Commissioner Maureen K. Ohlhausen

The FTC's Privacy Agenda for the 2014 Horizon

Forum for EU-U.S. Legal-Economic Affairs

Berlin, Germany

September 14, 2013

Professor Mestmacker and distinguished Berlin Forum Principals, it is an honor to have the opportunity to speak with you. Today, I will share my personal insights on the key privacy issues likely to face the Federal Trade Commission in 2014 and privacy-related activity in the U.S. Congress. My comments today are my own, however, and should not be construed as necessarily representing the views of my fellow Commissioners.

My long experience at the FTC before becoming a Commissioner—in the Office of General Counsel, as Attorney Advisor to Commissioner Orson Swindle, and as head of the Office of Policy Planning—gave me an extensive background in all three areas within the FTC's purview: 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.

I will start with a discussion of our statutory authority and the enforcement we have undertaken. 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. Next, I will identify issues that I believe will be significant for the FTC in 2014, as well as areas of possible Congressional interest. Finally, I will highlight some market developments that reflect a growing emphasis on offering consumers greater privacy options.

After touching on these topics, I look forward to an open exchange with you. Although I will focus on the U.S. approach to consumer privacy, we, like every other country, must consider our policies in the context of the global environment. An important part of my job is to reach out to the global community. I know that I will learn much from our exchange and hope that the discussion will enhance our mutual understanding of our priorities in the privacy arena.

Current U.S. Statutory Framework

We live in exhilarating and challenging times as technology evolves at lightning speed while the world continues to grapple with ways to protect consumer privacy without stifling innovation. I know Europeans care deeply about protecting their personal information as reflected by the fact that in the EU, privacy is viewed as a fundamental human right. The U.S. also values consumer privacy, but, as you know, we have a different approach.

The U.S. has a broad national legal framework to protect the kinds of personal data that American consumers care about most. Like other functions in the U.S. government, however, several agencies share responsibility for data and privacy protection. The FTC is the primary U.S. consumer protection agency and one of the two national competition regulators. We can enforce legal protections that cover financial and credit information under such laws as the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Gramm-Leach-Bliley Act.[1] We also enforce the Children's Online Privacy Protection Act (COPPA), which limits the online collection of information about children.[2]

There are also privacy laws enforced by other agencies to protect medical data, such as the Health Insurance Affordability and Accountability Act, better known as "HIPAA", as well as the Customer Proprietary Network Information Rules and cable privacy rules that provide important protections for consumers in their electronic communications.[3]

The FTC's general source of authority for privacy oversight, however, 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.[4] 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 in our consumer protection efforts.

A number of years ago, the Commission adopted separate policy 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. This is how they work:

According to our Policy Statement on Deception, deceptive practices are explicit or implicit representations about material facts that are likely to mislead consumers acting reasonably.[5] 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.

---

[1] The Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (2012); The Fair Debt Collection Practices Act, 15 U.S.C. § 1692 (2012); The Gramm–Leach–Bliley Act, 15 U.S.C. §§ 6801-6809 (2012).
[2] The Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2012).
[3] 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 (2012).
[4] 15 U.S.C. § 45.
[5] Fed. Trade Com'n, FTC Policy Statement on Deception (1983), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

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.

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 Policy Statement on Unfairness deems a practice to be unfair if it causes substantial harm, which is not outweighed by any offsetting consumer or competitive benefits, and the consumer could not have reasonably avoided the harm.[6]

The Policy Statement on Unfairness specifically identifies financial, health, and safety as varieties of harm that the Commission should consider substantial. It further states that emotional impact and more subjective types of harm will not make a practice unfair.

Using our statutory authority, the FTC has brought more than 100 spam and spyware cases and more than 47 data security cases, including those against an international hotel chain, a major data broker, a national drugstore chain, and the social media site, Twitter. We have also brought actions against companies such as Google and Facebook for violating their privacy promises. Additionally, we have brought over 20 cases to enforce COPPA and have collected more than $7 million in civil penalties. I believe the agency has a strong enforcement record, and I will continue to support our enforcement efforts against privacy violations.

