Remarks of Commissioner Maureen K. Ohlhausen
Marketing and Public Policy Conference 2013
The Changing Role of Policy in Consumer Well-Being
Washington, D.C.
May 31, 2013

Consumer Privacy: Someone May Be Watching You – And That May Not Always Be a Bad Thing

Introduction

Thank you for that kind introduction. It is an honor to be the keynote speaker at this Marketing and Public Policy Conference. Your agenda shows a couple of days packed with great speakers on important and timely topics, including several sessions on a Saturday, which truly demonstrates commitment to your craft. I also want to thank my FTC colleague, Jan Pappalardo, who encouraged me to participate in this event by highlighting the quality of the participants and the important research that past events have spearheaded, especially in the areas of food and health-related marketing.

After giving you a brief background on how I view my role as an FTC Commissioner, I will focus on the FTC's work in privacy, the importance of self-regulation to advance consumer privacy, and the need for empirical research to help guide policy decisions in this area. My remarks are my own, however, and do not necessarily reflect the views of my colleagues on the Commission.

Background

I was sworn in as an FTC Commissioner in April 2012. This was a bit of a homecoming for me as I had already served in the agency's General Counsel's Office, as an Attorney Advisor to a Commissioner, and as Deputy Director and finally Director of the Office of Policy Planning, as well as head of the agency's Internet Access Task Force. Also, during my tenure at the Office of Policy Planning, I led the agency's policy initiatives regarding the alleged link between food marketing and obesity. I also served as a law clerk for Judge David Sentelle at the U.S. Court of Appeals for the D.C. Circuit for several years before I first joined the FTC. Most recently, I served as a partner at the law firm Wilkinson, Barker and Knauer, working primarily on FTC issues.

My varied FTC roles have given me a broad understanding of the FTC's many activities and provided me with a wide perspective on the intersection of consumer protection and antitrust. All of my experience, both within and outside government, informs my perspective on FTC activities in my current role as a Commissioner.

As a Commissioner, my top priority is to support the FTC's mission to prevent business practices that are anticompetitive or deceptive or unfair to consumers; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish this without unduly burdening legitimate business activity. I support the agency using all of its tools to achieve these goals and to evaluate carefully what tool is appropriate to address any given problem. I also encourage the Commission to consider all possible approaches to any given problem, such as enforcement, research, consumer and business education, and sometimes allowing market forces to work on their own. I believe strongly in consumer and business education, which can help empower consumers to avoid fraud and make better-informed choices, and can help businesses improve their compliance with the law. The FTC should also, whenever possible, provide detailed explanations of what it is doing – or not doing, as the case may be – and why it is doing it.

My emphasis on carefully evaluating which of our many tools is appropriate for a given problem stems from my belief that our focus should be on outcomes, not output – that is, examining whether agency activity is actually improving consumer welfare and whether it can be done more effectively.

This focus on the efficient and effective operation of the agency is an outgrowth of my previous work as director of the FTC's Office of Policy Planning to help craft the FTC self-assessment in anticipation of our upcoming 100th anniversary next year. For those of you who are not familiar with this work, the "FTC at 100" self-assessment represented an effort by personnel across the agency to create a framework for assessing this agency's performance.[1] Its goal was not necessarily to assign the agency a set of grades, but to establish what subjects any future report cards ought to include. This self-assessment provides important guidance for the Commission as it enters its second century.

FTC and Privacy

With that background, I will now turn to one of the FTC's major areas of work, the impact of new technologies on consumer privacy. Since the emergence of ecommerce 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.

At the heart of the FTC's authority is Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in the consumer protection area and unfair methods of competition in the antitrust arena.[2] Section 5 provides a powerful law enforcement tool that has proven its

[1] *See* CHAIRMAN WILLIAM E. KOVACIC, THE FEDERAL TRADE COMMISSION AT 100: INTO OUR SECOND CENTURY: THE CONTINUING PURSUIT OF BETTER PRACTICES (Jan. 2009), *available at* http://www.ftc.gov/os/2009/01/ftc100rpt.pdf.
[2] 15 U.S.C. § 45.

mettle over time as the mainstay of the FTC's enforcement efforts. Although elegantly simple in its text, Section 5 can reach a multitude of acts and behaviors and has proven to be very flexible over the years.

A number of years ago, the Commission adopted separate statements on deception and unfairness to explain how we will interpret Section 5 in the consumer protection area. Those statements continue to guide the Commission today. Here's how they work:

The deception statement explains that deceptive practices are representations, whether explicit or implicit, about material facts that are likely to mislead consumers who are acting reasonably.[3] Challenging deception has long been the core of the Commission's consumer protection mission, and it should remain so. Fraud is a serious problem that leads to monetary losses as well as to a loss of trust in the marketplace, which hurts consumers and legitimate businesses alike.

In the areas of privacy and data security, the Commission most often 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 fails to keep that promise, resulting in consumer injury.

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. For an act or practice to be unfair, the Commission's unfairness statement requires the harm caused to be substantial, to not be outweighed by any offsetting consumer or competitive benefits, and for the consumer to not have been able to reasonably avoid the harm.[4]

The unfairness statement specifically identifies financial, health, and safety harms as varieties of harm that the Commission should consider substantial. It further states that emotional impact and more subjective types of harm are not intended to make an injury unfair.
Using its deception and unfairness authority, the FTC has brought over 100 spam and spyware cases and over 40 data security cases. When the Commission challenges practices related to privacy and/or data security, it usually obtains an administrative or federal court order prohibiting future violations of the law and requiring the defendants to abide by their promises to consumers. In some cases, the order requires a defendant to implement a compliance program and to undergo audits administered by an independent third party every two years. The results of these audits must be submitted to the Commission as part of the compliance review process. When defendants violate FTC orders, they can be liable for civil penalties. For example, Google paid $22.5 million to settle charges that it violated an earlier FTC order when it misrepresented to users of Apple's Safari browser that it would not place tracking cookies or serve targeted ads.[5]

---

[3] FEDERAL TRADE COMMISSION, FTC POLICY STATEMENT ON DECEPTION (1983), *available at* http://www.ftc.gov/bcp/policystmt/addecept.htm.
[4] FEDERAL TRADE COMMISSION, FTC POLICY STATEMENT ON UNFAIRNESS (1980), *available at* http://www.ftc.gov/bcp/policystmt/adunfair.htm.
[5] Press Release, Federal Trade Commission, Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), *available at* http://ftc.gov/opa/2012/08/google.shtm.

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.

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, as well as our research and study initiatives. The FTC can maximize its effectiveness and reach not just by bringing cases, but also by 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 becoming victims of fraud.

Accordingly, the FTC has worked to understand the online marketplace and the privacy issues it raises for consumers by hosting numerous public workshops, issuing public reports on online data collection practices, monitoring industry self-regulatory efforts, and closely following technological developments affecting consumer privacy. For instance, 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. 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. Specifically, the principles provide for transparency, consumer control, and reasonable security for consumer data. The principles 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.

The Commission also held workshops on the privacy challenges posed by new technologies in 2009 and 2010, and in March 2012, just before I started as a Commissioner, the agency released, "Protecting Consumer Privacy in an Era of Rapid Change," a comprehensive report that included recommendations for companies that handle consumer data.[6] 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

[6] *See* FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (Mar. 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

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, companies should adopt notice and choice options that appropriately reflect the context of the transaction 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 another area of privacy research, the Commission recently began a study of the data broker industry. We sent out formal requests for information to nine large data brokers to learn more about their practices, including how they use, share, and secure consumer data. It is vital that we have a good understanding of data usage by brokers because appropriate use of data can greatly benefit consumers through better services and increased convenience, while inappropriate use or insecure maintenance of data could cause significant harm to consumers. We will carefully analyze the submissions from the companies and use the information to decide how to proceed in this area. Congress is also taking a closer look at this industry, so I expect that it will be a hot topic of discussion in the data privacy and security community in the days ahead.

Privacy and Online Behavioral Advertising

Having outlined the FTC's privacy work generally, I will now turn to online behavioral advertising (also known as "OBA"), which includes a broad set of practices companies use to show ads or content that they believe is more relevant to consumers. Companies use different mechanisms to collect information about consumers' browsing habits. They typically use cookies, which may include flash cookies, beacons, or tracking pixels. These are small files stored on a device when a user visits a website. Companies use these files to help determine consumer interests based on the pages visited, the content that is clicked on, and other actions. In most cases, the data that behavioral advertising companies collect is not tied to personal information. For example, they don't know a user's name, home address, or phone number. Instead, they identify a user by an ID number and try to guess the users' interests and characteristics based on his or her online activity. The data they retain could include inferred age group, gender, or purchase interests.[7]

Behavioral advertising provides several benefits to consumers in the form of more relevant advertisements and less unwanted or potentially unwelcome advertisements. Behavioral advertising also helps subsidize a broad range of free online content and services, such as mobile apps, search engines, social networking, and instant access to news sources and information from around the world. This, in turn, helps provide a significant boost to innovation and the online economy.

[7] *See What Is Online Behavioral Advertising?*, TRUSTE, http://www.truste.com/consumer-privacy/about-oba/ (last visited May 31, 2013).

At the same time, behavioral advertising raises consumer privacy concerns. Some consumers express discomfort about the privacy implications of being tracked, as well as the specific harms that could result. For example, without adequate safeguards, consumer tracking data may fall into the wrong hands or be used for unanticipated purposes. These concerns may be more pronounced when the information relates to children, health, or finances.[8]

There is substantial debate about the need to regulate OBA because of consumer privacy concerns. Certainly not all consumers are the same, and the privacy debate is a great example of an issue on which there are differing views about 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. I doubt, however, that result can be reasonably extrapolated to say that most consumers strongly object to OBA.

I saw the results of a recent Zogby Analytics poll commissioned by the Digital Advertising Alliance (or DAA) in which only 4% of respondents said they are concerned about behavioral targeting.[9] According to the poll, 40% preferred that all of their ads be targeted, and 70% said that they prefer at least some of their ads be tailored directly to their interests. Many consumers place great value on the availability of online advertising, and 75% of the poll's respondents said that they prefer free content supported by ads, compared to 10% who stated that they would rather pay for ad-free content.

My view is that both groups of consumers should have options that comport with their preferences, and the first question for a policymaker should be whether those options are available to consumers through products or services available in the market 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.[10] 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 also 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. One such add-on, Ghostery, helps users easily detect trackers that behavioral advertisers often use to follow individuals across sites. Identifying such trackers promotes transparency by giving consumers more information on the advertising practice of the sites they regularly visit. For those interested in near complete

---

[8] *See Hearing on Privacy Implications of Online Advertising Before the S. Comm. on Commerce, Sci., and Transp.*, 110th Cong. 3-4 (2008), *available at* http://www.ftc.gov/os/2008/07/P085400behavioralad.pdf (statement of Lydia B. Parnes, Director, Bureau of Consumer Protection, Federal Trade Commission).

[9] *See Poll: Americans Want Free Internet Content, Value Interest-Based Advertising*, DIGITAL ADVERTISING ALLIANCE (Apr. 19, 2013), http://www.aboutads.info/DAA-Zogby-Poll.

[10] *See* Ryan Singel, *DuckDuckGo Challenges Google on Privacy (With a Billboard)*, WIRED (Jan. 19, 2011, 8:08 PM), http://www.wired.com/business/2011/01/duckduckgo-google-privacy/.

privacy on the web, Torbutton provides one-click access to the Tor network for true online anonymity. These are just a few examples of a range of available products that allow consumers to tailor their online services to better reflect their online privacy preferences.

Self-regulatory programs can also offer consumers choices, and they have the benefit of being nimble and keeping pace with rapid changes in technology and business practices in ways legislation and regulation cannot.

The Digital Advertising Alliance (DAA), for instance, leads an industry-wide effort to provide users with choice and control over how and whether they receive behavioral ads. The DAA operates a free opt-out tool that gives users the power to dictate their ad preferences. Since the program's launch in 2010, more than 23.5 million consumers have visited the DAA sites to learn about advertising data choices. Last year, more than a million consumers exercised their choice about how advertisers will use their data through the DAA's program.[11]

Another example of self-regulation is the ongoing initiative of the World Wide Web Consortium's Tracking Protection Working Group. This W3C working group is seeking to create an international industry-wide standard for Do Not Track that would operate in both desktop and mobile settings. The group met recently in San Francisco and seems to have made some progress. Some reports raise doubts as to whether the process will ultimately produce an agreement. I am closely monitoring the situation, while also evaluating the ramifications of different outcomes.

Privacy and Competition

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. Also, 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.

The Need for Empirical Research

I always strive to make decisions based on sound empirical evidence where available, and my analysis of privacy issues is no different. I see a significant need to measure consumer harm and strike the right policy balance through research-based parameters. However, when it comes to privacy, it appears that there is significant room for additional research, especially with regard

[11] *See Hearing on a Status Update on the Development of Voluntary Do-Not-Track Standards Before the S. Comm. on Commerce, Sci., and Transp.*, 113th Cong. (2013), *available at* http://www.aboutads.info/resource/4.23.13_DAA_Testimony.pdf (testimony of Luigi Mastria, Managing Director, Digital Advertising Alliance).

to consumer attitudes and preferences. It also seems that much of the existing research only depicts part of the story.

I have seen many privacy arguments based on studies showing that consumers value their privacy a great deal. For instance, TRUSTe's 2013 consumer confidence index reveals that 89% of U.S. adults worry about their privacy online, 72% of smartphone users are more concerned about their privacy than a year ago, and 81% of smartphone users avoid using apps that they do not believe protect their online privacy.[12]

But a recent New York Times article indicates that despite how much we say we value our privacy, we tend to act inconsistently.[13] As pointed out in that article, Professor Alessandro Acquisti, a behavioral economist at Carnegie Mellon University, used a series of experiments to suggest that policymakers should carefully consider how people actually behave. For example, in one experiment shoppers at a mall were offered a $10 discount card plus an extra $2 discount in exchange for their shopping data. Fifty percent of the shoppers declined the extra discount. In a separate test, mall shoppers were offered a $12 discount card and the option to trade it for a $10 card to keep their shopping record private. Ninety percent of those shoppers chose the $12 card, even if it meant giving away their shopping information.

At a recent panel hosted by the Internet Caucus Advisory Committee, a participant pointed out that "poll numbers show that a very high percentage of Americans don't want to be tracked on the Internet, but a very similar high percentage of Americans in other polls show that they want location-based services that are helpful to them."[14] Moreover, as I referenced earlier, a Zogby Analytics poll indicates that a significant proportion of consumers are willing to provide some of their information in exchange for better targeted ads and the availability of free online content.

Last year, Digital Trends reported on a study by Accenture, which found that the majority of consumers in both the U.S. and UK are willing to have trusted retailers use some of their personal data to present personalized and targeted products, services, recommendations, and offers.[15] The study found that while 86% of those surveyed said they were concerned that their data was being tracked, 85% said they realized that data tracking makes it possible for retailers to present them with relevant and targeted content. Almost half of those surveyed said they are receptive to having trusted brands track their data in return for a personalized shopping experience. Sixty four percent said they prefer the personalized experience. Another 64% said

---

[12] *See 2013 TRUSTe U.S. Consumer Confidence Index*, TRUSTE, http://www.truste.com/us-consumer-confidence-index-2013/ (last visited May 31, 2013).
[13] *See* Somini Sengupta, *Letting Down Our Guard with Web Privacy*, NEW YORK TIMES (Mar. 30, 2013), http://www.nytimes.com/2013/03/31/technology/web-privacy-and-how-consumers-let-down-their-guard.html?pagewanted=all&_r=0/.
[14] Congressional Internet Caucus Advisory Committee, *2013 State of the Mobile Net: Mobile Location: The Policies of Where*, YOUTUBE (May 10, 2013), http://www.youtube.com/watch?v=6GKqA0IzUWk (statement of Jason Weinstein, Partner, Steptoe & Johnson, Former Deputy Assistant Attorney General, Department of Justice, 44:29).
[15] *See* Grace Nasri, *Why Consumers Are Increasingly Willing to Trade Data for Personalization*, DIGITAL TRENDS (Dec. 10, 2012), http://www.digitaltrends.com/social-media/why-consumers-are-increasingly-willing-to-trade-data-for-personalization.

they would be willing to have brands send them text messages when shopping at brick and mortar stores to provide personalized offers based on previous purchase history. Additionally, the vast majority of consumers (88%) thought that companies should give them the flexibility to control how their personal information is used to personalize their shopping experience.

So, at this point you may be wondering why I am talking to you about online privacy today. My colleague Jan Pappalardo suggested that this audience would be quite receptive to proposed topics for research, and I would like to follow up on her suggestion.

For starters, I exhort you to pursue research that could shed light on specific consumer attitudes and preferences regarding privacy choices. I am especially interested in consumers' willingness to share personal information in exchange for online content and functionality, as well as their willingness to pay for different levels of privacy. Additionally, I would be interested in how those attitudes and preferences apply throughout various demographics, especially in different age groups. To put it bluntly, I am concerned that in the areas of technology generally and privacy specifically it may be a case of older folks who are not comfortable with these developments making rules that apply to young people, who see things differently.

I would also find useful sound consumer research related to the exercise of privacy choices that can help the market function properly. For instance, it would be helpful to have empirical evidence regarding consumer perception and understanding of privacy-related disclosures through various devices, screen sizes, and formats, such as icons or text.

Speaking of disclosures, I should make clear that I am unable to offer any funding for these proposals. What I can offer, however, is our sincere desire to partner with your institutions through a dialogue on these very relevant issues. I can also offer you the potential satisfaction and even glory that comes with making a significant contribution to consumer welfare. You may have heard about our recent Robocall Challenge, which sought private sector solutions to the ongoing problem of unsolicited, pre-recorded telemarketing calls. This initiative garnered quite a bit of media attention and was regarded as a positive example of public-private cooperation to seek ingenious solutions to difficult challenges. Again, I cannot offer you prize money, but I will do my best to ensure your work receives the recognition it deserves.

I want to thank you for your attention, and for all the good work that you have done throughout the years. I am pleased to have the opportunity to participate in this event and to take your questions.