# Federal Trade Commission

## Making Every Day "Data Privacy Day"

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

**Data Privacy Day – Keynote Introductory Remarks**
**January 2014**

### I. Introduction

Hello. I am delighted to be here to help kick off Data Privacy Day. I want to thank the National Cyber Security Alliance and my friend Dan Caprio for inviting me.

Today's consumers face privacy challenges wherever they go. Understanding the complex transfers of personal information that occur in the offline and online marketplaces is a daunting task, and these data flows take place in almost every conceivable part of our daily lives.

For example, a consumer may start off her day by putting a device on her wrist to track her health and fitness. She then goes to work and provides sensitive information to her employer, such as her Social Security Number to verify her employment eligibility, and her bank account number so she can get paid. After work, she visits her local

[1] The views expressed here are my own and do not necessarily represent the views of the Federal Trade Commission

grocery store and uses a loyalty card to get discounts on purchases. And upon returning home, she logs onto her computer and begins browsing the web and updating her social networking page.

All of these activities clearly benefit our consumer – she gets paid, enjoys free and immediate access to information, obtains discounts on purchases, stays connected with friends, tracks her health and fitness goals, and entertains herself and her family. Her life is made easier and better in a myriad of ways because of data flows. These are incredible developments and many consumers – myself included – are embracing them.

But they also raise serious concerns about where all of this data is going, and who has access to it and for what purposes. In this case, data about the consumer's grocery store purchases and web activities, as well as the health data from her connected device, may be collected and then sold to data brokers and other companies she does not know exist. These companies could use her information to market other products and services to her; make decisions about her eligibility for credit, employment, or insurance; and share with yet other companies. And many of these companies may not maintain reasonable safeguards to protect the data they maintain about her.

## II. The Challenges Today

Raising public awareness about these privacy issues is what Data Privacy Day is all about. And, of course, at the agency I work – the Federal Trade Commission – every day is Data Privacy Day. Protecting consumer privacy is one of the Commission's highest priorities and has been for decades.

---

or any Commissioner. Special thanks to Molly Crawford for assisting in the preparation of these remarks.

We'd like to make every day Data Privacy Day for consumers and businesses too. But today's privacy challenges are greater than they have ever been. While certain privacy concerns – for example, those raised by data brokers and credit reporting agencies – have long existed in the offline world, new online business models – such as social networking, mobile and location-based services, and the Internet of Things – complicate the privacy picture significantly. These models raise the stakes for all of us by permitting ever more collection, use, and sharing of data, and ever more combining, analyzing, and deducing of facts, characteristics, and likelihoods. They also make it difficult to provide meaningful disclosures and choices to consumers – for example, small screens on mobile devices and no screens whatsoever for some connected device complicate the issue of notice significantly**.** That is why many of us at the Federal Trade Commission strongly support enactment of new privacy and new data security legislation – to protect consumers across the many contexts in which their data is collected, and level the playing field and provide clear rules of the road for businesses.

But regardless of legislation, there is so much that we can and must do now to address privacy. In an era of massive data breaches and ubiquitous social networking and mobile devices, when consumers are becoming increasingly wary and worried about how companies are collecting and using their data, and at a time when we are being told that it's impossible to require transparency among data brokers collecting vast stores of consumer data because there are just too many of them, it has never been more urgent to address this important consumer issue. I'd like to take a few minutes to talk about what

the FTC is doing to protect consumer privacy, as well as the vital role the business community must play in providing more robust protections than we have today.

## III. The FTC's Privacy Agenda

The FTC promotes strong privacy protections using all of the tools at its disposal – law 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, the Gramm-Leach-Bliley Act, Do Not Call, CAN SPAM, and the Children's Online Privacy Protection Act. We've brought high-profile cases against companies like Facebook, Google, Microsoft, and ChoicePoint, as well as cases against smaller companies engaged in practices of particular concern – for example, deceptive tracking of consumers online, or failure to protect sensitive medical data.

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. Today, I'm delighted to announce the release of our updated version of *Net Cetera: Chatting with Kids About Being Online*, our guide to help parents and other adults talk to kids about being safe, secure, and responsible online.[2] This new version deals with such topics as mobile apps, public Wi-Fi security, text message spam, and updated guidance on COPPA.

And the FTC continues to examine the implications of new technologies and business practices on consumer privacy through workshops and other policy initiatives.

You can expect this year to be as busy as ever. We have an active agenda for 2014. It focuses on three basic – and in many ways, overlapping – themes: Big Data; Mobile Technologies and Connected Devices; and Protections for Sensitive Data.