Law enforcement is critically important but, in some respects, the Commission's consumer and business education mission impacts a greater percentage of American consumers than 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 we and our partners have distributed the paper edition through many channels to millions more. Also, if prevention does not work, we offer excellent resources on steps consumers can take to mitigate the damage of having their identity stolen. We educate consumers on how to establish and protect their credit scores, how to avoid falling victim to scams, and how to sign up for the ever popular Do Not Call list.[7]

In addition, the FTC produces consumer education about keeping children safe online, such as the award-winning brochure for parents, Net Cetera: Chatting with Kids About Being Online, and a related community outreach toolkit to help people share this information.[8] This type of outreach is an area of particular strength for the Commission.

---

[6] Fed. Trade Com'n, FTC Policy Statement on Unfairness (1980), *available at* http://www.ftc.gov/bcp/policystmt/adunfair.htm.

[7] http://www.consumer.ftc.gov/.

[8] FED. TRADE COM'N, NET CETERA: CHATTING WITH KIDS ABOUT BEING ONLINE (2010), *available at* http://business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf; http://www.onguardonline.gov/sites/default/files/articles/pdf/pdf-0001.pdf.

We also sponsor public workshops on a host of consumer issues, which help our staff understand complex issues from a variety of stakeholder perspectives and provide us a forum with which to share our agency expertise. This November we will hold a program on the Internet of Things; other recent workshops have covered mobile privacy disclosures, mobile security, and facial recognition technology. Recent reports include Mobile Apps for Kids, Facial Recognition, and the 2012 report "Protecting Consumer Privacy in an Era of Rapid Change."[9]

I am a strong believer in using all of the tools in the FTC's toolbox, and our education efforts are an essential part of those efforts.

On the Horizon in 2014

Looking to 2014, there are several trends in privacy that I believe will be the primary focus of FTC activity in enforcement, education, and research.

Data Security

Data security will continue to dominate the conversation in the privacy policy community in 2014. It is also an area where I believe new federal legislation would be helpful. Congress has expressed interest in moving forward on data security legislation in the past and 2014 may be the year in which it happens. Although the FTC can proceed using its Section 5 authority—and since 2001 it has brought over forty cases against companies for failing to protect consumer information—there are gaps that could be closed through carefully crafted federal legislation to protect sensitive data or notify individuals when such data is lost, stolen, or accessed without authority. Currently, 47 states have data security laws requiring consumer notification if personal information has been compromised. Although some of the laws are similar, they are not identical and thus companies need to comply with dozens of statutes that may require varying consumer notifications. A single national standard would let companies know what to do and consumers know what to expect when a breach occurs.

Whether or not additional federal legislation is enacted, the FTC will continue to pursue enforcement in the area of data security. Let me give you a few examples.

This summer, the FTC filed a complaint against LabMD, a company that conducts lab tests on consumer specimens. Our complaint alleged that LabMD failed to take reasonable and appropriate measures to prevent the unauthorized disclosure of sensitive consumer data,

---

[9] FED. TRADE COM'N, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE (2012), *available at* http://business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf; FED. TRADE COM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES (2012), *available at* http://ftc.gov/os/2012/10/121022facialtechrpt.pdf; FED. TRADE COM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICY MAKERS (2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf.

including health information.[10] We alleged that the company failed to implement a comprehensive data security program, use readily available measures to identify commonly known or reasonably foreseeable risks and vulnerabilities, use adequate measures to prevent employees from accessing personal information not needed to perform their jobs, and use readily available measures to prevent and detect unauthorized access to personal information. As a result of these failures, a LabMD spreadsheet containing sensitive personal information such as Social Security numbers and medical information for more than 9,000 consumers became available on a P2P network. This case is currently in litigation.

