Federal Trade Commission

The FTC's Privacy and Data Security Priorities for 2015

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

Privacy and Cybersecurity Roundtable
Sidley Austin LLP
March 3, 2015

Good afternoon. I'm delighted to be here in such good company. I've been asked to discuss the FTC's role and priorities in consumer privacy and data security. These are very important topics for us, so I always welcome the opportunity to discuss them.

I. The FTC's Jurisdiction and Authority

I'll start with a little background. Many of you are familiar with the FTC, but here's a quick FTC 101for those that aren't.

The FTC has broad jurisdiction covering most non-bank entities. We are first and foremost a law enforcement agency, and we enforce various laws applicable to many different types of businesses and business activities. Our primary authority is Section 5

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

of the FTC Act, which prohibits unfair and deceptive trade practices in or affecting commerce.[2] The basic rules are that companies cannot make deceptive claims about things that matter to consumers, or cause substantial injury to consumers in ways that consumers cannot avoid and in ways that do more harm than good. The FTC Act is flexible by design, and we've used our authority to challenge a wide range of practices related to consumer fraud, false and misleading advertising, financial products and services, and consumer privacy and data security.

The Commission also enforces a number of sector-specific statutes. In the privacy area, these laws include the Fair Credit Reporting Act, which protects the privacy and accuracy of sensitive consumer report information;[3] the Gramm-Leach-Bliley Act, which mandates privacy and security requirements for non-bank financial institutions;[4] the Children's Online Privacy Protection Act;[5] the CAN-SPAM Act;[6] and the Telemarketing and Consumer Fraud and Abuse Prevention Act[7] and the associated Do Not Call Rule.[8] Under these laws, the Commission has brought hundreds of privacy and security-related cases over the past few decades.

In addition, the FTC educates consumers and businesses, conducts studies, testifies before Congress, hosts workshops, and writes reports regarding the privacy and security implications of technologies and business practices that affect consumers. We issue educational materials on a wide range of topics – from mobile device security to

[2] 15 U.S.C. § 45(a).
[3] 15 U.S.C. §§ 1681–1681x.
[4] *See* 16 C.F.R. Parts 313 & 314, implementing 15 U.S.C. § 6801(b).
[5] 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312.
[6] 15 U.S.C. §§ 7701-7713; *see also* 16 C.F.R. Part 316.
[7] 15 U.S.C. §§ 6101-6108.
[8] 16 C.F.R. Part 310.

kids' online safety to preventing and repairing identity theft, our top source of consumer complaints from year-to-year. Our outreach efforts are designed to prevent law violations and harm before they happen, and are therefore integral to our mission.

We are not the only federal agency working on privacy and data security issues, but we have the broadest jurisdiction in this area, and I think it's fair to say we've been the most active and the loudest over the past two decades. In areas where we share jurisdiction with our sister agencies, we coordinate to ensure a consistent approach, avoid duplication, and sometimes to bring joint actions. Notably, we have a Memorandum of Understanding with the CFPB to coordinate on financial enforcement efforts, including those related to financial privacy.[9] We have an ongoing dialogue with the FCC, which is taking a more active approach to privacy in the telecommunications area. And we regularly work with HHS, the Department of Education, and of course the States.

II. Recent FTC activities

Given our very broad authority, we are always evaluating our priorities, and our areas of emphasis have varied over time. In the privacy area, our goal is to keep pace with developments and address the privacy and data security challenges we see in the current marketplace. And, indeed, there are many more challenges to privacy than there were even just a year ago. Today, data is collected from consumers wherever they go, often invisibly and without their knowledge or consent. Almost everyone carries a smartphone, uses social networks, and browses and shops through various devices.

[9] *Memorandum of Understanding Between the Consumer Financial Protection Bureau and the Federal Trade Commission To Ensure Effective Cooperation To Protect Consumers, Prevent Duplication of Efforts, Provide Consistency, and Ensure A Vibrant Marketplace For Consumer Financial Products and Services* (Mar. 2015), *available at* https://www.ftc.gov/policy/cooperation-agreements/ftc-cfpb-interagency-cooperation-agreement,

Consumers are tracked as they walk down the street, shop in stores, drive in their cars, and even as they monitor their health or exercise using health apps. And many companies that consumers have never heard of have access to all of this data.

