Data Privacy Day
Remarks of FTC Commissioner Maureen K. Ohlhausen
George Washington University
January 28, 2013

Thank you so much for your kind introduction, Dan. I think back fondly to our time working together on the staff of FTC Commissioner Orson Swindle a dozen years ago, and I am so pleased that we are still able to collaborate on issues that benefit American consumers. Data protection is a very important issue on the consumer protection front, and I am delighted to speak at the sixth annual Data Privacy Day. There is a natural synergy between Data Privacy Day and the mission of the FTC, which is to protect consumers against unfair and deceptive acts and practices without unduly burdening legitimate businesses and to promote competitive markets.

Data is an increasingly vital asset and companies need to protect their customers' personal information from theft and unauthorized access that can hurt customers and harm the business's reputation. That's where data security comes in. Data security is part of the broader topic of data privacy, which encompasses the use of consumer data by a wide variety of entities, with which the consumer often (but not always) has willingly shared information, for a wide variety of purposes. Data security, which I will focus on today, examines how entities safeguard the consumer data that they maintain from unauthorized access by data hackers or from insiders without a legitimate need for that information. Regardless of how one feels about the use of consumer data for marketing or targeting purposes, I believe we can all agree that failing to take reasonable precautions to secure data from identity thieves and other malicious parties hurts consumers and legitimate businesses alike.

This event is a good opportunity to educate consumers on how they can protect their personal data and to guide businesses on how to safeguard the consumer data they hold. Let me say at the outset that my remarks are my own and do not necessarily reflect the views of my fellow Commissioners.

I have three goals for my comments today. First, I want to share with you a bit about the FTC's role in data security: our enforcement record, our policy research, and our consumer and business education efforts. Next, I will offer some practical guidance on how businesses can best protect the data entrusted to them. Finally, I will make a few observations on where we are going with new technologies, such as mobile and facial recognition, that are creating new challenges in the data security landscape.

Enforcement

As the nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security. The Commission enforces several laws and rules that impose obligations upon businesses that possess consumer data. The Commission's Safeguards Rule[1] under the Gramm-Leach-Bliley Act (GLB)[2], for example, imposes data security requirements on financial institutions. The Fair Credit Reporting Act (FCRA) requires

[1] FTC Safeguards Rule, 16 C.F.R. § 314 (2013).
[2] The Gramm–Leach–Bliley Act, 15 U.S.C. §§ 6801-6809 (2006).

credit reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information.[3] It also imposes safe disposal obligations on entities that maintain consumer report information. Additionally, we enforce Section 5 of the FTC Act's prohibition of unfair or deceptive acts or practices in cases where a business makes false or misleading claims about its data security procedures, or where its failure to employ reasonable security measures causes or is likely to cause substantial consumer harm.[4] Using these statutes, we have brought over three dozen data security cases, including a new case we are announcing today.

That case involves a settlement with a leading cord blood bank, Cbr Systems, for failing to protect nearly 300,000 customers' personal information, including Social Security numbers, credit and debit card account numbers, and sensitive medical information.[5] The breach occurred when unencrypted back-up files and a laptop were stolen from a backpack left in an employee's car for several days. We also settled additional charges that Cbr also failed to take sufficient measures to prevent, detect, and investigate unauthorized access to computer networks.

In June 2012, the FTC filed a complaint against Wyndham Hotels for failure to protect consumers' personal information, resulting in three data breaches in less than two years.[6] 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 allegedly permitted improper software configurations that resulted in the storage of sensitive payment card information in clear readable text. The complaint alleges 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 currently in active litigation.

Data Broker Study

Another important tool used by the Commission is policy research, which helps us keep abreast of new business models that use consumer data and to understand how innovations may affect data security and consumer privacy. In this context, the Commission recently began a formal study of the data broker industry.[7] 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

[3] The Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (2006).
[4] 15 U.S.C. § 45.
[5] Press Release, Fed. Trade Com'n, Cord Blood Bank Settles FTC Charges that it Failed to Protect Consumers' Sensitive Personal Information (Jan. 28, 2013), *available at* http://www.ftc.gov/opa/2013/01/cbr.shtm.
[6] Complaint, FTC v. Wyndham Worldwide Corporation, et al. (D. Ariz. 2012) (No. 12 Civ. 1365).
[7] 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://ftc.gov/opa/2012/12/databrokers.shtm.