In June 2012, the FTC filed a complaint against Wyndham Hotels for its failure to protect consumers' personal information, resulting in three data breaches in less than two years.[11] According to the FTC's complaint, Wyndham and its subsidiaries failed to take security measures such as using complex user IDs and passwords and deploying firewalls and network segmentation between the hotels and the corporate network. In addition, Wyndham allowed improper software configurations that resulted in the storage of sensitive payment card information in clear readable text.

We alleged that these failures led to fraudulent charges on consumers' accounts, millions of dollars in fraud loss, and the export of hundreds of thousands of consumers' account information to an Internet domain address registered in Russia. A central allegation of the Commission's case is that Wyndham's privacy policy misrepresented the security measures that the company and its subsidiaries took to protect consumers' personal information and that its failure to safeguard personal information caused substantial consumer injury. This case is also currently in litigation.

Big Data

A second topic likely to dominate the privacy agenda in 2014 is so-called Big Data. The amount of data in the world is growing exponentially and will continue to increase with the added volume and detail of information collected by entities such as Internet Service Providers (ISPs), operating systems, browsers, social media, and mobile carriers. These trends could lead to increased competition, innovation, and growth in productivity. At the same time, however, the collection and use of very large data sets on individual consumers may raise certain privacy concerns.

In response to these trends, the FTC held a public workshop last December to explore the privacy implications of broad collection of data about consumers' online activities.[12] The

---

[10] Press Release, Fed. Trade Com'n, FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy (Aug. 29, 2013), *available at* http://ftc.gov/opa/2013/08/labmd.shtm.
[11] Complaint, FTC v. Wyndham Worldwide Corporation, et al. (D. Ariz. 2012) (No. 12 Civ. 1365).
[12] Press Release, Fed. Trade Com'n, FTC to Host Comprehensive Collection of Web Data Workshop Tomorrow (Dec. 5, 2012), *available at* http://www.ftc.gov/opa/2012/12/bigpicture_ma.shtm.

workshop brought together consumer protection organizations, academics, business and industry representatives, privacy professionals, and others to examine the collection and use of such data, its potential benefits, privacy concerns, and related issues.

The Commission also began a study of the data broker industry.[13] 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 brokers because appropriate use of data can greatly benefit consumers through better services and convenience while inappropriate use or insecure maintenance of data could cause significant harm. We will carefully analyze the submissions from the companies and use the information to inform our knowledge of the industry and help us decide how to proceed in this area.

In a similar vein, in July, the bipartisan Congressional Privacy Caucus launched an inquiry into practices of the data broker industry. Caucus co-chairmen Senator Edward Markey and Representative Joe Barton sent letters requesting information to credit reporting agencies, marketing services firms, and a provider of background checks asking for information about how they collect, analyze, and sell consumer information. The lawmakers are particularly interested in the types of information the companies collect.

With all of this activity, I am confident this will continue to be a hot topic of discussion in the data privacy and security community in 2014.

Mobile

Perhaps the most disruptive new technology of the past decade has been the mobile phone. Barely available a decade ago, a large percentage of the world's population now has access to such devices. The new mobile technologies have been nothing short of amazing, but, as is so often the case, they bring not only new opportunities but also new challenges.

Here are a few of the issues on which the FTC will continue to focus in 2014:

- As the smaller mobile screen takes over from the larger computer monitor as the means of delivering advertising to consumers, how do marketers ensure that the information consumers need to fully evaluate the advertiser's statements is clear and conspicuous?
- How do advertisers effectively communicate this information on social media platforms, such as Twitter, that have their own space or content limitations?

---

[13] Press Release, Fed. Trade Com'n, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 18, 2012), *available at* http://www.ftc.gov/opa/2012/12/databrokers.shtm.

- How should businesses relay key information about their privacy practices to consumers, including how they may be collecting, using, or sharing consumer data?