To help protect consumers in this era of ubiquitous and invisible data collection, our privacy program focuses on three inter-related themes: Big Data, Mobile Technologies, and Safeguarding Sensitive Data. I'll discuss each one in turn.

A. Big Data

First is Big Data. Big Data can drive valuable innovation across many fields – medicine, education, transportation, and manufacturing. But it also raises privacy concerns for consumers – vast collection and storage of their data; the risk that detailed profiles will fall into the wrong hands, enabling identity theft and other harms; the release of sensitive information consumers regard as private; and, of course, the potential use of this information by employers, insurers, creditors, and others.

Our central message is that, even in the face of rapidly changing business models and technologies, companies still need to follow the fundamental privacy principles – including, don't collect or retain more data than you reasonably need, tell consumers how you plan to use and share their data, give consumers choices about their privacy, and protect data from unauthorized access. As new business models and technologies develop, these principles remain relevant and important, although they may need to be adjusted and adapted.

We've emphasized these principles through both policy initiatives and enforcement. Most recently, we issued a staff report setting forth a number of

recommended best practices in the Internet of Things.[10] One particular issue we addressed was the question we hear again and again about whether notice and choice have continuing relevance, given the lack of traditional screens or interface to communicate with consumers. As to that question, we responded with an emphatic "yes" and discussed the different tools that Internet of Things companies are using to communicate with consumers – such as point of sale disclosures, set-up wizards, or even codes on the device. The report also discussed the importance of reasonable collection limits, de-identification of data, and strong security measures.

In addition, last year, we hosted a workshop entitled *Big Data: A Tool for Inclusion or Exclusion?*.[11] The workshop explored how the categorization of consumers may be both creating and limiting opportunities for consumers, with a focus on low income and underserved consumers. Participants discussed the benefits and concerns these practices raise, as well as how existing laws apply to such practices and where there are gaps in the legal framework. We plan to issue a report or guidance on this topic in the coming year.

We have also continued to focus on the unique privacy challenged presented by the data broker industry. Last May, we released a report detailing the findings of a study we conducted of nine brokers representing a cross-section of the industry.[12] The report

---

[10] FTC Staff Report, *Internet of Things: Privacy and Security in a Connected World* (Jan. 2015), *available at* http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[11] FTC Workshop, *Big Data: A Tool for Inclusion or Exclusion?* (Sept. 14. 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion.

[12] FTC Report, *Data Brokers: A Call for Transparency and Accountability* (May 2014), *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

discussed data brokers' sources of data; their clients; and the detailed information they collect, infer, store, and sell about individuals. The report also discussed various categories data brokers use to characterize consumers when they sell their data to businesses – for example "Urban Scramble" and "Mobile Mixers," which describe low income, minority consumers; "Thrifty Elders"; "Financially Challenged"; "Bible Lifestyle"; "Leans Left," and many other such categories. The concern about these practices, of course, is that consumers know nothing about them, even as companies buy this data to make business decisions about consumers. Our report highlighted the need for much greater transparency and consumer choice for these practices and called for congressional action to provide increased consumer protections in this area.

The Commission has also brought enforcement actions to address the concerns raised by Big Data, using our authority under both the FTC Act and the Fair Credit Report Act. Not everyone realizes this, but the FCRA is essentially a Big Data law. Passed in the 1970s to address the treasure trove of data being collected – invisibly and without accountability – by the credit reporting industry, it governs the use of Big Data to make some of the most important decisions there are – whether to give consumers credit, jobs, or insurance. We recently used this law to take action, for example, against two companies that advise stores on whether to accept consumers' checks, based on their financial history. Our complaints alleged that TeleCheck[13] and Certegy[14] failed to have appropriate procedures to maintain the accuracy of consumer data and correct errors,

[13] *U.S. v. Telecheck Servs., Inc.*, No. 1:14-cv-00062 (D.D.C. Jan. 16, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3183/telecheck-services-inc.

