PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Do Not Track

Before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

December 2, 2010

Chairman Rush, Ranking Member Whitfield, and members of the Subcommittee, I am David Vladeck, Director of the Bureau of Consumer Protection of the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to present the Commission's testimony on Do Not Track.[1]

Privacy has been central to the Commission's consumer protection mission for forty years. During this time, the Commission's goal in the privacy arena has remained constant: to protect consumers' personal information and ensure that consumers have the confidence to take advantage of the many benefits offered by the ever-changing marketplace. Nevertheless, from time to time, the Commission has re-examined its approach to privacy to ensure that it keeps pace with changing technologies and business practices.

The latest effort in this process is a Commission staff report, released just this week, which sets forth a proposed 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 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. Next, it sets forth some highlights from the Commission staff's new report on consumer privacy. Finally, it discusses

---

[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 testimony) is premature. My oral presentation and responses are my own and do not necessarily reflect the views of the Commission or of any Commissioner.

the concept of Do Not Track.

I. The FTC's Efforts to Protect Consumer Privacy

A. Enforcement

The Commission has an aggressive privacy enforcement agenda. In the last fifteen years, it has brought 29 data security cases; 64 cases against companies for improperly calling consumers on the Do Not Call registry; 83 cases against companies for violating the Fair Credit Reporting Act ("FCRA");[2] 96 spam cases; 15 spyware cases; and 15 cases against companies for violating the Children's Online Privacy Protection Act ("COPPA").[3] 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 through legislative recommendations.[5]

In addition, the Commission has brought numerous cases against companies for violating the FTC Act by making deceptive claims about the privacy of the information they collect,

---

[2] 15 U.S.C. §§ 1681e-i.

[3] 15 U.S.C. §§ 6501-6508.

[4] 15 U.S.C. §§ 7701-7713.

[5] *See*, *e.g.*, Prepared Statement of the Federal Trade Commission Before the Subcomm. on Consumer Protection, Product Safety, and Insurance of the S. Comm. on Commerce, Science, and Transportation, 111th Cong. (Sept. 22, 2010), *available at* http://www.ftc.gov/os/testimony/100922datasecuritytestimony.pdf; Prepared Statement of the Federal Trade Commission Before the Subcomm. on Interstate Commerce, Trade, and Tourism of the S. Comm. on Commerce, Science, and Transportation Committee, 110th Cong. (Sep. 12, 2007), *available at* http://www.ftc.gov/os/testimony/070912reauthorizationtestimony.pdf.

which has the effect of undermining consumer choices on privacy. Below are four recent examples.

First, the Commission just settled 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 the information that it collected from children via this software to third parties for marketing purposes, without 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.

Second, this past September, the Commission announced 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 names 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.[6]

Third, this summer, the Commission alleged that the social networking service Twitter deceived its customers by failing to honor their choices to designate certain "tweets" as private.[7] On one level, Twitter is a traditional data security case the FTC charged that serious lapses in

---

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

[7] *Twitter, Inc.*, FTC File No. 092 3093 (June 24, 2010) (consent order accepted for public comment).

the company's data security allowed hackers to obtain unauthorized administrative control of Twitter, including access to private "tweets" and non-public user information. 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 privacy of communications, requires Twitter to maintain reasonable security, and mandates independent, comprehensive audits of Twitter's security practices.[8]

Finally, last year the Commission settled allegations that Sears violated Section 5 of the FTC Act by failing to disclose adequately the scope of consumers' personal information collected via software that Sears represented would merely track their "online browsing."[9] The

---

[8] Many of the Commission's earliest consumer privacy cases similarly held companies accountable for their privacy statements and practices. *See, e.g., GeoCities, Inc.*, 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.*, 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.*, 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*, Docket No. C-4071 (Jun. 28, 2003) (consent order) (same); *Gateway Learning Corp.,* 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,* Docket No. C-4135 (Apr. 19, 2005) (consent order) (alleging that a service provider disclosed customer information in violation of merchant privacy policies).

[9] *Sears Holdings Mgmt. Corp.*, FTC Docket No. C-4264 (Aug. 31, 2009) (consent order).

