Federal Trade Commission

Quis Custodiet Ipsos Custodes?
(Who Watches the Watchers?)

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

American Bar Association
62nd Spring Meeting of the ABA Section of Antitrust Law
March 26, 2014

Hello. I am delighted to be here with this incredible panel. I'll take my turn in weighing in on some of the privacy issues already discussed, as well as the role of the FTC in this important area.

I. The Privacy Challenges Today

Like many of the other panelists, I've been working on privacy issues for years – in my case, since the mid-to-late 90s, when the FTC first launched its privacy program. I'd like to start with a brief trip down memory lane because it provides some good context for the privacy challenges we face today.

[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.

The FTC launched its privacy program in large part to respond to changes in the marketplace brought about by the growth of the Internet. The interactive nature of the new medium raised concerns about the ability of companies to collect more data from consumers in real time, and to use and share that data instantly, for unknown purposes. These changes seemed pretty dramatic at the time.

In the early days of our privacy program, it wasn't so much a matter of implementing *stronger* privacy 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. In other words, 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. The idea behind privacy policies, of course, was that consumers could use them to make choices about whether to do business with particular companies, which would in turn make companies more responsive to consumers, their customers.

This idea shows just how dramatically the landscape has changed since the mid-90s. It assumes 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 assumption seems absurd today, doesn't it?

Today, most of the companies that obtain consumer data are behind the scenes and never interact with consumers. These companies include hundreds of data brokers that collect and combine data from multiple sources and develop detailed profiles for sale to

other companies. 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, in stores and malls, and through devices in their cars and as they exercise.

In addition, the data is used for numerous purposes, well beyond the original collection – for marketing products and services; to decide what content the consumer sees when they do a search; to set prices for consumers; and to make decisions about eligibility for important benefits. And, of course, the companies that obtain and use all of this data may not store it securely, as shown by all of the breaches we are seeing in the marketplace. These are the many challenges that consumers – and we at the FTC – are dealing with today.

II. The FTC's Privacy Priorities for 2014

Our privacy agenda for 2014 focuses on three themes that reflect these challenges: Big Data, Mobile and Connected Devices, and Safeguarding Sensitive Data. These priorities are in many ways overlapping, but I'll take them one-by-one.

Big Data

First is Big Data. Big Data can, of course, drive valuable innovation – for example, it can be used to determine what medical treatments are most effective across a large population. However, it also raises obvious risks for consumers – virtually unlimited data collection without their knowledge or consent; data breaches involving this

treasure trove of information; 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. The purpose of the report is to shine a light on the data broker industry and promote greater transparency 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're in the midst of our Spring Seminar Series on three other topics – mobile device tracking in retail stores, the use of alternative scoring models to help companies predict consumer behavior; and data collection by health apps and devices that consumers increasingly use to manage their health data.

The FTC also 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 announced settlements with two companies that advise merchants on whether to accept consumers' checks, based on their financial history. The complaints alleged that TeleCheck and Certegy failed to have appropriate procedures to maintain the accuracy of consumers' data and correct errors – failures that can cause consumers to be denied the ability to write checks. The companies each paid a $3.5 million civil penalty to settle the charges.

Mobile Technologies and Connected Devices

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

Clearly, the marketplace is moving to mobile, and consumer protection needs to move with it. But it's not just "old wine in new bottles." Mobile technologies also raise special consumer protection challenges, due to the always-with-you, always-on nature of mobile devices; the ability of these devices to track your location and connect to each other; and, of course, the small screen or, increasingly, no screen at all.

On the policy front, the FTC has already issued several reports about kid's apps, mobile privacy disclosures, and mobile payments. We also hosted a workshop on mobile security last year.

We 've also 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 that allows consumers to use their mobile devices as flashlights. We alleged that Goldenshore promised it would collect data from users' devices for certain internal housekeeping purposes, but failed to disclose that the app transmitted the device's location and device ID to third parties.

The FTC's work on the Internet of Things, which I just mentioned, also falls into this mobile category. We'll be issuing a report on our workshop this year. 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 that they were "secure." In fact, the cameras had faulty software that allowed hackers to post consumers' live feeds on the Internet.

Safeguarding Sensitive Data

A third area of focus is providing strong safeguards for sensitive information – that is, kids', health, financial, and precise geo-location data. This 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 day long – 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.

Our work to protect sensitive data includes the 50 settlements we've obtained against companies that failed to secure consumers' data – including companies such as Microsoft, DSW, BJ's Warehouse, TJX, and Lifelock. Our most recent settlement – our 50th – against GMR Transcription Services – is a good example. According to our complaint, GMR relied on service providers to transcribe files for its clients, which included 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 data – including consumers' names, birthdates, and medical histories – were available to anyone on the Internet.

III. The Need for Legislation

Now, I don't do any speaking these days without making a pitch for privacy and security legislation. As I think our track record shows, the FTC has very strong tools to protect consumers, and we are using all of them. To date, we've brought hundreds of cases using out existing authority, protecting many millions of consumers. However, there's a critical need for new legislation to enhance the FTC's authority and provide stronger protections for U.S. consumers.

The Chairwoman is actually on the Hill today, reiterating the Commission's strong bipartisan call for Congress to enact legislation that would require companies to implement reasonable data security measures, and provide breach notification to consumers in certain circumstances. Almost a decade ago, the famous breach by data broker ChoicePoint was considered a "wake up" call to industry and the public about this important issue. But we've had so many wake up calls during the past decade – think TJX, and the many others I mentioned – but still no legislation.

The current Commission hasn't weighed in on privacy legislation. But many of us strongly support a baseline privacy law, as well as legislation requiring data brokers to provide consumers with reasonable access to the information they maintain about them.

Legislation would protect consumers across the many contexts in which their data is collected, create consistent standards and level the playing field for businesses, and

make non-consumer facing businesses like data brokers accountable. The changes that I talked about in the beginning of my remarks – ubiquitous data collection by more and more behind-the-scenes entities – have pushed us to the tipping point.

IV. Conclusion

Thanks again for including me here today. I'll be happy to answer questions.