Remarks of Commissioner Maureen K. Ohlhausen
NAI Summit: Third Parties and the Future of the Internet
New York City, NY
May 21, 2013

Thank you for that kind introduction, Will. It is an honor to be the opening keynote speaker at NAI's Inaugural Member Summit. I reviewed your agenda for the Summit, and you have a day packed with great speakers on important and timely topics related to the current debate on online behavioral advertising. As some of you may know, Marc Groman and I were colleagues at the FTC several years ago. He served as the first Chief Privacy Officer at the FTC, which is tasked with the protection of consumer privacy, and so he brings a lot of knowledge and experience to your organization. I also commend you for attending today's event. We are in the midst of a critical policy debate that will determine, in large part, the future of not just OBA but also the direction of the business model for supporting free web content through interest-based advertising. It is critically important that policymakers and industry work cooperatively to make sure that we get it right. My comments today will focus on the importance of self-regulation to advance consumer privacy. My remarks are my own and do not necessarily reflect the views of my colleagues on the Commission.

Background

Since the emergence of e-commerce in the mid-1990s, the online marketplace has grown at remarkable speed, continually accelerating and evolving to create new business models that allow greater interactivity between consumers and online companies. This expanding marketplace has provided many benefits to consumers, including free access to rich sources of information and the convenience of shopping for goods and services from home. At the same time, the ease with which companies can collect and combine information from consumers online has raised questions and concerns about consumer privacy.

One of the reasons the FTC is such an effective agency is that we use all of our tools to address issues within our jurisdiction, and privacy is no exception. Although law enforcement is at the core of the FTC's mission, that work is augmented by our business and consumer outreach and education, and our research and study initiatives. In a perfect world, it would not be necessary to bring cases—every company and individual would voluntarily comply—but that will never be reality. But by bringing cases, publicizing our law enforcement work, educating businesses on how to comply with the law, holding workshops and releasing

reports on best practices, and informing consumers on how to avoid being victims of fraud, the FTC can maximize its effectiveness and reach.

For almost two decades, the Federal Trade Commission has worked to understand the online marketplace and the privacy issues it raises for consumers by hosting numerous public workshops, issuing reports on online data collection practices, monitoring industry self-regulatory efforts, and closely following technological developments affecting consumer privacy. As part of this effort, the Commission has examined online behavioral advertising on several occasions. In November 2007, the FTC held a two-day "Town Hall," which brought together numerous interested parties to discuss online behavioral advertising in a public forum.[1] Following the Town Hall, FTC staff released for public comment a set of proposed principles designed to serve as the basis for industry efforts to address privacy concerns in this area.[2] Specifically, the principles provide for transparency and consumer control and reasonable security for consumer data. They also call on companies to obtain affirmative express consent from consumers before they use data in a manner that is materially different than promised at the time of collection and before they collect and use "sensitive" consumer data for behavioral advertising.

In March 2012, just before I started as a Commissioner, the Commission released "Protecting Consumer Privacy in an Era of Rapid Change," a comprehensive report that included recommendations for companies handling consumer data.[3] Although I do not agree with everything in the report—especially the call for additional, baseline privacy legislation—I do support as best practices many of the recommendations for protecting privacy, including:

- **Privacy by Design** – companies should build in consumer privacy protections at every stage in developing their products. These protections include reasonable security for consumer data, limited collection and retention of such data, and reasonable procedures to promote data accuracy;

- **Simplified Choice for Businesses and Consumers** – recognizing that there is no single best way to offer notice and choice in all circumstances,

[1] *See* Fed. Trade Comm'n, *Ehavioral Advertising, Tracking, Targeting & Technology* (Nov. 2, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml.
[2] *See* FED. TRADE COMM'N, ONLINE BEHAVIORAL ADVERTISING, MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES (2007), *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf.
[3] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

companies should adopt notice and choice options that appropriately reflect the context of the transaction and/or the relationship the company has with the consumer.

- **Greater Transparency** – companies should disclose details about their collection and use of consumers' information and provide consumers access to the data collected about them.

In addition to policy efforts and reports, the FTC has been a very active force in the privacy area. As I mentioned, I do not currently support a baseline privacy bill though I'm not against new privacy legislation *per se*. I hold this position largely because I believe that our current authority has been sufficient to reach all of the conduct I've identified in which FTC action was warranted. Until I become aware of a statutory gap, I do not see the purpose of enacting additional legislation in this area. The fact that the FTC has brought over 100 spam and spyware cases[4] and over 40 data security cases[5] under Section 5[6] suggests to me that we have the authority we need to be an effective law enforcement presence.

