PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

"Examining the Proposed FCC Privacy Rules"

Before the

UNITED STATES SENATE

COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE FOR PRIVACY, TECHNOLOGY AND THE LAW

Washington, D.C.

May 11, 2016

I. Introduction

Chairman Flake, Ranking Member Franken, and members of the Subcommittee, the Federal Trade Commission ("FTC" or "Commission") appreciates this opportunity to appear before you today to discuss the Commission's efforts to protect the privacy and security of consumers' information.[1] As the Federal Communications Commission (FCC) solicits and considers comments on its proposal to craft privacy regulations in the broadband sphere, we believe our experience and expertise can help inform the process.

Privacy today is a complex issue. Data is collected from consumers all day long, wherever they go – as they shop both online and in brick and mortar stores; as they use their smartphones and other connected devices; as they check and update their many social networks; even as they walk down the street. This ubiquitous data collection is invisible in many ways. Many of the companies that collect consumers' data are behind the scenes and do not interact with consumers. Privacy policies are difficult to understand even for those consumers with the will and ability to find and decipher them. And as we move further into the era of the Internet of Things, data collection will become even more invisible and hard to control.

The use of data has and will continue to drive valuable innovation across many fields – medicine, education, marketing, transportation, and manufacturing. But it also raises privacy concerns for consumers such as massive collection and storage of personal information; 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 the potential use of this data by employers, insurers, creditors, and others to make important decisions about consumers.

[1] While the views expressed in this statement represent the views of the Commission, the Commissioners' oral presentations and responses to questions are their own and do not necessarily reflect the views of the Commission or any other Commissioner.

Although the privacy landscape has evolved, the FTC's interest in privacy issues has remained constant over the last 40 years.[2] The FTC's objective in this area is to protect consumers' personal information and ensure that they can confidently take advantage of the many benefits offered by the ever-changing marketplace. To meet this objective, the FTC has undertaken law enforcement, policy, and education initiatives aimed at protecting consumers in a broad range of economic sectors, including retail, advertising, credit reporting, health, financial, mobile, social media, and hardware and software manufacturing. Given the breadth of its jurisdiction, the FTC has cooperated frequently with other agencies on areas of mutual concern. For example, the agency has worked with the Department of Health and Human Services on health privacy issues and with the Department of Education on student privacy issues. Notably, the FTC has had numerous occasions to engage in cooperative initiatives with the FCC on privacy-related issues such as Do Not Call, pretexting, and mobile security. The Commission's goal in working with other agencies is to use its complementary authority to protect consumers as effectively and efficiently as possible, to avoid duplication, and to promote consistency.

II. The FTC's Privacy Program

A. Enforcement

The FTC has unparalleled experience in consumer privacy enforcement. The Commission has used its core enforcement authority – Section 5 of the FTC Act – to take action against companies engaged in unfair or deceptive practices involving the privacy and security of consumers' information.[3] If a company makes materially misleading statements or omissions about a product or service, including its privacy or data security features, and such statements or omissions are likely to mislead reasonable consumers, such statements or omissions can be found

[2] *See generally* https://www.ftc.gov/tips-advice/business-center/privacy-and-security.
[3] 15 U.S.C. § 45(a).

to be deceptive and in violation of Section 5.[4] Further, if a company's privacy or data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition, those practices can be found to be unfair and in violation of Section 5.[5] The FTC also enforces sector-specific statutes that protect certain health,[6] credit,[7] financial,[8] and children's information.[9]

The FTC has brought over 500 enforcement actions protecting the privacy of consumer information. This body of cases covers both offline and online information and includes enforcement actions against companies large and small. These cases cover all parts of the Internet ecosystem, including social networks, search engines, ad networks, online retailers, mobile apps, mobile handsets, and Internet Service Providers (ISPs). In this wide range of cases, the FTC has alleged that companies made deceptive claims about how they collect, use, and share consumer data; failed to provide reasonable security for consumers' personal information; deceptively tracked consumers online; spammed consumers; installed spyware or other malware on consumers' computers; violated Do Not Call and other telemarketing rules; and publicly posted highly sensitive, private consumer data online without consumers' knowledge or consent. The FTC's enforcement actions – in both the physical and digital worlds – send an important message to companies about the need to protect consumer privacy.

The FTC's current privacy enforcement priorities include mobile, health, the Internet of Things, and data security. One example of FTC enforcement action in the mobile area is the

[4] *See* FTC Policy Statement on Deception, *appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984), *available at* https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.
[5] *See* FTC Policy Statement on Unfairness, *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984), *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness; 15 U.S.C. §45(n).
[6] 16 C.F.R. Part 318.
[7] 15 U.S.C. §§ 1681-1681x.
[8] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).
[9] 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312.

