Federal Trade Commission

The FTC's Privacy and Data Security Program: Where It Came From, Where It's Going

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

International Association of Privacy Professionals
Global Privacy Summit
March 6, 2014

Hello. I am delighted to be here again at IAPP, talking about the FTC's priorities and approach to privacy.

To set the stage for the broader discussion with the group, I'll start out with some high-level background on the origins of our privacy program, the challenges we see today, and our agenda for the coming year.

I. The Origins the FTC's Privacy Program

The world has changed enormously since the FTC first began working in the privacy area. Although we've been enforcing the Fair Credit Reporting Act since the 1970s, our current privacy program dates from the mid-90s. At that time, we held a

[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.

series of hearings on the consumer protection issues raised by the growth of the Internet. The hearings identified privacy as a critical and growing issue for consumers, due to the interactive nature of the new medium and the increased ability to collect data from consumers in real time. Privacy was seen as an important issue for businesses too, if they wanted to ensure the health and survival of the Internet as a commercial medium. We did not plan the hearings that way; privacy emerged from the discussion as a huge and fascinating surprise. So we turned our attention to the issue, using the various enforcement, policy, and educational tools at our disposal.

From the start, our privacy program was a combination of strict application of the law, on the one hand, and bully pulpit on the other. On the law enforcement side, we developed cases and entered into consents based on alleged evidence that companies had violated Section 5 – that is, they had engaged in unfair or deceptive practices.[2]

I want to emphasize that this is the same Section 5 that we have used for decades to challenge practices involving deceptive advertising and fraud; and the same Section 5 that has been litigated and developed in the courts. There is no separate privacy and data security jurisprudence, but simply application of a tried and true Section 5 standard to the data security context, just as the law has been applied to pyramid schemes, business opportunity scams, weight loss products, cramming, and many other areas of consumer protection.

---

[2] Many of the Commission's cases in the privacy area also enforce other, more specific statutes and rules, including the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Children's Online Privacy Protection Act, Do Not Call, and the CAN SPAM Act.

On the bully pulpit side, we exhorted companies to provide stronger privacy protections through surveys, workshops, reports, testimony, speeches, and education. These initiatives did not necessary reflect the current law; indeed, they often sought to move beyond it by encouraging companies to implement "best practices" over and above the law, or by recommending that Congress pass new and stronger laws.

In the early days, it wasn't so much a matter of implementing *stronger* protections but implementing any protections at all, including simply describing to consumers, in a prominent place on the website, what data the company collected and how it would be used. Yes, you can blame the FTC for privacy policies. In the mid-90s, there were none; there was no way to tell what a company was doing with data and no accountability. So we pushed companies to post privacy policies and we were quite successful in those efforts. The idea, of course, was that consumers could use privacy policies to make choices about whether to do business with particular companies, which would in turn make companies more responsive to consumers, their customers.

II. The Challenges Today

The very idea of a privacy policy illustrates just how dramatically the privacy landscape – indeed, the whole commercial landscape – has changed since the mid-90s. It rests on the notion that businesses collect information directly from consumers, and that businesses and consumers will have a negotiation of sorts about privacy as the information is collected. That idea was a stretch even then, but it seems truly absurd today.

Today, most of the companies that obtain consumer data are behind the scenes and never interact with consumers. Privacy policies – if you have the will and ability to find them – are impenetrable. And data is collected from consumers at every turn, all day long – on the internet, through their mobile phones and other connected devices, in stores and malls, and in their cars and kitchens. These are the challenges that the FTC is dealing with in its privacy program today.

For example, a consumer may start off her day wearing a connected device to track her health and fitness as she exercises in the morning. She may check her bank account balance online, to see if that check came through. When she gets to work, she provides sensitive information to her employer, such as her Social Security number and bank account number. On the way home, she may visit her local grocery store and use a loyalty card to get discounts on purchases. Or she may use a social networking app to find her friends at a local restaurant, and a mapping app to get there. When she gets home, she may update her social networking page and browse the web for news and to shop. And increasingly, she is doing all of this through her smartphone, which is tracking her location everywhere she goes.

These activities clearly benefit the consumer – we all want our smartphones and our apps and our discounts and our paychecks. But it's an order of magnitude we never would have imagined in those early days, when we were bowled over by the "real time" data collection enabled by the Internet. Where is all of this data going, and who has access to it and for what purposes?

The fact is, all of this data can be stored by the companies that collect it, and used for purposes well beyond the original collection – for marketing other products and services; to decide what content the consumer sees when they do a search; to set prices for consumers; to make decisions about important consumer benefits, such as eligibility for credit, employment, or insurance; and to sell to other companies the consumers have no idea exist.

Those other companies include data brokers, behind-the-scenes entities that combine data from multiple sources, develop detailed profiles on consumers, and sell it for all of the purposes I just described and more. And, of course, many of the companies that get all of this data may not store it securely, as shown by all of the breaches we are seeing in the marketplace. This Big Data phenomenon is a very Big Deal for consumers.

So what is the FTC doing about it? Our privacy agenda for 2014 focuses on three themes that reflect the challenges today: Big Data, Mobile and Connected Devices, and Protecting Sensitive Information.