Big Data

The term Big Data describes the vast capabilities of companies to gather data from numerous sources and combine it in ways 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 risks: virtually unlimited data collection without consumer 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. Data brokers collect, maintain, and sell a wealth of information about consumers, but they often do not interact directly with consumers.[3] Rather, they get data from public records or purchase it from other companies. As a result, consumers are often unaware of the existence of data brokers, let alone the purposes for which they collect and use consumers' data. The primary purpose of the upcoming report is to shine a light on the data broker industry and increase awareness about its practices.

---

2 *See* http://www.onguardonline.gov/articles/pdf-0001-netcetera.pdf.

3 *See, e.g., Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers* at 68 (Mar. 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf ("Privacy Report").

In addition, next month we are planning to hold the first of a three-part "Spring Seminar Series" to start a dialogue on several trends in Big Data and their impact on consumer privacy.[4] 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.

Finally, the FTC will continue to aggressively enforce the Fair Credit Reporting Act (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.[5] Recently, for example, the Commission obtained a $3.5 million penalty from TeleCheck, a company that advises merchants on whether to accept consumers' checks, based on their past financial history.[6] The complaint alleged that TeleCheck 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.

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 privacy priorities for the

4 FTC Press Release, *FTC to Host Spring Seminars on Emerging Consumer Privacy Issues* (Dec. 2, 2013), *available at* http://ftc.gov/opa/2013/12/springprivacy.shtm.
5 15 U.S.C. §§ 1681-1681x.
6 *U.S. v. TeleCheck Servs., Inc.*, No. 1:14-cv-00062 (D.D.C. Jan. 16, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/01/telecheck-pay-35-million-fair-credit-reporting-act-violations.

Commission. 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;[7] a report making recommendations on mobile privacy disclosures;[8] and a mobile payments report.[9] We also hosted a workshop on mobile security last year.[10]

We also have brought cases 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.[11] 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.

Of course, mobile is just the tip of the technology iceberg; beyond computers and smartphones, our world is getting more and more connected. Today, consumers can connect remotely to their refrigerators, bank accounts, thermostats, cars, and many other

7 FTC Staff Report, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (Dec. 2012), *available at* http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf; FTC Staff Report, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.

8 FTC Staff Report, *Mobile Privacy Disclosures: Building Trust Through Transparency* (Feb. 2013), *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.

9 FTC Staff Report, *Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments* (Mar. 2013), *available at* http://www.ftc.gov/os/2013/03/130306mobilereport.pdf.

10 FTC Workshop, *Mobile Security: Potential Threats and Solutions* (June 4, 2013), *available at* http://www.ftc.gov/bcp/workshops/mobile-security/.

11 *In the Matter of Goldenshores Technologies LLC & Erik M. Geidl*, File No. 132-3087 (Dec. 5, 2013), *available at* http://www.ftc.gov/opa/2013/12/goldenshores.shtm (settlement agreement).

products and devices. In December, the FTC held a workshop on this phenomenon known as the "Internet of Things."[12] The workshop examined increased connectivity in areas such as smart homes, connected health and fitness devices, and connected cars. The workshop also explored the challenges in this area, such as the difficulty of providing traditional notice and choice in the Internet of Things space and the fact that many players in this arena, such as auto manufacturers, have little experience with privacy and security issues. Following the workshop and a public comment period, we are developing a report to summarize the findings and potentially recommend some best practices for managing privacy and security in this area.

The FTC also recently announced its first "Internet of Things" case involving a video camera designed to allow consumers to monitor their homes remotely.[13] 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 data involving children, health information, and financial data. The FTC has long been concerned that this type of sensitive data warrants special protections.

12 FTC Workshop, *Internet of Things: Privacy & Security in a Connected World* (Nov. 19, 2013), *available at* http://www.ftc.gov/bcp/workshops/internet-of-things/.

For example, last year the FTC's final Children's Online Privacy Protection Act Rule went into effect. The new Rule responds to collection practices made possible by new technology – namely, data-gathering tools like social media and mobile applications – and gives parents greater control over the personal information that websites and online services may collect from children under 13.[14]

Also last year, the Commission settled 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.[15]

Finally, in its most recent case – notably, its 50th data security settlement – the FTC settled allegations that GMR Transcription Services – an audio file transcription service – violated the FTC Act.[16] 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.