Snapchat case. In that case, messaging app Snapchat promised that the photos and videos sent through its app would disappear at a time set by the sender.[10] In fact, the FTC alleged that recipients could use easy workarounds – such as third party apps – to keep the messages forever. Despite a researcher warning the company about this possibility, the complaint alleged, Snapchat continued to misrepresent that the sender could control how long a recipient can view a "snap."

One example in the health privacy area is the FTC's settlement with Payments MD, a medical billing service provider. The FTC alleged that PaymentsMD and its former CEO misled thousands of consumers who signed up for an online billing portal.[11] According to the complaint, the defendants used the registration process for the billing portal as a way to deceptively seek consumers' consent to obtain highly-detailed medical information about the consumers from pharmacies, medical labs, and insurance companies.

Finally, the Commission has brought 60 cases alleging that companies failed to implement reasonable safeguards for the consumer data they maintain. For example, the FTC recently announced a settlement with computer hardware company ASUS for allegedly failing to take reasonable steps to secure the software on its routers. According to the complaint, the company's failures to timely address vulnerabilities or notify consumers about the availability of security updates resulted in critical security flaws in its routers that put the home networks of thousands of consumers at risk.[12] The complaint also alleged that the routers' insecure "cloud" services led to the compromise of thousands of consumers' connected storage devices, exposing their sensitive personal data on the Internet. Under the order, ASUS must establish a

[10] *Snapchat, Inc.*, No. C-4501 (Dec. 23, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter.
[11] *PaymentsMD, LLC*, No. C-4505 (Jan. 27, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3088/paymentsmd-llc-matter.
[12] *ASUSTeK Computer Inc.*, Matter No. 142 3156 (Feb. 23, 2016) (proposed consent), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter.

comprehensive security program and notify consumers about software updates or other steps they can take to protect themselves from security flaws. This case marks the second time the FTC has entered into a data security settlement involving an Internet of Things-related product.[13]

B. Policy Initiatives

The FTC has also pursued numerous policy initiatives to enhance consumer privacy. The FTC has hosted workshops and issued reports recommending best practices designed to improve privacy, increase transparency, and highlight the privacy and security implications of new technologies and business practices. Indeed, the FTC held its first workshop on Internet privacy nearly twenty years ago, in June of 1996.[14]

Over the last few years, the FTC's policy work has built on recommendations from its 2012 Privacy Report, which set forth key privacy principles that should apply across diverse technologies and business models.[15] That report was the culmination of years of research and investigation, including three public workshops, a publicly released preliminary draft report, and multiple rounds of public comment. The report recommended that companies implement privacy protections, such as data minimization and security, at the outset of product development ("privacy by design"); simplify the ways they provide privacy choices to consumers; and improve transparency of their privacy practices.

The FTC has applied these principles to a broad array of emerging technologies and business practices. For example, in 2012 the FTC held a workshop to explore privacy issues

---

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

[14] *See* Press Release, FTC Workshop on Consumer Privacy in Cyberspace to Be Held June 1996 (May 15, 1996), https://www.ftc.gov/news-events/press-releases/1996/05/ftc-workshop-consumer-privacy-cyberspace-be-held-june-1996.

[15] FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* (Mar. 2012), *available at* https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

raised by the collection and use of comprehensive data about consumers' online activities by ISPs, operating systems, browsers, search engines, and social media.[16]

In a more recent example, the FTC issued a staff report on the Internet of Things last year. The report recommended best practices for companies, and also addressed how longstanding privacy principles can be adapted for the Internet of Things.[17] For example, the report addressed the continuing relevance of the principles of transparency and choice in the Internet of Things, even given the lack of traditional screens or interfaces to communicate with consumers. The report also discussed the different tools that IoT companies are using to communicate with consumers – such as point of sale disclosures, set-up wizards, or even codes on the device. And the report discussed the importance of reasonable collection limits, de-identification of data, and strong security measures.

Similarly, the FTC has hosted workshops and issued reports on so-called big data practices. In 2014, it issued a report on the data broker industry, which described the depth and breadth of data brokers' information collection and use practices; recommended improved transparency for the industry; and suggested additional tools through which consumers could exercise choices about their data.[18] Earlier this year, the Commission issued a report entitled *Big Data: A Tool for Inclusion or Exclusion?,*[19] which highlighted a number of innovative uses of big data that provide benefits to underserved populations, while also examining possible risks that could result from biases or inaccuracies in big data.

