Keynote Address by Commissioner Edith Ramirez
Federal Trade Commission

28th Annual Institute on
Telecommunications Policy &Regulation
Washington, D.C.

December 9, 2010

Good afternoon. Thank you for inviting me to be here today. As an FTC Commissioner, I appreciate the opportunity to speak to lawyers who practice more often in front of the Federal Communications Commission than the FTC. Both the FTC and FCC deal with technology-related questions of law and policy, and I'd like to speak to you about one such issue today: online privacy.[1]

Privacy has long been central to the FTC's consumer protection work, and today it is at the forefront of our agenda. There is good reason for that. With advances in online behavioral advertising, the exploding popularity of social networking, and the proliferation of smartphones, never before has so much information about consumers been collected, combined, and sold. And it's all happening in the blink of an eye. In the course of a single day, information about any one of us might be invisibly collected and shared in the following ways:

- As you browse the Internet, online advertising networks gather information about the websites you visit, the searches you run, the content you click on, and the purchases you make. This information is added to an ever-growing profile that advertising networks use to serve you targeted ads as you move from website to website;

- As you use your smartphone, information about your location might be shared not only with your carrier, but also with third-party applications and advertisers; and

- As you spend time on a social networking site, information that you and your friends post is likely shared with third-party applications.

[1] My remarks today are my own and may not reflect the views of the Commission as a whole or any other Commissioner.

In light of this non-stop and invisible collection and sharing of consumer information, the FTC last year embarked on an intense examination of today's privacy challenges. Last week, the FTC issued a preliminary staff report outlining a new approach to consumer privacy, which includes the creation of a universal Do Not Track mechanism. We are seeking comment on this new privacy framework, and will issue a final report next year. Today, I would like to discuss a few of the report's main concepts, including Do Not Track.

Overview of FTC's Privacy Enforcement

The FTC has been the nation's chief privacy agency for 40 years. Its main source of authority is Section 5 of the FTC Act, which prohibits deceptive and unfair commercial acts or practices. The FTC also enforces a number of focused privacy laws, including the Fair Credit Reporting Act, the Children's Online Privacy Protection Act (or COPPA), CAN-SPAM, and Do Not Call. The FTC has a strong track record of enforcement in this arena. In the last decade, it has brought approximately 200 data security, Do Not Call, spam, spyware, and COPPA cases. And I expect you will see more privacy enforcement actions in the coming months.

Preliminary FTC Staff Report: A New Approach to Privacy

The FTC staff report issued last week offers a number of ideas to help Congress as it considers privacy issues, and to guide and motivate businesses as they seek to develop better privacy practices. Although the report's call for a do not track system has generated the most attention, the report sets forth a comprehensive approach to today's wide-ranging privacy threats. I would like to touch on a few of the report's key concepts and recommendations.

The first issue I want to discuss is the changing nature of online anonymity. There is no longer a sharp line between personally identifiable information or "PII" —such as a consumer's name, address, or Social Security number — and other information. As it becomes increasingly

possible to piece together bits of data from disparate sources to identify an individual, information can no longer be easily classified as either anonymous or not. For that reason, the framework extends to any data that can be reasonably identified with an individual, computer, or other device.

The erosion of a bright-line between PII and other data also underlies many of the FTC's conclusions. It is in large part because ostensibly anonymous information can now often be linked to a particular person that stronger privacy protection is needed.

The ability to identify purportedly anonymous users has been vividly illustrated by two widely-reported incidents that you may remember. In 2006, AOL released to the public 20 million search queries of over 650,000 AOL users. AOL's intentions were good — it released the data for use by academic researchers. And to keep its customers anonymous, AOL stripped out consumers' names. This offered little protection, however, and the New York Times was able to link supposedly anonymous consumers with their search histories.[2]

Similarly, in 2008, Netflix publicly released certain data about its customers' movie queues so that researchers could improve its algorithm for recommending films. Netflix sought to anonymize the data by stripping it of names and other direct identifying information. Nonetheless, researchers using public information were able to identify specific Netflix customers and associate information about the films they had rented.[3] Some researchers report

[2] Michael Barbaro & Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, *available at* http://www.nytimes.com/2006/08/09/technology/09aol.html.

[3] *See* Arvind Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets*, The Univ. of Texas at Austin, http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf; *see also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); Steve Lohr, *How Privacy Vanishes Online*, N.Y. TIMES, Mar. 16, 2010, *available at* http://www.nytimes.com/2010/03/17/technology/17privacy.html?scp=2&sq=netflix%20privacy%20anonymous&st=cse.

that all that is needed to uniquely identify one individual is 33 "bits" of information.[4] In fact, some researchers say that you can zero in on a person with only their birthdate, zip code, and gender.[5] Developments like these have transformed what it means to be anonymous.

This new reality leads to the first key recommendation of the report—"Privacy by Design." Privacy by design means that companies should build privacy protections into their everyday business practices and products. Good data practices are also an essential element of privacy by design. For example, companies should collect only the data they need for a specific business purpose; they should retain that data only as long as necessary to fulfill that purpose; and they should then safely dispose of data that is no longer being used. Privacy by design is not a new idea,[6] but it is one that needs to be deployed on a systematic basis.

