FTC Commissioner Maureen K. Ohlhausen
Speech Before the Hudson Institute
October 16, 2012
The Government's Role in Privacy: Getting it Right

Thank you for that kind introduction and for inviting me to address the Hudson Institute on the important topic of the government's role in privacy and how to get it right. As you may know, prior to leaving private practice to join the FTC as a Commissioner in April of this year, I had previously served at the Commission for almost 12 years, starting in 1997. My long experience at the Commission—in the GC's office, as an Attorney Advisor to Commissioner Orson Swindle, and as head of the Commission's Office of Policy Planning, provided me an extensive background in all areas of the FTC's jurisdiction and activity: consumer protection, competition, and economics.

This experience guides how I approach all issues at the Commission, including privacy. In this spirit, I would like to discuss privacy in the broader context of the FTC's current statutory authority to protect American consumers against deceptive and unfair practices, as well the Commission's important mission to preserve competition in the market.

I am going to start with a discussion on our enforcement record, based on our current statutory authority. Then, I will describe another important tool in our arsenal, our business and consumer education function, and the critical role it has played in the privacy area, especially in the online environment. Finally, I will highlight the way that the Commission stays on top of the mobile technologies sweeping the globe.

After my opening remarks, I would like to spend some time learning from you. One of the most valuable things I do is listen. When I hear directly from consumers, businesses, and policymakers, my ability to do my job is greatly enhanced. So I will pose several questions related to issues with which the agency is currently grappling. I hope that you will be willing to share with me your thoughts on these issues and how they impact you. And, since turnabout is fair play, I will conclude my time with you by responding to any questions you may have for me.

Section 5 of the FTC Act

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.[1] Section 5 provides a powerful law enforcement tool that has proven its 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.

[1] 15 U.S.C. § 45.

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 acting reasonably.[2] 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 it fails to keep that promise and consumer injury results.

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.[3]

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.

DesignerWare Settlement

To illustrate how the FTC's deception and unfairness authority works in the area of privacy, particularly online privacy, I would like to highlight a recent FTC case. Two weeks ago, we announced a settlement with DesignerWare, a software firm, and the seven rent-to-own companies that deployed DesignerWare's software product in laptops they rented to consumers.[4] DesignerWare's software had some legitimate features, such as a "kill switch" that the rent-to-own stores could use to disable a computer if it was stolen or if the renter failed to make payments on it. DesignerWare's product also had a "Detective Mode" that was intended to help the rent-to-own operators track the location of the computers. But the way that Detective Mode was installed and the way it was operated by DesignerWare and the rent to own stores, as well as the failure to provide users notice of certain features, raised a host of privacy issues.

---

[2] FTC, *The FTC Policy Statement on Deception* (Oct. 14, 1983), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm (last visited Oct. 2, 2012).
[3] FTC, *The FTC Policy Statement on Unfairness* (Dec. 17, 1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm (last visited Oct. 2, 2012).
[4] Proposed DesignerWare, LLC. Consent Agreement, 77 Fed. Reg. 60,119 (Oct. 2, 2012).

When Detective Mode was activated, the software could log key strokes, capture screen shots, and take photographs using a computer's webcam. It also presented a fake software program registration screen that tricked consumers into providing their personal contact information and did not register software. Data gathered by DesignerWare and provided to rent-to-own stores using Detective Mode revealed private and confidential details about computer users, such as user names and passwords for email accounts, social media websites, and financial institutions; Social Security numbers; medical records; private emails to doctors; bank and credit card statements; and webcam pictures of children, partially undressed individuals, and intimate activities at home, as well as geolocation data.

Our complaint against DesignerWare and the rent to own companies included both unfairness and deception counts. The deception count was straightforward and was based on sending consumers the fake registration forms to obtain their contact information. Clearly, this was an explicit representation about a material fact that was likely to mislead a consumer acting reasonably.

The Commission also charged that licensing and enabling Detective Mode, gathering sensitive personal information about renters, and disclosing that information to the rent-to-own businesses was unfair. Specifically, the complaint alleged that the collection and disclosure of private and confidential financial and medical information about consumers caused or is likely to cause substantial injury to consumers. I believe that this is consistent with the unfairness statement, which identifies financial and health harms as substantial.

The complaint also alleged that the defendants' intrusion into consumers' homes, the tracking of their locations over time, and the capture and disclosure of information, including images of partially undressed individuals and sexual activity, was also unfair. This intrusion into the home, the sharing of such images, and the tracking of precise consumer locations over time, in my opinion, caused substantial injury to consumers by creating an unwarranted safety risks that could arise from stalking or similar behavior triggered by such exposure and tracking.