In the areas of privacy and data security, the Commission uses its deception authority in cases where a company makes a representation to consumers about the collection and/or use of their personal data but it fails to keep that promise.[7]

By contrast, the Commission's unfairness authority does not require a representation to consumers but instead focuses on the consumer harm that an act or practice may cause. The Commission's unfairness statement requires that for the Commission to find an act or practice unfair, the harm it causes must be substantial, it must not be outweighed by any offsetting consumer or competitive benefits, and the consumer could not have reasonably avoided the harm.[8]

The Commission's unfairness statement specifically identifies financial, health, and safety harms as varieties of harm that the Commission should consider

---

[4] Press Release, Fed. Trade Comm'n, *FTC Testifies on Protecting Consumers' Privacy* (Jul. 14, 2011), *available at* http://www.ftc.gov/opa/2011/07/privacy.shtm.

[5] *See, e.g.*, Fed. Trade Comm'n, Bureau of Consumer Protection, *Business Center Legal Resources*, http://business.ftc.gov/legal-resources/29/35 (describing data security cases).

[6] 15 U.S.C. § 45 (2012).

[7] *See generally* FED. TRADE COMM'N, FTC POLICY STATEMENT ON DECEPTION (1983), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

[8] FED. TRADE COMM'N, FTC POLICY STATEMENT ON UNFAIRNESS (1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

substantial.[9] It further states that emotional impact and more subjective types of harm are not intended to make an injury unfair.[10]

The Commission's deception and unfairness standards are effective and flexible complements. Unfairness provides a strong baseline of protection for consumers who suffer a substantial harm from the misuse of their personal information, regardless of whether the entity using the information made a promise to the consumer. Consumers who wish for a higher standard of protection for their information or wish to share less information can seek out businesses that promise a higher standard of care that matches the consumers' preference. This allows consumers to express their varying preferences and encourages companies to compete on the basis of privacy protections offered. If a company does not live up to its promises, the FTC can bring a case on deception grounds.

Asking the Right Question

Turning to the debate over OBA, I am both amused and frustrated by some of the voices in the privacy debate. The FTC is charged with protecting one constituency: consumers. Certainly not all consumers are the same, and the privacy debate is a great example of an issue on which there are differing views on the right level of protection for consumer data. But, too often, the debate takes place on a superficial level. Not many consumers will respond in a survey that they don't care about the privacy of their personal information. But I doubt that result can be reasonably extrapolated to say that most consumers object to OBA.

I saw the results of a recent Zogby Analytics poll commissioned by the Digital Advertising Alliance in which only 4 percent of respondents said they are concerned about behavioral targeting.[11] According to the poll, 40 percent preferred that all of their ads be targeted, and 70 percent said that they prefer at least some of their ads be tailored directly to their interests.[12] Many consumers place great value on the availability of online advertising, and 75 percent of the poll's respondents said they prefer free content, supported by ads, compared to 10 percent who stated they would rather pay for ad-free content.[13]

---

[9] *Id.*
[10] *Id.*
[11] Zogby Analytics, *Interactive Survey of US Adults* at 9 (Apr. 2013), *available at* http://www.aboutads.info/resource/image/Poll/Zogby_DAA_Poll.pdf.
[12] *Id.* at 6.
[13] *Id.* at 2.

My position is that both groups of consumers should have options that comport with their preferences. The first question for a policymaker should be whether those options are available to consumers through products or services or through industry self-regulation.

Many companies are now developing products that cater directly to consumers with heightened privacy preferences. In the area of search, DuckDuckGo offers consumers the ability to search the web anonymously by not tracking the query activity of their users.[14] Without the raw data of a user's search history, search results are less tailored to a consumer's preferences, but privacy is preserved. The extensibility of the modern browser allows developers to incorporate privacy protections into consumers' everyday browsing. A wide range of privacy and security protection add-ons are available for all of the major Internet browsers.

These are just a few examples of a wide range of available products that allow consumers to tailor their online services to better reflect their personal balance between privacy and advertising relevance.

Self-regulation can also offer consumers more privacy choices. The best self-regulatory programs are nimble, keeping pace with rapid changes in technology and business practices in ways legislation and regulation cannot. The NAI demonstrates this benefit of self-regulation, evolving to take into account changes in data collection and use practices, technologies, and public policy. For example, I was pleased to see the NAI release an updated Code of Conduct last week and also to see the NAI address the collection and use of data from mobile apps for the first time.[15] I hope that having the NAI establish and enforce standards for mobile advertising will raise the privacy bar in the rapidly growing mobile advertising market. I know from my meetings with NAI staff that you all are giving serious consideration to emerging technologies and will work to ensure that all technologies used by NAI member companies provide users transparency and control. This is exactly what we want to encourage.

