Federal Trade Commission

Privacy Today and the FTC s 2014 Privacy Agency

***Jessica Rich*[1]**
Director, Bureau of Consumer Protection, FTC

International Association of Privacy Professionals
December 6, 2013

I. Introduction

Hello. I am delighted to be here among so many familiar faces, talking about the important issue of privacy. I want to thank IAPP for inviting me here today.

As we get ready to greet another new year, I can't help but think about how much the world has changed for consumers in the last few decades – and even just the last few years. Not too long ago, cell phones were a novelty. Now, virtually everyone in this country has a mobile device that they take everywhere, and over half of consumers have smartphones.[2]

Companies across many industries are using increasing amounts of data – Big Data – to create better products and services, tailor their messages to consumers in real time, and develop new solutions to nagging global problems. Big Data has the potential to improve the quality of health care while cutting costs; enable forecasters to better predict the weather and spikes in

[1] The views expressed here are my own and do not necessarily represent the views of the Federal Trade Commission or any Commissioner. Special thanks to Molly Crawford for assisting in the preparation of these remarks.
[2] Nielsen Wire, *America's New Mobile Majority: A Look at Smartphone Owners in the U.S.* (May 7, 2012), *available at* http://blog.nielsen.com/nielsenwire/?p=31688.

energy consumption; and improve industrial efficiencies in order to deliver better, and lower cost, products and services to consumers.

Mobile shopping is exploding. Not only can a consumer buy her winter coat while commuting on her train to the office, but she can compare prices, get reviews, conduct a virtual fitting, and have her purchase posted to her social networking page. All of this capability literally sits in the palm of her hand.

Developments in device connectivity also offer many new conveniences and benefits. Wireless medical and fitness devices can not only chart your fitness goals and progress, but also share your latest blood glucose readings with your doctor. And connected cars promise better navigation systems, remote activation of climate control so you are toasty right when you get in your car, and an easy way to find your vehicle in that huge parking lot at Target.

These are incredible developments, and many consumers – myself included – are embracing them. But they also can be unnerving, even scary. Consumers are asking: where is

consumer data. Next, I will talk about the Commission's privacy agenda for the upcoming year. At the end, I would be happy to take your questions.

II. The Importance of Privacy Today

So let's talk about why privacy is – or should be – so important to businesses today.

For many companies in recent years, privacy has simply been a matter of legal and regulatory compliance, best left to lawyers and IT professionals hired to "take care of it." But increasingly, privacy has become a C-suite issue – part of a broader business strategy as consumer awareness and demand for privacy continues to grow.

There is growing evidence of real consumer concern about privacy, and even consumer reluctance to engage fully in the marketplace as a result. Surveys of consumers show not only rising levels of concern but also concrete actions consumers have taken to shield their personal information. For example, a recent Pew study found that 86% of consumers have taken steps to remove or mask their digital footprints.[3] These include steps ranging from clearing cookies to encrypting email, and from consumers avoiding use of their names to using virtual networks that mask their IP addresses. Surveys also show that younger consumers care about privacy, despite assertions to the contrary. In fact, a second Pew survey found that children and teenagers actively engage with their privacy settings on social networks, often set their profiles to privacy-protective settings, and value the control that the settings provide.[4]

Other evidence of consumer concern comes from their reactions to privacy and security breaches when revealed by the company or in the press. Let me take you *way* back to 2005 and the now infamous ChoicePoint breaches. These incidents provided a good lesson about the business impact of poor privacy and security practices. Due to ChoicePoint's allegedly poor

[3] Pew Research Center, *Anonymity, Privacy, and Security Online* (Sept. 5, 2013), *available at* http://pewinternet.org/Reports/2013/Anonymity-online.aspx.

year, we alleged that social networking app Path deceived consumers by secretly capturing and storing contact information from their mobile device address books without their knowledge or consent.[9] Even apart from the FTC's case, there was a huge public outcry about Path.[10] The

oversight – and, yes, I am sure that's part of it. But companies also sign on to these codes because they think privacy is a selling point with both consumers and their business clients.