As for the other requirements of unfairness, because Detective Mode functioned secretly, consumers could not reasonably avoid this harm, and any possible benefits of the practice did not seem to outweigh its harms, particularly because the rent-to-own stores had effective alternative methods for collections.

I would note that, as a general rule, I do not support holding third parties who simply create a product, like software, liable for actions others take using that product. In this case, the determinative factor for me in holding not just the rent to own stores but also DesignerWare liable was that DesignerWare knowingly collected the sensitive medical and financial data and images from consumers and sent them the fake web registration forms. That rightly puts them on the hook, in my view.

Why did I belabor this case? It's not simply to highlight some distasteful computer snooping but to emphasize that the Commission was able to stop this behavior under Section 5. No additional authority was necessary. And the Commission's strong action in this matter is not an exception. With its current statutory authority the FTC has brought more than a hundred spam and spyware cases and more than thirty data security cases, including against many

prominent companies, as well as nineteen Children's Online Privacy Protections Act (COPPA)[5] actions.

Calls for New Legislation

In the FTC's Privacy Report, released shortly before I joined the Commission, some of my fellow Commissioners called for a new privacy law that would go beyond Section 5, but did not specify what such new legislation should look like.[6] The Report also did not identify what substantial harms are occurring now that Section 5 cannot reach, although it did appear to embrace an expansion of the concept of harm to include reputational or other intangible privacy interests, which the FTC's unfairness statement indicated would not make an injury unfair. In addition to the FTC Report, there have been other calls for a new, more general privacy law from other quarters.

In thinking about these calls for new legislation, I would like to share with you a personal analogy that I readily confess may have a bit of a gender bias to it. With the onset of such nice, crisp fall days, I start thinking about transitioning my closet to my cooler weather wardrobe. But before I hit the stores and buy new items, I've learned from experience to take an inventory of the clothes already in my closet to avoid buying things I already have.

I believe it is similarly important for policymakers to take an inventory of what is already in stock in the FTC closet before seeking new privacy laws. I'm not necessarily against legislation and there are a number of existing laws in addition to Section 5, such as COPPA, the Fair Credit Reporting Act, GLB, and others, that are an important part of the agency's enforcement arsenal.[7] There are also other privacy laws, such as HIPPA, as well as the CPNI and cable privacy rules, that provide important protections for consumers.[8]

Before seeking new privacy legislation, it is important to identify a gap in statutory authority or to identify a case of substantial consumer harm that we'd like to address, but can't, with our existing authority, especially given the array of financial, medical, and health and safety harms already reachable under our current FTC authority or other laws. Otherwise, it is difficult to tell whether the additional protections are necessary or will, on balance, make consumers better off because information sharing has benefits for consumers such as reducing online fraud, improving products and services, and increasing competition in the market overall.

---

[5] The Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506 (2006).
[6] FED. TRADE COM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUS. AND POLICYMAKERS (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
[7] The Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506 (2006); The Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (2006); The Gramm–Leach–Bliley Act, 15 U.S.C. §§ 6801-6809 (2006).
[8] The Health Insurance Portability and Accountability Act (HIPPA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, 42 U.S.C.); The Customer Proprietary Network Information Rule, 72 Fed. Reg. 31,947 (June 8, 2007) (codified at 47 C.F.R. pt. 64); The Cable TV Privacy Act of 1984, 47 U.S.C. §551 (2006).

Privacy and Competition

This is why I am concerned about treating privacy 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. The FTC is uniquely positioned among federal agencies to balance consumer protection and competition in its analysis.

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 (and services and products that depend on accessibility and use of such data), which may be an unintended (or intended, depending on the type of data) effect caused by compliance with new requirements.

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.[9]

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. 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. 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 stated in the *Virginia State Bd. of Pharmacy* case "advertising, 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 made through numerous private economic decisions. It is a matter of

[9] ABA Antitrust Section's Comment on FTC's Preliminary Privacy Report (Feb. 1, 2011), *available at* http://www.ftc.gov/os/comments/privacyreportframework/00272-57555.pdf.

public interest that those decisions, in the aggregate, be intelligent and well informed. To this end, the free flow of commercial information is indispensible."[10]

A policy that limits the ability of advertisers to access and use information (whether collected directly from consumers, or indirectly through affiliates, different brands within the company, or from third parties) 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.

To raise the question of the effect on competition does not mean that I would never support any new privacy law, it simply means that I believe we must at least ask the question if we want to ensure the best outcome for consumers.

