an April 2011 workshop to begin the public dialogue with

---

[29] Jessica Vascellaro, *Websites Rein in Tracking Tools*, WALL ST. J., Nov. 9, 2010, *available at* http://online.wsj.com/article/SB10001424052748703957804575602730678670278.html.

[30] *See e.g.*, Do Not Track: Hearing before the Subcomm. On Commerce, Trade and Consumer Prot. of the H. Comm. On Energy and Commerce, 111th Cong. (Dec. 2, 2010), *available at* http://www.ftc.gov/os/testimony/101202donottrack.pdf (prepared statement of the FTC, Commissioner Kovacic dissenting).

[31] *See* Press Release, Microsoft, Providing Windows Customers with More Choice and Control of Their Privacy Online with Internet Explorer 9 (Dec. 7, 2010), *available at* http://www.microsoft.com/presspass/features/2010/dec10/12-07ie9privacyqa.mspx; Mozilla Blog, Mozilla Firefox 4 Beta, now including "Do Not Track" capabilities, http://blog.mozilla.com/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities/ (Feb. 8, 2011).

relevant stakeholders regarding how to incorporate do not track preferences into Internet browsing so websites can respect a user's preference not to be tracked.[32] Finally, just last week, Stanford's Center for Internet and Society and Mozilla jointly submitted a proposal to the Internet Engineering Task Force outlining a header-based Do Not Track mechanism and discussing how web services should respond to such a mechanism.[33]

The online advertising industry has also made progress in this area. For example, an industry coalition comprised of media and marketing associations, known as the Digital Advertising Alliance, has developed self-regulatory guidelines and an opt-out mechanism for behavioral advertising.[34] The coalition has developed an icon to display in or near targeted advertisements that links to more information and choices and has pledged to implement this effort industry-wide.[35] The coalition reports that adoption of the icon and simplified disclosures

---

[32] *See* W3C Blog, Do Not Track at W3C, http://www.w3.org/QA/2011/02/do_not_track_at_w3c.html (Feb. 24, 2011).

[33] *See* Do Not Track: A Universal Third-Party Web Tracking Opt Out (Mar. 7, 2011), *available at* http://tools.ietf.org/html/draft-mayer-do-not-track-00; *see also* http://firstpersoncookie.wordpress.com/2011/03/09/mozilla-makes-joint-submission-to-ietf-on-dnt/.

[34] *See* Press Release, Interactive Advertising Bureau, Major Marketing Media Trade Groups Launch Program to Give Consumers Enhanced Control over Collection and Use of Web Viewing Data for Online Behavioral Advertising (Oct. 4, 2010), *available at* http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-100410; Tony Romm and Kim Hart, Political Intel: FTC Chairman on Self-Regulatory Ad Effort, POLITICO Forums, http://dyn.politico.com/members/forums/thread.cfm?catid=24&subcatid=78&threadid=4611665 (Oct. 11, 2010).

[35] The coalition has stated that providing consumers with choices about online advertising is essential to building the trust necessary for the marketplace to grow. *See Interactive Advertising Bureau, supra* note 34.

grew dramatically at the end of last year.[36] In addition, Google has developed a browser add-on that can be used to block targeted advertisements from companies that participate in the Digital Advertising Alliance.[37]

These recent industry efforts to improve consumer control are promising, but they are still in the embryonic stage, and their effectiveness remains to be seen. As industry continues to explore technical options and implement self-regulatory programs, and Congress continues to examine Do Not Track, several issues should be considered. 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.[38]

---

[36] *See Written Comment of the Direct Marketing Assoc. Responding to Preliminary Staff Report*, cmt. #00449, at 21.

[37] *See* Google Chrome Web Store, Keep My Opt-Outs, *available at* https://chrome.google.com/webstore/detail/hhnjdplhmcnkiecampfdgfjilccfpfoe; *see also* Google Public Policy Blog, Keep your opt-outs http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html (Jan. 24, 2011).

[38] For example, consumers may believe they have opted out of tracking if they block third-party cookies on their browsers; yet they may still be tracked through Flash cookies or other mechanisms.

A Flash cookie, or a Flash local shared object, is a data file that is stored on a consumer's computer by a website that uses Adobe's Flash player technology. Like a regular http cookie, a Flash cookie can store information about a consumer's online activities. Unlike regular cookies, Flash cookies are stored in an area not controlled by the browser. Thus, when a consumer deletes or clears the cookies from his browser using tools provided through the browser, this may not delete Flash cookies stored on his computer.

Finally, it is important to emphasize what is meant by "tracking" as stakeholders continue to consider "Do Not Track" approaches. Consumers certainly may want to opt out of more than targeted advertising – they may want to opt out of the creation and use of behavioral profiles for any secondary purposes. For example, they may want to be sure that their browsing behavior is not used to make employment or insurance decisions about them. They may also want to opt out of having their browsing behavior sold to data brokers for unspecified future uses. At the same time, no system that allows for unrestricted web browsing can or should prohibit information collection entirely. As noted the Staff Report, information collection is necessary for fraud prevention and other commonly accepted practices, such as capping the number of times a consumer sees a particular advertisement. The limited nature of that collection, however, is qualitatively different from the collection of information to track and profile consumers as they browse the web. Given these considerations, 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 that are not commonly accepted.

Commission staff will monitor further industry innovation in this area, which may build upon existing industry initiatives and incorporate elements of the different mechanisms being proposed today.

Recently, a researcher released a software tool that demonstrates several technical mechanisms in addition to Flash cookies that websites can use to persistently track consumers, even if they have attempted to prevent such tracking through existing tools. *See* http://samy.pl/evercookie; *see also* Tanzina Vega, *New Web Code Draws Concerns Over Privacy Risks,* N.Y. TIMES, Oct. 10, 2010, *available at* http://www.nytimes.com/2010/10/11/business/media/11privacy.html.

III. Conclusion

Thank you for the opportunity to provide the Commission's views. We look forward to continuing this important dialogue with Congress and this Committee.