FTC charged that the software, in fact, monitored consumers' online secure sessions as well including those on third-party websites and collected information such as the contents of shopping carts, online bank statements, email headers and subject lines, drug prescription records, and other sensitive data. In addition to requiring that Sears destroy information previously collected, the settlement provides that if Sears advertises or disseminates tracking software in the future, it must clearly and prominently disclose the types of data the software monitors, records, or transmits and whether any of the data will be used by a third party. This disclosure must be made prior to installation of the tracking software and separate from any user license agreement.

The Commission also looks for opportunities short of formal law enforcement to ensure that companies keep their privacy promises. For example, this past summer, the Commission's Bureau of Consumer Protection sent a letter to individual stakeholders in XY Corporation, which operated a now-defunct magazine and website directed to gay male youth.[10] The letter expressed concern about these individuals' efforts to obtain and use old subscriber lists and other highly sensitive information including names, street addresses, personal photos, and bank account information from gay teens. The letter warned that selling, transferring, or using this information would be inconsistent with the privacy promises that were previously made to the subscribers, and may violate the FTC Act; thus, the letter urged that the data be destroyed. After receiving a copy of the FTC letter, the court overseeing bankruptcy proceedings involving the

[10] *See* Letter from David C. Vladeck to Peter Larson and Martin E. Shmagin (Jul. 1, 2010), *available at* http://www.ftc.gov/os/closings/100712xy.pdf.

XY Corporation ordered the destruction of the information.[11]

B. Consumer and Business Education

The FTC has done pioneering 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 file sharing, social networking, laptop security, and identity theft.[12]

The FTC has developed additional resources specifically for children, parents, and teachers to help kids 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.[13] 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 6 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,

---

[11] The Commission staff has issued similar types of letters in other matters involving privacy and data security. For example, earlier this year, it sent letters to companies that had experienced breaches of their computer networks through peer-to-peer file-sharing programs, urging them to review their security practices and take steps necessary to protect their information from unauthorized access. *See, e.g.,* FTC Press Release, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), *available at* www.ftc.gov/opa/2010/02/p2palert.shtm.

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

[13] *See* FTC Press Release, 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.

for example, social networking and peer-to-peer file ("P2P") sharing.[14]

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.

C. Policy Initiatives

The Commission's privacy work also includes 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.[16] Based upon the Town Hall discussions, staff released for public comment a set of proposed principles to encourage industry to improve their behavioral advertising practices.[17] 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)

---

[14] *See* http://www.onguardonline.gov/topics/social-networking-sites.aspx.

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

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

[17] *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.

affirmative express consent for the use of sensitive data.[18] This report was the catalyst for industry to institute a number of self-regulatory initiatives, discussed further below.

The Commission also recently conducted a series of public roundtables on consumer privacy,[19] which took place in December 2009, and January and March 2010. The report issued this week 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.

At the roundtables, stakeholders 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, 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 Commission staff released its report this week, proposing a new framework to guide policymakers and industry as they

---

[18] *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.

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

consider further steps to improve consumer privacy protection. Staff is seeking comment on the proposed new framework through January 2011 and expects to issue a final report in 2011.

II. The Proposed Framework

The proposed framework contains three main concepts. First, the Commission staff proposes 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, companies that collect and use small amounts of non-sensitive 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 proposes that companies provide choices to consumers about their data practices in a simpler, more streamlined manner than has been used in the past. 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 improving services offered, fraud prevention, legal compliance, and first-party marketing. Some of these practices, such as where a retailer collects 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. 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. The Commission supports such a mechanism, as discussed further below.

Third, the Commission staff proposes 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 consumer groups, regulators, and others can compare data practices and choices across companies, thus promoting competition among companies. The Commission staff also proposes 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 Commission staff believes that the extent of access should be proportional to both the sensitivity of the data and its intended use. In addition, 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 Commission staff proposes 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 facilitating competition on privacy across companies.

In addition to proposing these broad principles, the Commission staff is seeking comment from all interested parties to help guide further development and refinement of the proposed framework.