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 it will be a hot topic of discussion in the data privacy and security community in the days ahead.

Consumer and Business Education

The Commission also promotes better data security practices through extensive use of consumer and business education. On the consumer education front, the FTC sponsors OnGuardOnline.gov, a website designed to educate consumers about basic computer security. Since its launch in 2005, the site has received over 17 million visits.

In addition, the Commission engages in wide-ranging efforts to educate consumers on the issue of identity theft, one of the serious, potential consequences of a data breach. Our efforts focus on providing consumers practical tips on how to avoid having their identities stolen, as well as steps to take if they are victims of identity theft. The FTC's identity theft primer and victim recovery guide[8] have been distributed to millions of consumers in print and online, and every week around 20,000 consumers contact our identity theft hotline and dedicated website for victims.

The FTC does outreach to businesses as well. Our business guide on data security, along with an online tutorial, has been widely disseminated.[9] It is designed to offer practical and concrete advice to businesses—especially small businesses—on how to develop and implement data security plans.

Better Data Security Practices for Businesses

What are the basic steps that businesses can take to minimize the risk of a data breach or security compromise? Much of it is just common sense. First, businesses should build in privacy and security considerations from the start, a concept we call "privacy by design." This means incorporating privacy protections into the development of a business plan or product. Other steps include limiting information collected to just what is truly necessary, securely storing collected data, and safely disposing of data that is no longer needed. This seems so simple, yet many of the data security cases brought by the Commission involve companies who engaged in careless practices, such as dumping sensitive medical or financial records into open trash bins or failing to take basic steps to secure computer networks.

It is critical that businesses honor the promises they make to protect consumers' privacy. This is at the heart of the Commission's law enforcement against deceptive practices. Businesses must live up to the assurances they make regarding security standards.

---

[8] FED. TRADE COM'N, TAKING CHARGE: WHAT TO DO IF YOUR IDENTITY IS STOLEN (2012), *available at* http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

[9] FED. TRADE COM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2011), *available at* http://business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf; Online Tutorial, Fed. Trade Com'n, Protecting Personal Information: A Guide for Business (2011), http://business.ftc.gov/multimedia/videos/protecting-personal-information.

Because breaches may still occur even in the most security-conscious companies, however, it is also critical to have a plan for responding to data breaches before they happen. Putting together a response plan now may help reduce the impact of a data breach on a business and its customers later.

Data Security with New Technologies

New technologies and business models bring great benefits to consumers but also new data security challenges. In the Commission's 2010 case against social networking service Twitter, the FTC charged that serious lapses in the company's data security allowed hackers to obtain unauthorized administrative control of Twitter.[10] As a result, hackers had access to private "tweets" and non-public user information – including users' mobile phone numbers – and took over user accounts. The Commission's order, which applies to Twitter's collection and use of consumer data, including through mobile devices or applications, prohibits misrepresentations about the extent to which Twitter protects the privacy of communications, requires Twitter to maintain reasonable security, and mandates independent, comprehensive audits of Twitter's security practices.[11]

Facial recognition is another technology offering both great benefits and potential risks in the area of data security. This technology can identify a specific face by evaluating and comparing unique biometric data from facial images. This can benefit consumers by, for example, allowing a mobile phone user to use her face, rather than a password, to unlock her phone. Millions of consumers enjoy one of the most prevalent current uses of this technology that enables semi-automated photo tagging or photo organization on social networks and in photo management applications. Facial recognition technology also has particular data security risks, however, because a face is a unique identifier that, unlike a credit card number or ID number, cannot be changed easily if the biometric data information is compromised.

Data Security Legislation

Speaking of faces, some familiar faces from past privacy and data security legislative efforts will be absent in the new Congress, and it will be interesting to see how this will affect the discussion. One effort that had bipartisan support in the past Congress was a federal breach notification and data security law. 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

[10] Complaint, In re Twitter, Inc., No. 092-3093, (F.T.C. June 24, 2010), http://www.ftc.gov/os/caselist/0923093/100624twittercmpt.pdf.
[11] Decision and Order, In re Twitter, Inc., No. 092-3093, (F.T.C. Mar. 2, 2011), http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf.

both consumers and businesses, 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.

Thank you for allowing me to kick off this important day. I am happy to take a few questions.