There's actually a fourth too – which is the critical need for privacy and data security legislation. Legislation in both of these areas would protect consumers across the many contexts in which their data is collected, and would level the playing field and provide clear rules of the road for businesses. Since this panel is about the FTC's privacy work, however, I'll focus on the things that are more under our control for now.

III. The FTC's Privacy Priorities for 2014

Big Data

Our three priorities are in many ways overlapping, but I'll try to tackle them one-by-one. First is Big Data. This term is used in various ways, but I'm using it to describe the vast capability of companies to gather data from numerous sources and combine it in ways to make inferences about people. In other words, it's the narrative I just discussed.

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 determine what medical treatments are most effective across a large population. However, it also raises obvious risks for consumers – virtually unlimited data collection without consumers' knowledge or consent; data breaches involving this treasure trove of information; the risk that data will be obtained by identity thieves and other scam artists; and the concern that companies will make inferences about consumers that simply aren't true.

Our activities on the Big Data front include the release of a report on data brokers in the coming months. We have long been concerned about the lack of transparency among data brokers, particularly because they collect and use so much consumer data without any interaction with the consumer. And the Commission is on record having supported legislation to address concerns about data brokers. The primary purpose of the upcoming report is to shine a light on the data broker industry and increase awareness about its practices.

In addition, we are hosting a series of workshops to start a dialogue on several trends in Big Data and their impact on consumer privacy. We held the first one last December, focused on the Internet of Things. And we are in the midst of our Spring Seminar Series on three other topics – mobile device tracking in retail 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.

Also, the FTC will continue to aggressively enforce the FCRA, which sets forth procedures governing some of the most important uses of Big Data – determining whether to give consumers credit, a job, or insurance. Recently, for example, we brought two cases against companies that advise merchants on whether to accept consumers' checks, based on their past financial history. The complaints alleged that the companies (TeleCheck and Certegy) violated the FCRA by failing to have appropriate procedures for consumers to dispute potential errors in their financial histories and failing to maintain the accuracy of the data provided to merchants. These types of violations can cause consumers to be denied the ability to write checks and obtain essential goods and services, like food and medicine, based on errors in the data maintained about them. Each company paid a $3.5 million penalty as part of the settlement of these actions.

Mobile Technologies and Connected Devices

A second area of focus is mobile technologies and connected devices. Over the last few years, mobile technology has become one of the main priorities for the Commission – in privacy and more generally – for several reasons.

First and most basic, commerce is going mobile and consumer protection need to keep up. Second, mobile technologies raise new challenges for consumer protection, due to the always-with-you, always-on nature of mobile devices; the ability of these devices to track you location and connect to each other; and of course the small screen or, increasingly, no screen.

On the policy front, the FTC has already issued several reports, including two reports showing the lack of mobile privacy disclosures about how kids apps are collecting and using data; a report making recommendations on mobile privacy disclosures; and a mobile payments report. We also hosted a workshop on mobile security last year.

We also have brought enforcement actions challenging law violations occurring in the mobile ecosystem. For example, the FTC announced a settlement with Goldenshore Technologies, the maker of Brightest Flashlight, a popular app – installed more than 50 million times – that allows consumers to use their mobile devices as flashlights. According to the complaint, Goldenshore promised that it would collect information from users' mobile devices for certain internal housekeeping purposes, but failed to disclose that the app transmitted the device's location and precise device ID to third parties, including mobile advertising networks.

Our work on the Internet of Things, which I just mentioned in discussing Big Data, also falls into this mobile category. In the next few months, we'll be issuing a report on our workshop. Also, the FTC recently announced its first "Internet of Things" case involving a video camera designed to allow consumers to monitor their homes remotely. The complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from home 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 even in some cases listening, resulting in hackers posting 700 consumers' live feeds on the Internet.

Protecting for Sensitive Data

A third area of focus is providing strong safeguards for sensitive information – that is, kids', health, or financial data. Protecting sensitive information isn't really a new priority – it's one of those bedrock privacy principles that was here at the beginning and will be here at the end. But the changes I've been talking about – the ubiquitous and invisible data collection that takes place all the live-long day – raise the stakes for sensitive data as consumers buy their children smartphones, strap on health and exercise devices, and make purchases through their mobile devices, all without knowing where their information is going or who will get it.

We care about sensitive data for two primary reasons. First, the risk of harm is often increased. Second, consumers generally have a greater expectation of privacy with respect to their children's, financial, and health data.

One example of our work to protect sensitive data is our recent cases against GMR Transcription Services, an audio file transcription service. This is actually our 50th data security settlement, a big milestone for us. According to the complaint, GMR relied on service providers and independent typists to transcribe files for their clients, which include healthcare providers. As a result of GMR's failure to implement reasonable security measures and oversee its service providers, at least 15,000 files containing sensitive personal information – including consumers' names, birthdates, and medical histories – were available to anyone on the Internet.

Other work in this area also includes our update of COPPA last year – to address to increasing use of interactive technologies by kids – and our ongoing litigation of the Wyndham and LabMD cases.

IV. Conclusion

This was just a brief overview of "where we have been and where we are going." We obviously have important work that doesn't fall neatly into these categories, such as the work we are doing to strengthen and enforce the U.S./E.U. Safe Harbor Agreement. I'm happy to answer any questions as part of the broader discussion with the group.