The Commission is devoting significant resources to addressing the mobile phenomena: in addition to setting up a dedicated Mobile Technology Unit of tech-savvy folks, we have held workshops on Mobile Privacy Disclosures, Mobile Cramming, and Mobile Apps for Kids.[14] Last June, the FTC hosted a public forum entitled *Mobile Security: Potential Threats and Solutions*, which brought together researchers, technologists, and industry participants from across the mobile ecosystem to discuss a variety of mobile security issues, including the threat posed by the rise of mobile malware.[15] We have also issued reports, conducted research, and developed extensive consumer and business education materials.

We have also been active on the enforcement front, bringing two mobile cramming cases resulting from companies placing unauthorized charges on phone bills, which will lead to refunds for consumers.[16] We have many more cases in the mobile area in the pipeline.

Market Developments

Aside from focusing solely on government activities, an important question that I will continue to focus on in 2014 is whether the privacy options consumers desire are available to them through products or services in the marketplace or through industry self-regulation.

Many companies are now developing products that cater directly to consumers with heightened privacy preferences. For example, 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. One such add-on, Ghostery, helps users easily detect tools that behavioral advertisers often use to track individuals across sites.[17] Identifying these tools promotes transparency by giving consumers more information on the advertising practices of the sites that they visit regularly.

---

[14] Press Release, Fed. Trade Com'n, FTC Announces Final Agenda and Panelists for Workshop about Advertising and Privacy Disclosures in Online and Mobile Media (May 28, 2012), *available at* http://ftc.gov/opa/2012/05/dotcomdiscl_ma.shtm; Press Release, Fed. Trade Com'n, FTC to Host Mobile Cramming Roundtable May 8 (Mar. 8, 2013), *available at* http://www.ftc.gov/opa/2013/03/mobilecramming.shtm; Press Release, Fed. Trade Com'n, FTC's Second Kids' App Report Finds Little Progress in Addressing Privacy Concerns Surrounding Mobile Applications for Children (Dec. 10, 2012), *available at* http://www.ftc.gov/opa/2012/12/kidsapp.shtm.

[15] Press Release, Fed. Trade Com'n, FTC Announces Agenda, Panelists for Upcoming Mobile Security Forum (May 24, 2012), *available at* http://ftc.gov/opa/2013/05/mobilethreats.shtm.

[16] Press Release, Fed. Trade Com'n, FTC Files Its First Case Against Mobile Phone "Cramming" (April 17, 2013), *available at* http://www.ftc.gov/opa/2013/04/wisemedia.shtm; Press Release, Fed. Trade Com'n, Jesta Digital Settles FTC Complaint it Crammed Charges on Consumers Mobile Bills Through 'Scareware' and Misuse of Novel Billing Method (Aug. 21, 2013), *available at* http://www.ftc.gov/opa/2013/08/jesta.shtm.

[17] http://www.ghostery.com/.

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. A good example of a self-regulatory program is the Network Advertising Initiative (NAI), which this year released an updated Code of Conduct and a new Mobile Application Code, which for the first time addresses the collection and use of data from mobile apps.[18] Another example of self-regulation is the Digital Advertising Alliance (DAA), which has developed a notice and choice mechanism through a standard icon in ads and on publisher sites, deployed the icon broadly, obtained commitments from the vast majority of the behavioral advertising market, and established an enforcement mechanism to ensure compliance.

Conclusion

I hope that I have reassured you that the U.S. does care deeply about consumer privacy. Through the FTC's enforcement, education and policy work, we are able to provide strong privacy protections to American consumers. This important work will continue to be a top priority for the agency in 2014 and beyond.

Thank you for the opportunity to address you today. I look forward to our discussion.

---

[18] Network Advertising Initiative, 2013 NAI Code of Conduct, *available at* http://www.networkadvertising.org/sites/default/files/2013_nai_code_pr.pdf; Network Advertising Initiative, 2013 NAI Mobile Application Code, *available at* http://www.networkadvertising.org/mobile/NAI_Mobile_Application_Code.pdf.