The report also recommends giving consumers choice over data practices in a simple and clear way. Privacy policies today impose too heavy a burden on consumers to locate, read, and understand documents that even many of us lawyers would find confusing. This needs to change. Information should be presented in plain English, and, where possible, on a "just-in-time" basis—at the moment when consumers are about to provide their information. For example, before a consumer's location is shared with a mobile app, the consumer could be asked in a few words whether she approves this disclosure.

---

[4] *See* Emily Steel & Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, WALL ST. J., Aug. 4, 2010, *available at* http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html.

[5] *See, e.g.*, Dave Yates, Mark Shute, & Dana Rotman, *Connecting the Dots: When Personal Information Becomes Personally Identifying on the Internet*, Proceedings of the Fourth International AAAI Conference on Weblogs and Social Media, (2010).

[6] Privacy by Design is an approach advocated by Ann Cavoukian, Ph.D., the Information and Privacy Commissioner of Ontario. *See Privacy by Design*, http://www.privacybydesign.ca.

The third recommendation is transparency. Companies should do a much better job of bringing their data practices out into the open. One way to do that is through just-in-time notices. We do not, however, propose scrapping comprehensive privacy policies altogether. Such policies should exist in addition to shorter, just-in-time notices. But they should be clearer and standardized, so privacy polices of different companies can be compared at a glance.

Like many others, I would also like to see companies compete more on privacy.[7] The FTC is charged with promoting both competition and consumer protection, and spurring competition on privacy is an idea that holds particular appeal to an FTC commissioner. One factor contributing to the lack of competition on privacy is the invisible nature of most information collection and sharing. If consumers do not know how companies are using their information, then they cannot consider privacy when choosing among competing firms.

Clear and standardized privacy notices that can be compared at a glance should enhance consumers' ability to compare privacy practices across companies and could stimulate competition on privacy. And with standardized privacy notices, perhaps one day Consumer Reports or other groups will rate companies on their practices, giving businesses further incentive to compete on privacy.

Do Not Track

I also want to spend a few minutes discussing Do Not Track, which is one way to give consumers more choice in connection with online behavioral advertising.

Let me begin with a brief description of how online behavioral advertising works: When a consumer visits a website, an online advertising network installs a tracking file. The file —

[7] *See, e.g.*, Commissioner Pamela Jones Harbour, Concurring Statement Regarding Staff Report, "Self-Regulatory Principles for Online Behavioral Advertising," at 7-8 (Feb. 2009), *available at* http://ftc.gov/speeches/harbour.shtm.

usually a cookie — assigns the computer a unique ID number. Later, when the user visits other websites affiliated with the same ad network, information about the user's online actions are recorded. Over time, the network builds a detailed profile of the user's online activities, used to show ads tailored to the user's perceived interests.

Numerous surveys show some level — often quite high — of consumer discomfort with online tracking.[8] Of course, online tracking is not new. But the methods that companies use to capture information about consumers are becoming smarter and more powerful. For example, some online advertising networks now use tools, like web beacons, to scan in real time what consumers are doing on a website, including what they type or where they place their mouse.[9] Likewise, websites, by using computer "fingerprinting" technology, now gather and combine

[8] *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; Consumers Union, Press Release, *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy* (Sept. 25, 2008), *available at* http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html; Harris Interactive Inc., Press Release, *Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles* (Apr. 10, 2008), *available at* http://www.harrisinteractive.com/harris_poll/index.asp?PID=894; TRUSTe, Press Release, *TRUSTe Report Reveals Consumer Awareness and Attitudes About Behavioral Targeting* (Mar. 26, 2008), *available at* http://www.truste.org/about/press_release/03_26_08.php.

[9] *See* Julie Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., Jul. 30, 2010, *available at* http://online.wsj.com/article/SB10001424052748703940904575395073512.

information about a consumer's web browser configuration to uniquely identify and track consumers.[10]

Consumers may have once been able to control online behavioral advertising by blocking or deleting third-party cookies. But this technique does not disable Flash cookies, computer fingerprinting, or other new tracking tools. And, a recent news report indicates that some businesses are developing services to match people's real names with the pseudonyms they use on blogs or social networking sites.[11] The CEO of an Internet marketing firm has recently described a "sea change" in the industry, with advertisers wanting to "buy access to people, not Web pages."[12]

Is this really a problem? In the physical world, we would certainly never tolerate someone following us around and recording our every move — in fact, we might call that stalking. Many online marketers respond by emphasizing that the virtual world is different, because they do not collect or maintain consumer names or other PII. And it is different, but that gap is narrowing. As I have already discussed, it has become increasingly possible to identify specific individuals from ostensibly anonymous data. And there are few legal or other limits on what information is collected or how it is used.