III. Do Not Track

In considering a uniform choice mechanism for online behavioral advertising, the Commission recognizes the benefits of such advertising, which helps support some of the online content and services available to consumers and allows personalized advertising that many consumers value.[20] At the same time, the practice continues to be largely invisible to consumers.

---

[20] *See* Comment of Microsoft Corporation at 1 (November 6, 2009), *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00020.pdf.

Some surveys show that certain consumers who are aware of the practice are uncomfortable with it.[21] In addition, according to a recent Wall Street Journal article, because of concerns that third party tracking may be intrusive, some websites are increasing their scrutiny of such tracking on their sites.[22] To address these concerns, the Commission, consumer groups, and leading industry participants[23] have supported the idea of improved transparency and consumer choice over the practice of tracking consumers to serve targeted advertisements.

---

[21] *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.

One laboratory study demonstrates that consumers are willing to pay more to shop at websites that have better privacy policies. Serge Egelman, Janice Tsai, Lorrie Faith Cranor and Alessandro Acquisti, *Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators*, Carnegie Mellon University, *available at* http://www.guanotronic.com/~serge/papers/chi09a.pdf. Although the study included only consumers who stated they had privacy concerns about shopping online, it showed that these consumers were willing to pay more for privacy.

[22] Jessica Vascellaro, *Websites Rein in Tracking Tools*, Wall St. J., Nov. 9, 2010, *available at* online.wsj.com/article/SB10001424052748703957804575602730678670278.html.

[23] *See* Press Release, Interactive Advertising Bureau Press Release, 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.

Indeed, the FTC repeatedly has called on stakeholders to create better tools to allow consumers to control the collection and use of their online browsing data. In response, several companies have developed new tools that allow consumers to control their receipt of targeted advertisements and to see and manipulate the information companies collect about them for targeting advertisements.[24] An online certification company has launched a pilot program to display an icon on advertisements that links to additional information and choices about behavioral advertising.[25] An industry group comprised of media and marketing associations has developed self-regulatory guidelines and an opt-out mechanism for behavioral advertising.[26] This group has formed a coalition to develop an icon to display in or near targeted advertisements that links to more information and choices. The coalition has pledged to implement this effort industry-wide.[27]

In addition, each of the major browser vendors offers a mechanism to limit online tracking with varying scope and ease of use. These browser vendors recognize the importance of offering consumers choices in this area.

---

[24] *See, e.g., Google's Ad Preferences Manager*, Google, http://www.google.com/advertisements/preferences (last visited Oct. 21, 2010); *Yahoo's Ad Interest Manager*, Yahoo http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/ (last visited Oct. 21, 2010).

[25] *See* Press Release, TRUSTe, TRUSTe Lanches TRUSTed Ads Privacy Platform (Oct. 4, 2010), *available at* http://www.truste.com/about_TRUSTe/press-room/news_truste_trustedads.html.

[26] *See supra* note 23; Tony Romm and Kim Hart, *Political Intel: FTC Chairman on Self-Regulatory Ad Effort*, POLITICO Forums (Oct. 11, 2010), *available at* http://dyn.politico.com/members/forums/thread.cfm?catid_24&subcatid_78&threadid_4611665.

[27] 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 supra* note 23.

While some industry members have taken positive steps toward improving consumer control, there are several concerns about existing consumer choice mechanisms. First, industry efforts to implement choice on a widespread basis have fallen short. The FTC has been calling on industry to implement innovations such as "just-in-time" choice for behavioral advertising since 2008. Although there have been developments in this area as described above, an effective mechanism has yet to be implemented on an industry-wide basis. Second, to the extent that choice mechanisms exist, consumers often are unaware of them, and click-through rates remain low.[28] For example, consumers are largely unaware of their ability to limit or block online tracking through their browsers, in part because these options may be difficult to find; further, those consumers who know about these options may be confused by the lack of clarity and uniformity among the browsers in how choices are presented and implemented.

