

**Remarks of FTC Commissioner Maureen K. Ohlhausen**  
**Google Data Security Event**  
**Washington, D.C.**  
**April 17, 2013**

Thank you so much for your kind introduction. I appreciate the invitation to discuss one of the most important and timely topics in the consumer protection area—data security. This is a core issue for the Federal Trade Commission and I would like to share with you our role in regulating it. Let me preface my remarks by saying that my comments are my own and do not necessarily reflect those of my colleagues on the Commission.

Data is an increasingly vital asset, and as companies collect more and more personal information from their customers, they need to protect this information from theft and unauthorized access, which can hurt customers and harm the business' 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.

As with most issues, the FTC approaches its role in data security on several fronts: law enforcement, policy and research, and business/consumer education. This multi-prong approach allows the agency to maximize its impact by challenging the actions of wrong-doers, educating consumers on how to protect themselves and their data, and sharing practical tips and best practices with businesses to help them keep their consumer data secure.

I will begin by sharing with you a bit about the FTC's enforcement record and the types of cases we bring in the data security arena. Next, I will discuss the excellent materials we offer to consumers and businesses alike on data security. Then, 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 for both the FTC and Congress.

### **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<sup>1</sup> under the Gramm-Leach-Bliley Act (GLB)<sup>2</sup>, for example, imposes data security requirements on financial institutions. The Fair Credit Reporting Act (FCRA) requires credit reporting agencies to use reasonable procedures to ensure that recipients of sensitive consumer information have a permissible purpose for receiving that information from the agencies.<sup>3</sup> It also imposes safe disposal obligations on entities that maintain consumer report information.

---

<sup>1</sup> FTC Safeguards Rule, 16 C.F.R. § 314 (2013).

<sup>2</sup> The Gramm–Leach–Bliley Act, 15 U.S.C. §§ 6801-6809 (2006).

<sup>3</sup> The Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (2006).

Additionally, we enforce Section 5 of the FTC Act, which prohibits 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.<sup>4</sup> Under these statutes, we have initiated over three dozen data security cases.

In January, the Commission brought a case against Cbr, a leading cord blood bank, for failing to protect nearly 300,000 customers' personal information, including Social Security numbers, credit and debit card account numbers, and sensitive medical information.<sup>5</sup> 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 failed to take sufficient measures to prevent, detect, and investigate unauthorized access to computer networks.

Last June, 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.<sup>6</sup> 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 that these failures resulted in 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 aids our understanding of how innovations may affect data security and consumer privacy. In this context, the Commission recently began a study of the data broker industry.<sup>7</sup> 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 it will be a hot topic of discussion in the data privacy and security community in the days ahead.

---

<sup>4</sup> 15 U.S.C. § 45.

<sup>5</sup> 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>.

<sup>6</sup> Complaint, FTC v. Wyndham Worldwide Corporation, et al. (D. Ariz. 2012) (No. 12 Civ. 1365).

<sup>7</sup> 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>.

## Consumer and Business Education

The Commission also promotes improved data security practices through extensive use of consumer and business education. On June 4, the FTC is sponsoring a public forum to address security threats facing users of smartphones and other mobile technology. This session will provide an opportunity for the Commission's staff to learn more about data security challenges facing consumers and businesses, as well as educate the public on how to secure and protect their data.

One of the most effective ways the FTC supports data security is through OnGuardOnline.gov, a website designed to educate consumers about basic computer security. Since its launch in 2005, the site has received nearly 20 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 with practical tips on how to protect their identities, as well as steps to take if they have already become victims of identity theft. The FTC's identity theft primer and victim recovery guide have been distributed to millions of consumers in print and online, and every week around 20,000 consumers contact our identity theft hotline and website dedicated to helping victims.

The FTC provides outreach to businesses as well. Our business guide on data security, along with an online tutorial, has been widely disseminated.<sup>8</sup> It is designed to offer practical and concrete advice to businesses—especially small businesses—on how to develop and implement data security plans. We have developed other materials specifically for business through the BCP Business Center, which has a section dedicated to helping businesses learn best practices to protect sensitive data in their possession.<sup>9</sup>

### Better Data Security Practices for Businesses

The saying is that an ounce of prevention is worth a pound of cure, so we strive to provide guidance to businesses on better data security practices. So, 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 phrase means incorporating privacy protections into the development of a business plan or product. Other steps include limiting information collected to what is necessary for business operations, securely storing collected data, and safely disposing of data that is no longer needed. These steps seem 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 concern 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.

---

<sup>8</sup> 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](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>.

<sup>9</sup> FED. TRADE COM'N, <http://business.ftc.gov/privacy-and-security/data-security> (last visited Apr. 17, 2013).

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**

As we look to the future, 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 lapses in the company's data security allowed hackers to obtain unauthorized administrative control of Twitter.<sup>10</sup> 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 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.<sup>11</sup>

Facial recognition is another cutting-edge 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 technology 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 already enjoy one of the most prevalent current uses of this technology, which enables semi-automated photo tagging or photo organization on social networks and in photo management applications. On the other hand, facial recognition technology also creates particular data security risks because a face is a unique identifier that, unlike a credit card number or ID number, cannot be changed easily if the biometric data is compromised.

### **Data Security Legislation**

Speaking of faces, some familiar faces from past privacy and data security legislative efforts are absent in the 113<sup>th</sup> Congress, and it is not yet clear how this will affect the discussion. In the last Congress, there was strong, bipartisan support for data security legislation. One effort that had bipartisan support in the past Congress was a federal breach notification and data security law. There is some ongoing discussion about including this as part of a cybersecurity bill. The theory is that combining two important—and somewhat related—measures would increase the likelihood of passage.

Although the FTC can proceed using its Section 5 authority—and since 2001 has brought almost forty 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 lack of uniformity in the laws means that companies must comply with all of the different state notice requirements, and consumers may get notifications that are substantively different and are triggered by different types of breaches. A single standard would create uniform procedures within companies and would clarify consumer expectations. 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,

---

<sup>10</sup> Complaint, In re Twitter, Inc., No. 092-3093, (F.T.C. June 24, 2010), <http://www.ftc.gov/os/caselist/0923093/100624twittercmpt.pdf>.

<sup>11</sup> 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>.

there are no benefits to consumers or competition from allowing consumer data to be stolen. At the same time, any such law would have to carefully consider what are reasonable precautions for safeguarding various types of data without imposing undue costs that are not justified by consumer benefits.

Thank you for inviting me to speak with you. I am happy to take questions.