Finally, as I think everyone in this audience knows, privacy is critical as we move to an increasingly global economy where data must flow between different privacy regimes for commerce to thrive. This is precisely what the US-EU Safe Harbor is all about – adhering to broadly accepted privacy principles in order to allow data to flow between the US and the EU, which is particularly critical for multinational corporations.[13] This is also why the FTC is working on cross border rules through APEC, which establishes a system of accountability when companies transfer data across national borders.[14] Global frameworks like these are what businesses need to broaden their customer base in the global market, and also to efficiently manage day-to-day operations all over the world.

All of this is mounting evidence that companies can leverage consumers' demand for privacy as part of a broader business strategy. One of the greatest assets a business has is the trust of its customers. Companies that get ahead in privacy – and I should stress that I mean *real* privacy and not just empty promises – can get ahead with consumers.

III. The FTC s Privacy Agenda

Not surprisingly, privacy is a top priority for the Commission. We promote strong privacy protections using all of the tools at our disposal – enforcement, workshops, studies, reports, and consumer and business education and outreach. Over the past few decades, the Commission has brought hundreds of privacy and data security cases targeting violations of the Federal Trade Commission Act, the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act, Do Not Call, CAN SPAM, and the Children's Online Privacy Protection Act (COPPA).

---

[13] *See generally* http://export.gov/safeharbor/eu/eg_main_018365.asp.

Since just 2001, the Commission has brought 44 privacy cases, 47 data security cases, and 21 COPPA cases. We've brought high-profile cases against companies like Facebook, Google, Microsoft, and ChoicePoint; cases against smaller companies engaged in practices of particular concern; and cases challenging unfair and deceptive uses of cutting-edge technology.

The Commission also has distributed millions of copies of educational materials for consumers and businesses to improve their understanding of ongoing threats to security and privacy. And the FTC continues to examine the implications of new technologies and business practices on consumer privacy through ongoing policy initiatives.

We have no intention of slowing down. Our privacy work will continue at a rapid pace in the coming year. We have a full agenda, which can best be described in three basic – and in many ways, overlapping – categories: Big Data; Mobile Technologies and Connected Devices; and Protections for Sensitive Data.

A. Big Data

The first area of focus I will discuss is the phenomenon of Big Data, a phrase that seems to be in vogue when discussing the vast capabilities of companies to gather data from numerous sources and "crunch" it to make inferences about people. Big Data can, of course, drive valuable innovation – for example, it can be used to track traffic patterns in order to ease congested commutes home, or even determine what medical treatments are most effective across a large population. However, the pooling of vast stores of data raises obvious consumer privacy concerns. These concerns stem from the risk of indiscriminate and virtually unlimited data collection without consumer knowledge or consent; the risk of data breaches involving this

[14] *See, e.g.*, FTC Press Release, *FTC Welcomes a New Privacy System for the Movement of Consumer Data Between the United States and Other Economies in the Asia-Pacific Region* (Nov. 14, 2011), *available at* http://www.ftc.gov/opa/2011/11/apec.shtm.

or even across multiple devices, and at a high level of detail.[17] We are working to finalize a report based on our findings from the workshop, and expect to release it in the coming months.

In addition, as we announced just this week, we are planning a three-part "Spring Seminar Series" to shine a light on several trends in Big Data and their impact on consumer privacy.[18] The series will focus on mobile device tracking in retails stores, the use of predictive scoring to help companies predict consumer behavior and shape how they market to particular consumers, and health apps that consumers increasingly use to manage and analyze their health data.

The FTC also will continue to aggressively enforce the FCRA, which sets forth procedures governing the use of data to make decisions about whether to give consumers credit, a job, or insurance.[19] The FCRA covers some of the practices of greatest concern when it comes to Big Data and remains a highly effective tool.

For example, the Commission recently obtained a $3.5 million penalty from Certegy, a company that advises merchants on whether to accept consumers' checks, based on their past financial history.[20] The complaint alleged that Certegy violated the FCRA by failing to have appropriate dispute procedures and failing to maintain the accuracy of the information it provided to merchants. This resulted in consumers – many of them elderly – being denied the ability to write checks and obtain essential goods and services.

We also sent warning letters to companies that were skirting too close to the FCRA line. Earlier this year, we conducted undercover test shops and issued warning letters to ten data

[17] FTC Workshop, *The Big Picture: Comprehensive Online Data Collection* (Dec. 6, 2012), *available at* http://www.ftc.gov/bcp/workshops/bigpicture/.