[14] *U.S. v. Certegy Check Servs., Inc.*, No. 1:13-cv-01247 (D.D.C. Aug. 15, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3184/certegy-check-services-inc.

which could result in consumers being denied the ability to use checks to make payments. The companies each paid a $3.5 million penalty to settle the charges.

Another case we brought in this area – our first Internet of Things case – involved video monitoring company TRENDnet.[15] We alleged that the company failed to provide reasonable security for IP cameras used for home security and baby monitoring, resulting in hackers being able to post private video feeds of people's bedrooms and children's rooms on the Internet. It's great that consumers can keep an eye on their homes from work or monitor their babies from a downstairs monitor, but not when criminals can watch too.

B. Mobile Technologies

A second area of focus for our privacy program is mobile technologies. In the past few years, this area has become one of the main priorities at the FTC – in privacy and more generally. We've brought cases against Apple,[16] Amazon,[17] and Google[18] related to kids' in-app purchases; against T-Mobile[19] and AT&T[20] for mobile cramming (that is, the unlawful practice of placing unauthorized third-party charges on mobile phone

---

[15] *TRENDnet, Inc.*, No. C-4426 (Jan. 16, 2014), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.

[16] *Apple, Inc.*, No. C-4444 (Mar. 25, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3108/apple-inc.

[17] *FTC v. Amazon.com*, No. 2:14-cv-01038 (W.D. Wash. filed July 10, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3238/amazoncom-inc,

[18] *Google, Inc.*, No. C-4499 (Dec. 2, 2014) (F.T.C. consent), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3237/google-inc.

[19] *FTC v. T-Mobile USA, Inc.*, No. 2:14-cv-0097-JLR (W.D. Wash. filed Dec. 19, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3231/t-mobile-usa-inc.

[20] *FTC v. AT&T Mobility, Inc.*, No. 1:14-cv-3227-HLM (N.D. Ga. filed Oct. 8, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3248/att-mobility-llc.

accounts); and against AT&T[21] and TracFone[22] related to the companies false claims of providing "unlimited data" to consumers. These cases are all about applying basic consumer protection rules to the mobile platform.

Clearly, the marketplace is moving to mobile, and consumer protections need to move with it. 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, which makes disclosures to consumers ever more challenging.

On the policy front, we've issued several reports about kids' apps, mobile privacy disclosures, and mobile payments.[23] These reports stress the need for privacy by design, transparency, and easy-to-exercise choices for consumers. They also provide guidance about how to provide these protections effectively on the mobile platform.

We've also brought law enforcement actions challenging violations occurring in the mobile ecosystem. For example, we announced a settlement with mobile messaging app Snapchat for, among other things, promising that the photos and videos sent through

---

[21] *FTC v. AT&T Mobility, Inc.*, No. C-14-4785 EMC (N.D. Cal. filed Oct. 28, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3253/att-mobility-llc-mobile-data-service.

[22] *FTC v. TracFone Wireless, Inc.*, No. 3:15-cv-00392 (N.D. Cal. filed Jan. 28, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3176/straight-talk-wireless-tracfone-wireless-inc.

[23] *See, e.g.*, FTC Staff Report, *What's the Deal?: An FTC Study on Mobile Shopping Apps* (Aug. 2014), *available at* https://www.ftc.gov/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014 ; FTC Staff Report, *Mobile Privacy Disclosures: Building Trust through Transparency* (Feb. 2013), *available at* https://www.ftc.gov/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission; FTC Staff Report, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (Dec. 2012), *available at* https://www.ftc.gov/reports/mobile-apps-kids-disclosures-still-not-making-grade; FTC Staff Report, *Mobile Apps for Kids: Current Privacy Disclosures are Dis(app)ointing* (Feb. 2012), *available at* https://www.ftc.gov/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing.

the devices would disappear at a time set by the sender.[24] In fact, recipients could use easy workarounds to keep the messages forever. We also announced a case against Goldenshores Technology, the maker of a popular flashlight app.[25] We alleged that the app 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, including mobile ad networks. Finally, we've brought a number of cases involving mobile security, including against mobile device manufacturer HTC[26] and mobile apps Credit Karma[27] and Fandango.[28] Mobile continues to be a central area of focus for 2015.

