



Federal Trade Commission

The FTC's Privacy and Data Security Priorities for 2015

Jessica Rich¹

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 101 for 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 Act⁷ 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. §§

kids' online safety to preventing and repairing identity theft, our top source of consumer complaints from year-to

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

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

accounts); and against AT&T²¹ and TracFone²² 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), m

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 HTC²⁶ and mobile apps Credit Karma²⁷ and Fandango.²⁸ Mobile continues to be a central area of focus for 2015.

C. Safeguarding Sensitive Data

Our third main area of focus

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*

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 Yelp³⁴ 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.