There may be a tipping point where so much detailed information about consumers is being collected and shared among so many entities, with no real limits on its use, that consumer

---

[10] *See* Julia Angwin & Jennifer Valentino-DeVries, *Race is on to 'Fingerprint' Phones, PCs*, WALL ST. J., Nov. 30, 2010, *available at* http://online.wsj.com/article/SB10001424052748704679204575646704100959546.html.

[11] *See* Julia Angwin & Steve Secklow, *'Scrapers' Dig Deep for Data on Web*, WALL ST. J., Oct. 12, 2010, *available at* http://online.wsj.com/public/page/what-they-know-digital-privacy.html?mod=quicklinks_whattheyknow.

[12] Julie Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., Jul. 30, 2010, *available at* http://online.wsj.com/article/SB10001424052748703940904575395073351.

trust in the Internet is seriously eroded. It is therefore, ultimately, in websites' and advertisers' own interest to provide greater transparency about their privacy practices and to give consumers greater control over what data about them is collected and how it is used. Do Not Track, which is supported by four FTC Commissioners, is one way to give consumers an easy, universal way to control the monitoring of their online activities and ensure their trust remains intact.

Opponents have raised several main objections. First, some argue that creating a list or registry of consumers who do not want to be tracked would create privacy problems of its own. Unlike Do Not Call, Do Not Track would not involve a list or registry of consumers. The FTC is also not calling for a centralized database run by the government. Rather, one way a Do Not Track system could be implemented is through a persistent setting on the consumer's browser that would communicate the consumer's tracking preferences, via a Do Not Track header, to each website the consumer visits. Web servers would see the Do Not Track header and would then refrain from both collecting information about the computer user and serving targeted ads to him or her. But we are not wedded to any specific approach; and FTC staff is seeking comment on how best to implement a universal do not track mechanism.

Second, some argue that industry already offers adequate opt-out choices. I, however, do not believe the status quo is acceptable. Since 2008, the FTC has been calling for industry to give consumers better choices for behavioral advertising. It is now nearly 2011, and consumers still have to navigate their way to multiple sites to exercise limited opt-out choices. Moreover, these tools only allow users to block the *receipt* of targeted ads, but not the *collection* of information about them. That is a crucial shortcoming. Likewise, the existing tools do not block the collection of information through Flash cookies or computer fingerprinting, among other more recent tracking mechanisms. And, although browsers offer the ability to limit tracking, few

consumers use these features, perhaps because the choices are not uniform, clear, or widely-understood.

Third, some claim that Do Not Track would undermine the availability of free online content and services. I am keenly aware that advertising helps support a great deal of Internet content, and that targeted ads command a premium. I also recognize that online behavioral advertising results in personalized ads that many consumers value and prefer.

I nonetheless believe this concern about Do Not Track is overstated. Recent research sponsored by an industry coalition, the Digital Advertising Alliance, shows that consumers feel more positively towards brands that give them greater transparency and control, including the ability to opt-out.[13] Further, this industry coalition has acknowledged that consumer choice about online advertising is essential to building the trust necessary for the marketplace to grow.[14]

I also believe that Do Not Track should not be all or nothing. In my view, consumers should be able to make more precise choices about the information that is collected and the kind of targeted ads they are shown. For example, some consumers may be comfortable receiving ads based on their interest in yoga or hiking, but may not be comfortable with companies collecting or using demographic data about them. A well-designed intermediate option would give consumers more control, while promoting a high level of continued participation in online behavioral advertising.

---

[13] *See* Digital Advertising Alliance, *Consumer Interactions with In-Ad Notice*, at 7-13, Nov. 3, 2010, *available at* http://cdn.betteradvertising.com/misc/consumer%20impact%20of%20ad%20notice%2011_11.pdf.

[14] *See* 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.

While I do not believe Do Not Track poses a serious threat to industry, if industry members or others believe that Do Not Track is not the answer, then I am eager to hear what they believe would address the growing threats to consumer privacy. There is frenzied competition to meet advertisers' demand for more and more data about consumer behavior and interests. Consumers need a strong counterweight to that pressure to capture and mine information about their moment-to-moment thoughts and actions online.

The Commission has not yet taken a position on whether Do Not Track should be accomplished via legislation or robust self-regulation. Industry has an opportunity to give consumers an effective, universal opt-out tool. I am encouraged that earlier this week, in response to the FTC's report, Microsoft announced a plan to allow consumers to block tracking by selected sites.[15] Although we have yet to see how this will develop, it is certainly a positive step. For the moment, the ball is in industry's court to deploy a Do Not Track tool that obviates the need for legislation.

Conclusion

In closing, the release of the FTC staff report last week was a significant milestone. The FTC's goal has always been, and remains, to protect consumers' personal information and ensure they have the confidence to take advantage of the marketplace. The process for determining what policies will best advance that goal is by no means over, and we look forward to a continuing dialogue with all stakeholders.

Thank you.

[15] Tanzin Vega, *Microsoft, Spurred by Privacy Concerns, Introduces Tracking Protection to Its Browser*, N.Y. TIMES, Dec. 7, 2010, *available at* http://www.nytimes.com/2010/12/08/business/media/08soft.html.