C. Safeguarding Sensitive Data

Our third main area of focus is safeguarding sensitive consumer data – that is, kids', health, financial, and precise geolocation information.

Protecting sensitive data isn't really a new priority – it's one of the original priorities we started with at the very beginning of our privacy program. But in today's marketplace, the stakes are even higher for sensitive data as it's captured all day long and then used and shared in ways consumers would never expect.

---

[24] *Snapchat, Inc.*, No. C-4501 (Dec. 23, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter.
[25] *Goldenshores Technologies, LLC & Eric M. Geidl*, No. C-4446 (Mar. 31, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3087/goldenshores-technologies-llc-erik-m-geidl-matter.
[26] *HTC America, Inc.*, No. C-4406 (June 25, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter.
[27] *Credit Karma, Inc.*, No. C-4480 (Aug. 13, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc.
[28] *Fandango, LLC*, No. C-4481 (Aug. 13, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc.

Most recently, the FTC settled allegations against Craig Brittain, the operator of the now-defunct website isanybodydown.com. Brittain used this so-called "revenge porn" website to collect and post intimate images and personal data of more than 1000 individuals.[29] Our complaint alleged that he used deceptive practices on Craigslist to acquire the images, and also solicited the images from angry boyfriends and by offering money on his site. He then advertised on another site that he could get the images deleted, charging a hefty payment and pretending that the new site was operated by a third party. Our complaint alleged both deception and unfairness.

We also recently settled charges with a PaymentsMD, a health billing company, for allegedly deceptive practices related to its online patient portal.[30] The company offered the portal to consumers as a way for them to view their billing history with various medical providers. Our complaint alleged that the company used a deceptive sign-up process – including hidden disclosures and confusing check boxes – to trick consumers into giving their permission to gather sensitive health data from pharmacies, medical testing companies, and insurance companies to create a patient health report. The data included prescriptions, medical diagnoses, and the results of lab tests.

Our work to protect sensitive data also includes 55 cases to date against companies that failed to implement reasonable security protections – including such diverse

[29] *Craig Britton*, File No. 132-3120 (Jan. 29, 2015) (proposed consent), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3120/craig-brittain-matter. .

[30] *PaymentsMD, LLC*, No. C-4505 (Jan. 27, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3088/paymentsmd-llc-matter.

companies as Microsoft, TJX, Lifelock, CVS, RiteAid, BJ's, and Wyndham.[31] Many of these cases have involved not just consumers' financial data, but health information, account IDs and passwords, and other sensitive data. Data security continues to be a top FTC priority and, indeed, the Commission unanimously supports federal data breach and data security legislation to strengthen our authority in this area.[32]

Finally, the Commission has a special interest in protecting the privacy of our kids, who may not have the judgment to avoid dangers online and may share information about themselves or their families. Much of our work in the mobile area, which I already discussed, protects kids and teens, since they are particularly high users of mobile technologies.

We also enforce the Children's Online Privacy Protection Act, which requires notice and consent to parents before information is collected from kids under 13.[33] To date, we've brought 25 cases to protect kids' privacy, including two announced last fall against the mobile app for Yelp[34] and the gaming app TinyCo,[35] both of which paid substantial civil penalties. Protecting sensitive data, including from kids, continues to be a top FTC priority.

---

[31] *See generally Commission Statement Marking the FTC's 50th Data Security Settlement* (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[32] *See, e.g.*, Prepared Statement of the Federal Trade Commission, "Discussion Draft of H.R.__, Data Security and Breach Notification Act Of 2015," Before the Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce, 114th Cong., Mar. 18, 2015, *available at* https://www.ftc.gov/public-statements/2015/03/prepared-statement-federal-trade-commission-discussion-draft-hr__-data.

[33] 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312.

[34] *U.S. v. Yelp Inc.*, No. 3:14-cv-04163 (N.D. Cal. filed Sept. 17, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3066/yelp-inc.

[35] *U.S. v. TinyCo, Inc.*, No. 3:14-cv-04164 (N.D. Cal. filed Sept. 17, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3209/tinyco-inc.

III. Conclusion

I hope my remarks have been helpful in giving you a window into the FTC's privacy priorities for the coming year. I am happy to take questions.