I also commend the NAI's efforts to think creatively about the application of fair information practice principles in an ever-changing digital landscape. Through

---

[14] *See* Ryan Singel, *DuckDuckGo Challenges Google on Privacy (With a Billboard)*, WIRED (Jan. 19, 2011), http://www.wired.com/business/2011/01/duckduckgo-google-privacy/.

[15] Network Advertising Initiative, *Network Advertising Initiative Releases Final 2013 Code of Conduct for Interest-Based Advertising* (May 16, 2013), *available at* http://www.networkadvertising.org/sites/default/files/2013_nai_code_pr.pdf.

these efforts, the NAI encourages responsible data management across the entire third-party industry.

Self-regulation works best when it is backed up by serious compliance efforts and tough enforcement. And that's why the keystone of the NAI's self-regulatory framework is a comprehensive compliance program. I know this work is not easy for NAI staff or for your companies, and that it includes hundreds of hours in annual reviews and ongoing technical monitoring. This work improves the overall health of the online advertising industry by ensuring that companies live up to the promises they make to abide by the NAI Code. It also helps to spread best practices that go above and beyond the NAI Code throughout NAI membership. At times, this may seem like a thankless effort, but I assure you that it is not. When a company violates the NAI Code, they know that they will be subject to public naming or sanctions procedures. The work the NAI does to correct minor issues before they become serious problems and to enforce its Code of Conduct frees the FTC and other enforcement agencies to focus on egregious actors. These factors make NAI a great partner in the effort to get it right.

Do Not Track

Other self-regulatory efforts are also underway. Like many of you, I've watched with great interest the current effort of the World Wide Web Consortium (W3C), an Internet standards-setting entity, to create an international, industry-wide standard for Do Not Track, working to make a system that would operate in both desktop and mobile settings. The W3C's recent meeting in San Francisco seems to have made some progress, but reports raise doubts about whether the process will ultimately produce an agreement. I am closely monitoring the situation while also evaluating the ramifications of different outcomes for consumers and competition. I believe, however, that a voluntary, self-regulatory process should operate without undue government involvement. Otherwise, industry may lose the incentive to participate and instead take a wait and see attitude about whether Congress would ever impose such requirements through legislation.

Intersection of Competition and Consumer Protection

I am also concerned that too often privacy is viewed solely as a consumer protection issue. I believe that privacy, like most issues under FTC jurisdiction, must also be viewed through a competition lens if we are to reach the best outcome for consumers. For example, new privacy restrictions may have an effect on

competition by favoring entrenched entities that already have consumer information over new entrants who need to obtain such information, or encouraging industry consolidation for purposes of sharing data. As a competition agency, the FTC should be sensitive to these concerns as well.

The Commission has consistently recognized the crucial role that truthful non-misleading advertising plays in fostering competition between current participants in the market and lowering entry barriers for new competitors. However, in its Privacy Report, the Commission did not address the possible competitive effects of its recommendations, including potentially reducing the flow of information in the marketplace, which may be an unintended effect caused by compliance with new requirements.[16]

Notably, the ABA Antitrust Section filed a comment on the FTC's Preliminary Privacy Report that highlighted the need to weigh carefully the benefits and costs associated with proposals to enhance privacy.[17] The ABA comment pointed out that although the Report emphasized that, to make meaningful choices, consumers need more information about how their data will be used, it did not assess the value consumers may reap from additional uses of their information that facilitate competition.[18] For example, consumers who choose not to allow the collection or sharing of broad categories of information may no longer be exposed to offers by competitors selling products or services that provide better value, pricing, or quality.[19] In turn, these changes could have negative consequences not just for individual consumers exercising their choice over how their information is used following a particular transaction, but also on the market economy in general.

As the Supreme Court has recognized,

> "[A]dvertising, however tasteless and excessive it sometimes may seem, is nonetheless dissemination of information as to who is producing and selling what product, for what reason, and at what price. So long as we preserve a predominantly free enterprise economy, the allocation of our resources in large measure will be

[16] *See generally* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
[17] *See* Comments of the American Bar Association, Section of Antitrust Law, *A Preliminary FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Feb. 1, 2011), *available at* http://ftc.gov/os/comments/privacyreportframework/00272-57555.pdf.
[18] *Id.* at 4.
[19] *Id.*

> made through numerous private economic decisions. It is a matter of public interest that those decisions, in the aggregate, be intelligent and well informed. To this end, the free flow of commercial information is indispensable."[20]

A policy that limits the ability of advertisers to access and use information to reach target audiences may have unintended effects on consumers and the marketplace that any policymaker, particularly one with responsibility for consumer protection and competition, must consider.

I want to thank you for your attention and commend each of you for your hard work and dedication to the NAI's self-regulatory framework. The NAI helps to raise the bar for responsible data management practices across the entire third-party ecosystem, and I am pleased to have the opportunity to participate in the summit.

[20] *Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748, 765 (1976).