A Uniform Standard for Data Security

Turning back to my earlier shopping analogy, there is one new accessory that I would support adding to the FTC's fall wardrobe: a uniform federal law for data security and breach notification. Although the FTC can proceed using its Section 5 authority—and since 2001 it has brought over thirty cases against companies for failing to protect consumer information—there are gaps that could be closed through carefully crafted federal legislation. Currently, almost all states have data security laws on the books that require consumer notification if personal information has been compromised. Although some of the laws are similar, they are not identical. This means that companies need to comply with separate state notice requirements and consumers may get notifications that are different and are triggered by different types of breaches.

A single standard would let companies know what to do and consumers know what to expect. I believe that, if carefully crafted, such a law is likely to benefit both consumers and business, particularly because, unlike uses of consumer information for advertising, product improvement, or fraud reduction, there are no benefits to consumers or competition from allowing consumer data to be stolen. Any such law would have to consider carefully, however, what are reasonable precautions for safeguarding various types of data to avoid imposing undue costs that are not justified by consumer benefits.

Business and Consumer Education

Law enforcement is critically important, but in some respects the Commission's consumer and business education mission impacts a greater percentage of American consumers that anything else we do. For example, the information available on our webpage to help consumers avoid becoming victims of identity theft has had millions of hits, and the paper edition has been distributed through many channels to millions more. And if prevention doesn't work, we offer excellent resources on steps to take to mitigate the damage of having your

[10] *Va. Pharm. Bd. v. Va. Consumer Council*, 425 U.S. 748, 765 (1976).

identity stolen. We educate consumers on how to establish and protect their credit scores, how not to fall victim to scams, and, the ever popular, how to sign up for the Do Not Call list.

In addition, the FTC produces consumer education about keeping kids safe online, such as the award-winning brochure for parents, Net Cetera: Chatting with Kids About Being Online, as well as the Net Cetera Community Outreach Toolkit to help people share this information. This type of research, inquiry and outreach is an area of particular strength for the Commission.

We also sponsor public workshops on a host of consumer issues. These events help our staff understand complex issues from a variety of stakeholder perspectives and also provide us a forum with which to share our agency expertise. On Thursday, we are hosting a public workshop on RoboCalls to explore innovations designed to trace robocalls, prevent wrongdoers from faking caller ID data, and stop unwanted calls. It will include a report on the current state of robocall technology and the industry, along with a discussion of the laws surrounding the use of robocalls, including how they are enforced, enforcement limitations, and what this means for consumers. Panelists will discuss developing solutions to the problem of illegal robocalls, including caller ID spoofing, call authentication, and call-blocking.

Just yesterday, the Commission announced a workshop to be held on December 6th, to Explore the Practices and Privacy Implications of Comprehensive Collection of Internet Users' Data. This workshop, like all others sponsored by the FTC, will include speakers representing all of the major stakeholders in the debate on data collection. Details are available at our website at: www.ftc.gov.

Keeping Abreast of the Technology Wave: Mobile Technology Unit

One of the biggest challenges faced by the FTC is to keep abreast of new technologies and to understand how they impact consumers and privacy. Mobile technology is a great example. While smart phones have only been available for a few years, the market penetration has been phenomenal. By February 2012, over 88 percent of American adults owned a mobile device, compared with 58 percent owning a desktop and 61 percent owning a laptop. Mobile devices offer many consumer benefits such as new services and convenience, but they also raise unique privacy issues. These arise from the phone's ability to provide real-time location data, its small display screen for disclosures, and its wide variety of uses, from a payment channel to a medical device.

Because mobile technologies are moving with lightning speed, the Commission determined it needed to have dedicated staff working exclusively on mobile issues. Thus, the Mobile Technology Unit was established.

The Mobile Technology Unit issued a report on mobile apps for children and hosted a workshop on mobile disclosures, including privacy disclosures. The report and workshop examined the adequacy of information that app stores and developers provide to parents about what information is being collected, how it will be shared, and who will have access to it. We

have also reached out to industry to work on improving the disclosures. The Unit is now following up with a survey to find out how frequently apps aimed at kids actually collect data. In addition, it has brought six law enforcement cases.

Conclusion

I've covered a lot of territory with you today. Let me briefly restate the three points with which I hope to leave you. First, I am not convinced that the FTC is currently lacking any statutory authority in the general privacy area; for now, Section 5 is sufficient to protect consumers. Second, the Commission must analyze issues under its purview from a perspective that covers both consumer protection and competition scrutiny, or it will not reach the best result for consumers. Finally, the Commission should use all of the tools in its arsenal: law enforcement, regulatory and business and consumer education to reach the maximum target audience. As the newest Commissioner, but the one with the most experience at the agency, I pledge to ensure that we do all in our power to further the interests of American consumers.