---

[16] FTC Workshop, *The Big Picture: Comprehensive Online Data Collection*, Dec. 6, 2012, *available at* https://www.ftc.gov/news-events/events-calendar/2012/12/big-picture-comprehensive-online-data-collection.
[17] FTC Staff Workshop Report, *The Internet of Things: Privacy and Security in a Connected World* (Jan. 2015), *available at* https://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things.
[18] FTC Report, *Data Brokers: A Call For Transparency and Accountability* (May 2014), *available at* https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014.
[19] FTC Report, *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues* (Jan. 2016), *available at* https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report.

The FTC also regularly holds events designed to enhance public understanding of key issues involving privacy and data security. For example, last fall the agency held a workshop on cross-device tracking to examine the privacy and security issues around the tracking of consumers' activities across their different devices for advertising and marketing purposes.[20]

In January 2016, the Commission hosted the first-of-its-kind PrivacyCon, which provided a platform for academics to discuss cutting-edge research and trends in protecting consumer privacy and security.[21] The FTC recently announced the second PrivacyCon, to be held in January 2017.[22] The FTC is seeking empirical research on topics such as the harms associated with privacy violations, attack vectors and trends, the uptake of ad blocker tools, the costs of malware, transparency and control, and user and research tools for privacy and security.

And most recently, the FTC announced that it will host a series of seminars this fall to examine three new and evolving technologies that are raising critical consumer protection issues. The FTC Fall Technology Series will explore the privacy and security issues raised by ransomware, drones, and smart TVs.[23]

C. Business Guidance and Consumer Education

Finally, the FTC creates business guidance and consumer education to enhance the impact of its enforcement and policy development initiatives. The Commission has used a variety of tools – publications, online resources, workshops, and social media – to provide

---

[20] FTC Workshop, *Cross-Device Tracking*, Nov. 16, 2015, *available at* https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking.

[21] FTC Conference, *PrivacyCon*, Jan. 14, 2016, *available at* https://www.ftc.gov/news-events/events-calendar/2016/01/privacycon. Research topics included the current state of online privacy; consumers' privacy expectations; transparency tools for revealing data discrimination; the economics of privacy and security; and security and usability.

[22] *See PrivacyCon: Call for Presentations* (last visited Apr. 27, 2016), *available at* https://www.ftc.gov/privacycon-call-for-presentations.

[23] *See* Press Release, FTC to Host Fall Seminar Series on Emerging Consumer Technology Issues (Mar. 21, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-host-fall-seminar-series-emerging-consumer-technology-issues.

educational materials on a wide range of topics, including mobile apps, children's privacy, and data security. For example, the FTC has long sponsored OnGuard Online, which educates consumers about many online threats to consumer privacy and security, including spam, spyware, phishing, peer-to-peer file sharing, and social networking.[24] Furthermore, the FTC provides consumer education to help consumers better understand the privacy and security implications of new and existing technologies. For example, the FTC's *Netcetera* publication helps parents, teachers, and other adults talk to children about how to be safe, secure, and responsible online.[25]

Additionally, the Commission has also issued numerous education materials to help consumers protect themselves from identity theft and to deal with its consequences when it does occur. The FTC recently launched an improved version of IdentityTheft.gov[26] (robodeidentidad.gov in Spanish[27]), a free, one-stop resource people can use to report and recover from identity theft. Now, identity theft victims can use the site to create a personal recovery plan based on the type of identity theft they face, and get pre-filled letters and forms to send to credit bureaus, businesses and debt collectors. During 2015, people viewed IdentityTheft.gov more than 1.3 million times and ordered more than 3.7 million related publications in English, Spanish, and four other languages.

Business education is also an important priority for the FTC. The Commission seeks to educate businesses by developing and distributing free guidance. Most recently, the Commission launched its *Start with Security* initiative, which includes a guide for businesses that summarizes

[24] *See* www.onguardonline.gov. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alerta en Línea have attracted more than 25 million visits.
[25] *Netcetera: Chatting with Kids About Being Online* (Jan. 2014), *available at* https://www.onguardonline.gov/articles/pdf-0001-netcetera.pdf.
[26] *See* https://identitytheft.gov/.
[27] *See* https://robodeidentidad.gov/.

the lessons learned from the FTC's 60 data security cases,[28] as well as videos.[29] As part of this initiative, the FTC also has organized one-day conferences in Austin, San Francisco, and Seattle, as well as an upcoming event in Chicago, to bring business owners and developers together with industry experts to discuss practical tips and strategies for implementing effective data security.[30]