Third, existing mechanisms may not make clear the scope of the choices being offered. It may not be clear whether these mechanisms allow consumers to choose not to be tracked, or to be tracked but not delivered targeted advertising. Also, consumers may believe that opting out at one company or website will prevent tracking or will block personalized advertising or even all advertising everywhere. Finally, consumers are not likely to be aware of the technical limitations of existing control mechanisms. For example, they may believe they have opted out of tracking if they block third-party cookies on their browsers; yet they may still be tracked

---

[28] *Transcript of December 7, 2009, FTC Privacy Roundtable*, Remarks of Alan Davidson of Google, at 113, *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec2009_Transcript.pdf.

through Flash cookies or other mechanisms.[29]

Given these limitations, the Commission supports a more uniform and comprehensive consumer choice mechanism for online behavioral advertising, sometimes referred to as "Do Not Track." The most practical method of providing uniform choice for online behavioral advertising would likely involve placing a setting similar to a persistent cookie on a consumer's browser, and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements. To be effective, there must be an enforceable requirement that sites honor those choices.[30]

Such a mechanism would ensure that consumers would not have to exercise choices on a company-by-company or industry-by-industry basis, and that such choices would be persistent. It should also address some of the concerns with the existing browser mechanisms, by being

---

[29] 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, the consumer does not delete Flash cookies stored on his computer. Instead, the consumer must know that Flash cookies exist, go to the Adobe website, and follow the instructions provided there to have them removed.

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.

[30] As is often true with online privacy, it may be difficult for consumers to ascertain which parties are not respecting their choices. However, technical methods exist that may reduce the ability of sites to track users, or that may identify parties that do not respect consumer choices not to be tracked for behavioral advertising. The Commission believes these tools could be effective to help monitor and enforce a uniform choice mechanism.

more clear, easy-to-locate, and effective, and by conveying directly to websites the user's choice to opt out of tracking. Such a universal mechanism could be accomplished through legislation or potentially through robust, enforceable self-regulation.

If Congress chooses to enact legislation, the Commission urges Congress to consider several issues.

First, any such mechanism 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.

Second, such a mechanism should be different from the Do Not Call program in that it should not require a "Registry" of unique identifiers. In the context of the Do Not Call program, each telephone already has a unique identifier in the form of a phone number. In contrast, there is no such persistent identifier for computers, as Internet Protocol ("IP") addresses[31] can change frequently. Rather than creating such an identifier in this context, which would raise significant privacy issues,[32] the Commission recommends a browser-based mechanism through which consumers could make persistent choices.[33]

Third, some companies currently offer consumers a choice between opting out of online behavioral advertising altogether or affirmatively choosing the types of advertising they receive.

---

[31] An Internet Protocol address (IP address) is a number that is assigned to any device that is connected to the Internet.

[32] A new identifier would be yet another piece of personally identifiable information that companies could use to gather data about individual consumers.

[33] Although the practicalities of a proposed choice mechanism here would differ from Do Not Call, it would be similar in that it would allow consumer to express a single, persistent preference regarding advertising targeted to them.

For example, at the roundtables, one company described how it shows consumers the categories of advertising associated with them, and allows them to de-select those categories and select additional ones.[34] The panelist noted that, when given this option, rather than opting out of advertising entirely, consumers tend to choose to receive some types of advertising.

As this example illustrates, consumers may want more granular options. We therefore urge Congress to consider whether a uniform and comprehensive choice mechanism should 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.

Fourth, it is imperative that any universal choice mechanism be understandable and simple. In addition to being easy to find and use, such a mechanism should make it clear to consumers exactly what they are choosing and if there are limitations to that choice.

Finally, if Congress does choose to enact legislation, the Commission requests the authority to conduct rulemaking under the Administrative Procedure Act and to obtain civil penalties to enforce the legislation. Rulemaking authority is important so that the Commission can have flexibility in an area where technology evolves rapidly. And the ability to fine violators would provide a strong incentive for companies to comply with any legal requirements, helping to deter future violations.

---

[34] *Transcript of December 7, 2009, FTC Privacy Roundtable*, Remarks of Alan Davidson of Google, at 101-02, *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec2009_Transcript.pdf.

V. Conclusion

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