[18] FTC Press Release, *FTC to Host Spring Seminars on Emerging Consumer Privacy Issues* (Dec. 2, 2013), *available at*

security to baby monitoring, and claimed in numerous product descriptions that they were "secure." In fact, the cameras had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet address. This resulted in hackers posting 700 consumers' live feeds on the Internet. Under the FTC settlement, TRENDnet must maintain a reasonable security program, obtain outside audits, notify consumers about the security issues and the availability of the software update to correct them, and provide affected customers with free technical support for the next two years.

C. Protecting for Sensitive Data

A third area of focus is providing strong safeguards for sensitive data involving children, health information, and financial data. The FTC has long been concerned that this type of sensitive data warrants special protections.

When it comes to protecting children's privacy, this has been a big year at the FTC. In July, the final Children's Online Privacy Protection Act (COPPA) Rule went into effect. The Rule strengthens kids' privacy protections and gives parents greater control over the personal information that websites and online services may collect from children under 13.[29]

The FTC updated the Rule to respond to collection practices made possible by new technology – namely, data-gathering tools like social media and mobile applications. To assist the business community with compliance, the Commission has sought to educate companies through a variety of means such as webinars, a compliance hotline, the business center blog, and other business guidance. Since going into effect, the FTC has been mindful of the impact of the Rule on businesses and has exercised prosecutorial discretion in enforcing the Rule, particularly with respect to small businesses that have attempted to comply in good faith in the early months

[28] *In the Matter of TRENDnet, Inc.*, Matter No. 122-3090 (Sept. 4, 2013), *available at* http://www.ftc.gov/opa/2013/09/trendnet.shtm.
[29] 16 C.F.R. Part 312.

after the Rule became final. However, as we approach six months since the effective date of the Rule, the FTC will begin to ramp up enforcement where needed to ensure compliance.

The Path case, which I mentioned earlier, illustrates the importance of kids' privacy and COPPA. Social networking app Path didn't just capture personal information from adults' address books; it also captured address book information from kids' devices, including full names, addresses, phone numbers, email addresses, dates of birth and other information, where available. In addition, Path enabled children to create personal journals and upload, store, and share photos, written "thoughts," their precise location, and the names of songs to which the child was listening. According to the complaint, Path did this without obtaining parental consent, in violation of COPPA.[30] The order required Path to pay $800,000 civil penalty, delete information from kids under 13, and prohibits Path from engaging in future violations.

In the area of health data, the FTC recently brought two cases of particular interest. 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.[31] 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 related allegations that Cbr failed to take sufficient measures to prevent, detect, and investigate unauthorized access to computer networks.

Most recently, the FTC filed a complaint against LabMD, a medical testing lab whose security we allege is unreasonable.[32] For example, the complaint alleges that LabMD's lax security enabled a high-level official to install a peer-to-peer (P2P) file-sharing application on a

---

[30] *U.S. v. Path, Inc.*, No. C-13-0448-JCS (N.D. Cal. Filed Jan. 31, 2013), *available at* http://www.ftc.gov/opa/2013/02/path.shtm.

[31] *In the Matter of Cbr Systems, Inc.*, Docket No. C-4400 (Apr. 29, 2013), *available at* http://www.ftc.gov/os/caselist/1123120/130503cbrcmpt.pdf.

[32] *In the Matter of LabMD, Inc.*, Docket No. 9357 (Aug. 28, 2013), *available at* http://www.ftc.gov/opa/2013/08/labmd.shtm.

Bureau enforce the online advertising principles of the Digital Advertising Alliance (DAA)[34] – and we want those efforts to continue.

Best wishes for the upcoming year. I am happy to take questions.

[34] *See, e.g.*, Better Business Bureau Press Release, *Accountability Program Instructs Advertiser, Agency and Platform to Work Together to Deliver AdChoices Icon* (Nov. 20, 2013), *available at* http://www.bbb.org/council/migration/bbb-news-releases/2013/11/accountability-program-instructs-advertiser-agency-and-platform-to-work-together-to-deliver-adchoices-icon/; Better Business Bureau Press Release, *Accountability Program Decisions Throw Spotlight on Website Operators' Compliance* (Nov. 18, 2013), *available at* http://www.bbb.org/council/migration/bbb-news-releases/2013/11/accountability-program-decisions-throw-spotlight-on-website-operators-compliance/.