---

13 *In the Matter of TRENDnet, Inc.*, Matter No. 122-3090 (Sept. 4, 2013), *available at* http://www.ftc.gov/opa/2013/09/trendnet.shtm.

14 16 C.F.R. Part 312.

15 *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.

16 *In the Matter of GMR Transcription Servs., Inc. et al.*, Matter No. 122-3095 (Jan. 31, 2014) (settlement agreement), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/122-3095/gmr-transcription-services-inc-matter.

These are just a few examples of the FTC's commitment to protecting the security of consumers' sensitive information, but they emphasize principles that are common to all of our data security cases. Most critically, the touchstone of the Commission's approach to data security is "reasonableness" – a company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to prevent and reduce vulnerabilities.

Using this approach, the Commission has challenged practices that were unreasonable in light of the full range of circumstances. None of our cases have challenged isolated mistakes or have been "close calls." Rather, we've considered the company's practices as a whole, whether the risks to data were reasonably foreseeable, what tools were available and in use in the marketplace at the time, and the costs and benefits of implementing various protections. These factors are very much within a company's ability to learn and consider for itself, and it's essential for all companies to undertake this responsibility.

## IV. How Businesses Must Protect Privacy

And that brings me to the vital role that companies must play in protecting privacy – for consumers and for themselves.

Businesses must invest in privacy. Increasingly, privacy has become part of a broader business strategy as consumer awareness and demand for privacy continues to grow. Indeed, surveys of consumers show growing concerns about privacy, and even

their reluctance to engage fully in the marketplace as a result.[17] And the business impact of a security breach or of failing to adequately consider privacy is enormous. Take, for example, Target's recent revelations of a security breach involving upwards of 40 million consumers.[18] The company's loss of goodwill and reputational injury is still unfolding.

And more than ever before, transparency and consumer choice have become selling points for business. Take, Acxiom, the nation's largest data broker. In response to calls for greater transparency among data brokers, Acxiom has launched a web-based tool, "About the Data," that allows consumers to view portions of their marketing profile.[19] While it still has a long way to go and is by no means a perfect tool, it is a step in the right direction.

In addition, privacy is more critical than ever as we move to an increasingly global economy where data must flow between different privacy regimes for commerce to thrive. Global frameworks like the US-EU Safe Harbor[20] and APEC[21] permit data to flow across borders with accountability and oversight. 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.

---

17 For example, a recent Pew study found that 86% of consumers have taken steps to remove or mask their digital footprints such as clearing cookies, encrypting email, avoiding use of their names, and using virtual networks to mask their IP addresses. *See* Pew Research Center, *Anonymity, Privacy, and Security Online* (Sept. 5, 2013), *available at* http://pewinternet.org/Reports/2013/Anonymity-online.aspx.

18 *See, e.g.*, Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow*, N.Y. Times, Jan. 10, 2014, *available at* http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?_r=0.

19 *See generally* https://aboutthedata.com/.

20 *See generally* http://export.gov/safeharbor/eu/eg_main_018365.asp.

21 *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.

All of this is mounting evidence that 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.

Now, for all of the increasing challenges and changes in technology we've discussed, privacy still boils down to some essential principles. The FTC laid these out in its 2012 Privacy Report[22] and we encourage companies to keep coming back to them as they design their privacy and security programs.

First, we have called on companies to incorporate Privacy by Design by baking privacy and security protections into the development of products and services from the start, and thinking about these issues throughout every stage of development. By considering privacy and security from the beginning, companies can develop protections that are in harmony with their business models and compatible with innovation.

Second, companies should address basic transparency by improving the ways they communicate with consumers about how their data is collected and used. Sure, companies should write clearer privacy policies but, more importantly, they should find ways to communicate with consumers outside privacy policies – in the context of their interactions with consumers about the services they're providing.

Third, companies should give consumers easy-to-exercise choices for practices that would come as a surprise, given their relationship with the consumer. For example, if you're an auto dealer, your customers might expect you to send them a coupon for an oil change. But they wouldn't expect you to sell their data to a data broker, who then

appends it to a larger profile to sell to marketers. So tell your customers about that beforehand, and give them a choice.

## V. Conclusion

In closing, whether motivated by the bottom line, connecting with customers, or enforcement responsibilities or oversight, we all have a shared interest in privacy – because it's really all about consumer trust. Building and maintaining trust ultimately fosters innovation and growth in the marketplace. And it has never been more important for all of us to do our part. Thank you for allowing me to help celebrate Data Privacy Day with you.

22 *See supra* note 2.