In addition, the FTC develops privacy guidance for specific industries. For example, the FTC has developed specific guidance for mobile app developers as they create, release, and monitor their apps.[31] The FTC also creates business educational materials on specific topics – such as a tool for health-related mobile app developers to understand what federal laws and regulations might apply to their apps,[32] as well as business guidance aimed at helping health app developers comply with the FTC Act.[33] Further, the FTC released guidance about ways to provide data security for Internet of Things devices, which includes tips such as designing products with authentication in mind and protecting the interfaces between devices connected to the Internet.[34]

III. Privacy-Related Initiatives with the FCC

The Commission has a long history of successful cooperation with the FCC on consumer protection issues, including issues related to privacy and data security. Last year, the agencies

---

[28] *Start with Security: A Guide for Business* (June 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.
[29] *Start with Security: Free Resources for Any Business* (Feb. 19, 2016), *available at* https://www.ftc.gov/news-events/audio-video/business.
[30] *See, e.g.*, FTC Event, Start with Security – Seattle, Feb. 9, 2016, *available at* https://www.ftc.gov/news-events/events-calendar/2016/02/start-security-seattle.
[31] *Mobile App Developers: Start with Security* (Feb. 2013), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security.
[32] Mobile Health Apps Interactive Tool (Apr. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.
[33] *Mobile Health App Developers: FTC Best Practices* (Apr. 2016), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices.
[34] *See Careful Connections: Building Security in the Internet of Things* (Jan. 2015), *available at* http://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.

affirmed and formalized this collaboration by entering into a Memorandum of Understanding agreeing to coordinate on their respective consumer protection efforts.[35]

One example of our privacy collaboration is the federal Do Not Call registry, created in 2003. The FTC and FCC Do Not Call teams hold regularly-scheduled conference calls to discuss enforcement issues, targeting, litigation, and complaint trends. The teams share data when investigations overlap. And the FCC has participated in the FTC's various robocall initiatives, including the FTC's Robocall Summit and the FTC's Robocall Challenges.

Furthermore, almost a decade ago, both agencies cooperated to investigate the practice of obtaining unauthorized access to consumers' sensitive information through fraud, otherwise known as "pretexting." While the FTC focused its enforcement efforts on the companies that were engaging in pretexting and then selling consumers' sensitive information, the FCC leveraged its resources to examine the carriers' roles in pretexting.

In addition, in two recent FTC cases against AT&T[36] and T-Mobile,[37] the FCC and state authorities were essential in negotiating two major settlements providing for injunctive relief and hundreds of millions of dollars in consumer redress for unauthorized third party charges on mobile phones, a practice known as mobile cramming. These settlements demonstrate how the agencies use their complementary tools to remedy harms and deter future non-compliance. While the FTC's focus is typically to put money back in the pockets of consumers, the FCC traditionally has exercised its authority to fine companies for noncompliance.

---

[35] *Memorandum of Understanding on Consumer Protection Between the Federal Trade Commission and the Federal Communications Commission* (Nov. 2015), *available at* https://www.ftc.gov/policy/cooperation-agreements/memorandum-understanding-consumer-protection-between-federal-trade.

[36] *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.

[37] *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.

Finally, most recently, the FTC and FCC announced separate studies of security in the mobile ecosystem.[38] The FTC is seeking information from mobile device manufacturers and operating systems about how they provide security updates to address vulnerabilities in smartphones, tablets, and other mobile devices. At the same time, the FCC is examining common carriers' policies regarding mobile device security updates. Given the complexity of the mobile ecosystem and the number of entities involved in developing and deploying security patches, it is difficult to discern how carriers, operating systems, and handset manufacturers determine when any specific device model receives a security update and on what timeline. The responses to the studies should provide important information about who is responsible for providing mobile security patches to consumers.

In addition, in response to the FCC's request for comment on its proposed rules governing the privacy of consumer information collected by broadband Internet access services providers, the FTC is carefully considering the proposal and intends to file a comment. Based on our decades of experience and leadership on consumer privacy issues, we believe the Commission can provide unique insights to the FCC.

IV. Conclusion

Thank you for the opportunity to provide the Commission's views. The FTC is committed to protecting the privacy and security of consumers' data, and we look forward to continuing to work with the Subcommittee and Congress on this important issue.

[38] *See* Press Release, *FTC To Study Mobile Device Industry's Security Update Practices* (May 11, 2016), *available at* https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices.