United States of America

Federal Trade Commission

Reactions to the FCC's Proposed Privacy Regulations
Remarks of Maureen K. Ohlhausen[1]
Commissioner, U.S. Federal Trade Commission

2016 Advertising and Privacy Law Summit
Kelley Drye & Warren LLP
Watergate Hotel
June 8, 2016

Thank you to Kelley Drye & Warren for inviting me to participate in the 2016 Advertising and Privacy Law Summit. Modern advertising, particularly online advertising, is a very productive use of data about consumers. Online advertising has, in turn, fueled the internet as we know it today – bursting with free, useful platforms that are ad-supported. Of course, use of consumer data can raise privacy concerns. Privacy is a complex regulatory issue, in part because misguided privacy protections can preclude the massive benefits of data use and increase the harms from data misuse. I'm here today to discuss the FTC's approach to protecting consumer privacy and my views on the Federal Communications Commission's recent notice of proposed rulemaking, or NPRM, which proposes to regulate the privacy and data security practices of Broadband Internet Access Service, providers, more commonly known as ISPs.[2]

[1] The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission, its staff, or any other Commissioner.

[2] *In re Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500 (Apr. 1, 2016), https://www.fcc.gov/document/fcc-releases-proposed-rules-protect-broadband-consumer-privacy (NPRM).

By now, most of you likely know what triggered the FCC's new privacy efforts. When the FCC adopted its net neutrality rules, it chose to reclassify Broadband Internet Access Service as a Title II common carrier service.[3] This affected the FTC's oversight of ISPs. Although the FTC has general jurisdiction, there are a few carve outs, including common carriers acting as common carriers.[4] Thus, the FCC's reclassification affected the FTC's long-standing authority to protect consumers' privacy in their interactions with ISPs. Subsequently, the FCC decided to step into the consumer protection gap that it created, issuing a Notice of Proposed Rulemaking.[5]

As you may know, on May 27th the FTC's Bureau of Consumer Protection filed comments in the FCC's proceeding.[6] I will discuss staff's comments at some length, but my standard disclaimer applies: these thoughts are my own, and do not necessarily represent the views of the FTC staff or other Commissioners. However, I strongly support staff's comments. I also filed a separate statement highlighting some additional points.[7] I'd like to quickly

---

[3] *See Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (Mar. 12, 2015).

[4] 15 U.S.C. § 45(a)(2) (FTC authority does not reach "common carriers subject to the Communications Act of 1934"). "An entity is a common carrier … only with respect to services it provides on a common carrier basis." FED. TRADE COMM'N, BROADBAND CONNECTIVITY COMPETITION POLICY STAFF REPORT at 38 (June 2007), https://www.ftc.gov/reports/broadband-connectivity-competition-policy-staff-report, (citing 47 U.S.C. § 153(44). *See also*, FTC v. AT&T, No. C-14-4785 EMC, Order Denying Defendant's Motion to Dismiss at 23 (Mar. 31, 2015) (holding that the FTC's "common carrier exception applies only where the entity has the status of common carrier and is actually engaging in common carrier activity").

[5] Press Release, Fed. Comm. Comm'n, March 2016 Open Commission Meeting (Mar. 2016), https://www.fcc.gov/news-events/events/2016/03/march-2016-open-commission-meeting.

[6] Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16-106 (filed May 27, 2016), https://www.ftc.gov/policy/policy-actions/advocacy-filings/2016/05/comment-staff-bureau-consumer-protection-federal (Comment).

[7] Statement of FTC Commissioner Maureen K. Ohlhausen Regarding Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16-106 (filed May 27, 2016), https://www.ftc.gov/public-statements/2016/05/statement-ftc-commissioner-maureen-k-ohlhausen-regarding-comment-staff.

summarize those two filings, which describe the differences between the FTC's established approach and the FCC's proposed approach.

Staff's Comment. BCP's comment supported the overall goal of the FCC rulemaking, which is to protect the privacy and security of information about consumers, but critiqued the method proposed to achieve those goals.

As the comment recognized, consumer data is a valuable resource that can benefit both businesses and consumers. The advertising industry knows this well. Beneficial uses of consumer data go far beyond targeted advertising, of course. In the ISP context, such benefits could include lower prices and improved security and services. Regulatory restrictions on use of consumer data may foreclose these benefits, imposing significant costs on consumers – a fact often overlooked by advocates who may have different privacy preferences than average consumers. Of course, as staff's comment notes, consumers do value privacy, and the collection, use, and sharing of consumer data creates some risks that should be addressed.

Staff's comment describes how the FTC addresses these risks to protect consumer privacy. It notes that the FTC is *the* primary privacy and data protection agency in the U.S., and probably the most active enforcer of privacy laws in the world. (No doubt many of you are very aware of this active enforcement.) We have brought more than 500 privacy and data security related enforcement actions for online and offline practices, including actions against ISPs and against some of the biggest companies in the Internet ecosystem.[8] We also conduct extensive consumer and business outreach and guidance, facilitate workshops to foster discussions about

[8] *See* Letter from Edith Ramirez, Chairwoman, Fed. Trade Comm'n, to Věra Jourová, Commissioner for Justice, Consumers, and Gender Equality, European Commission, 3 (Feb. 23, 2016), https://www ftc.gov/public-statements/2016/02/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice.

privacy in emerging areas, coordinate on privacy efforts internationally, and advocate for policies about privacy and data use that improve consumer welfare.[9]

As staff explains, and as I note in my separate statement, the FTC built its privacy program on the long-established legal principles of unfairness and deception.[10] This framework focuses on the sensitivity of consumer data and particular promises made about data collection and use, rather than on what type of entity collects or uses that data. The FTC recommends opt-in consent for unexpected collection or use of consumers' sensitive data such as Social Security numbers, financial information, and information about children. The FTC's framework applies to any entities, including browsers and Internet platforms, that access such sensitive information.

This approach reflects the fact that consumer privacy preferences differ greatly depending on the type of data and its use. On one hand, consumer preferences are fairly uniform with regard to certain uses of sensitive data. For example, the overwhelming majority of consumers object to entities accessing their financial or medical data without permission. On the other hand, we know from experience as well as academic research – including a recent Pew

---

[9] *See* FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES (Jan. 2016), https://www ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report (Big Data Report); FED. TRADE COMM'N, PRIVACYCON (Jan. 14, 2016), https://www.ftc.gov/news-events/events-calendar/2016/01/privacycon; FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (June 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

[10] The FTC's case-by-case application of these general principles has major advantages over a prescriptive rulemaking approach. The FTC's approach minimizes the regulator's knowledge problem, fosters incrementalism, and focuses limited resources on addressing consumer harm. *See* Maureen K. Ohlhausen, *The FCC's Knowledge Problem: How to Protect Consumers Online*, 67 FED. COMM. L.J. 203 (2015), https://www.ftc.gov/public-statements/2015/09/fccs-knowledge-problem-how-protect-consumers-online. These advantages are particularly beneficial in fast-changing areas such as privacy and data security. No rulemaking framework can capture all of these advantages of the case-by-case approach, although some frameworks are certainly preferable to others.

study – that for uses of non-sensitive data, such as advertising, people have widely varying privacy preferences.[11]

Obtaining or giving consent can be burdensome, not only for businesses, but also for consumers. Reading a notice and making a decision takes time that, in the aggregate, can be quite substantial.[12] To maximize consumer benefits, regulation should minimize these costs. One key way to do this is to set defaults so that those who value the choice most highly incur the time and effort of making an active decision, and those who do not care as much are not burdened by an unnecessary interaction. This means that setting opt-in or opt-out so that the default position matches typical consumer preferences for that type of data and use. For advertising based on non-sensitive information, this generally means an opt-out approach. For uses of sensitive information, this generally means an opt-in choice.

Let me be clear on this point: FTC experience demonstrates that more onerous privacy regulation does ***not*** always benefit consumers. Some, however, believe that more stringent regulation adds costs to business but only provides benefits to consumers. Yet because privacy preferences vary widely, regulation can impose significant costs on consumers. Consumers who wish to receive targeted advertising or to benefit from services funded by advertising are harmed by regulation that increases the difficulty of using information. As a result, if a regulation imposes defaults that do not match consumer preferences, it forces unnecessary costs on consumers without improving consumer outcomes. The burdens imposed by overly restrictive

[11] A recent Pew survey and focus groups testing consumer privacy preferences with regard to six different scenarios found 17% of polled rejected all the scenarios, 4% accepted all the scenarios, and the substantial majority indicated that at least one of the scenarios was potentially acceptable. *See* LEE RAINIE & MAEVE DUGGAN, PEW RESEARCH CENTER, PRIVACY AND INFORMATION SHARING (Dec. 2015), http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.

[12] *See, e.g.*, Raluca Budiu, *Interaction Costs*, NIELSEN NORMAN GROUP (Aug. 31, 2013) (describing interaction costs and the value of assessing such costs), https://www nngroup.com/articles/interaction-cost-definition/.

privacy regulation, such as broad opt-in requirements for non-sensitive data, may also slow innovation and growth, harming all consumers.[13]

After describing the benefits and risks of collecting consumer data and detailing the FTC's approach to protecting privacy, the staff comment discusses the FCC's proposal. The key takeaway: the FCC's proposed approach is inconsistent with the FTC's long-standing framework. In fact, the staff comment politely recognizes that the FCC's current proposal would impose more restrictions than are necessary to protect consumer privacy in many cases, and yet would fail to protect consumer privacy in others.

BCP's comment first notes that the FCC's framework places ISPs under a different set of regulations than those governing edge providers such as Google or Netflix, even though companies throughout the internet ecosystem collect and use significant amounts of consumer data.[14] The comment dryly describes this disparity as "not optimal."[15] Let me be a bit more explicit: these proposed rules would hamper ISPs from competing with other businesses to serve consumers in data-driven industries, including online advertising.

This barrier to competition could be large, because the differences between the FCC and FTC approaches are significant. Staff's comment details many of them. For example, staff notes that the FCC's proposed definition of personally identifiable information, or PII, is both under-

---

[13] *See* Daniel Castro & Alan McQuinn, *The Economic Costs of the European Union's Cookie Notification Policy*, THE INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (Nov. 2014), https://itif.org/publications/2014/11/06/economic-cost-european-unions-cookie-notification-policy; Catherine Tucker, *Empirical Research on the Economic Effects of Privacy Regulation*, 10 J. ON TELECOM. & HIGH TECH. L. 265 (2012); PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE x-xi (May 2014) ("[A] policy focus on limiting data collection will not be a broadly applicable or scalable strategy – nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth.").

[14] Comment at 8.

[15] *Id.*

and over-inclusive.[16] The proposed PII definition improperly includes data that is not reasonably linkable to an individual.[17] Conversely, the NPRM's proposal for emergency sharing could potentially expose sensitive information to abusive family members.[18] Furthermore, staff explains, the NPRM risks harming consumers because it doesn't require affirmative express consent for retroactive material changes to privacy policies.[19] Staff also questions the NPRM's strict liability standard for data breaches.[20] And staff expresses concern that the proposed data breach rules would result in over-notification and unnecessarily truncated times for breach investigations.[21]

Staff also details perhaps the most fundamental difference between the two approaches: the treatment of the sensitivity of consumer data.[22] The FCC's approach does not consider the sensitivity of different types consumer data, and therefore does not necessarily reflect consumers' privacy preferences. Instead, the FCC's three-tiered "implied consent / opt-out / opt-in" framework focuses on whether the holder of the data is a BIAS provider, an affiliate, or a third party.[23] Thus, the FCC would require opt-in consent for many uses of non-sensitive consumer data by ISPs, yet would require no consent at all for certain uses of sensitive data by

[16] *Id.* at 9-11.

[17] *Id.* at 9.

[18] *Id.* at 16-17.

[19] *Id.* at 14-15.

[20] *Id.* at 27-28.

[21] *Id.* at 30-33.

[22] *Id.* at 20-24.

[23] NPRM, Appendix A at 107 (proposing 47 C.F.R. § 64.7002).

those providers.[24] As FTC's staff's comment notes, this approach is inconsistent with the FTC's approach and with international approaches to privacy protection.[25]

Importantly, staff noted that many of its recommendations are interdependent.[26] Indeed, many of the FTC's suggested modifications only make sense if the FCC's final rules make distinctions based on the sensitivity of consumer data. For example, FTC staff suggests that the FCC's definition of PII include information that is "linked or reasonably linkable to a consumer or a consumer's device."[27] This definition would capture persistent identifiers such as cookies, static IP addresses, MAC addresses, and other device identifiers when they are tied to an individual consumer. However, many types of PII, such as names or IP addresses, are not sensitive by themselves. Under the FTC's approach, such non-sensitive PII about adults does not typically require heightened privacy protections such as opt-in consent. But under the FCC's proposal, an ISP would have to get opt-in approval for most uses of non-sensitive PII. Staff therefore notes that if the FCC rejects FTC staff's recommendation and subjects even non-sensitive PII to opt-in requirements, "it may be necessary to revisit FTC's staff's proposed definition of personally identifiable information."[28] Similar caveats apply to FTC staff's recommendations on transparency, access and correction, and data security.[29]

---

[24] Comment at 20-22.

[25] *Id.* at 22-23, n.94.

[26] *Id.* at 7 and n.27 ("Many of these recommendations are interdependent … For example, if the FCC does not accept FTC staff's recommendations on choice, it may be necessary to revisit FTC staff's proposed definition of personally identifiable information.").

[27] *Id.* at 10.

[28] *Id.* at n.27.

[29] *See, e.g., Id.* at n.63 ("The required level of access and correction should also be tied to the importance of the benefit or transaction in question, and should not undermine the development of accurate risk mitigation tools" *citing* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 54 (May 2014), https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-

However, I am familiar with a situation where Congress mandated protecting the privacy of online, non-sensitive PII. In the Children's Online Privacy Protection Act, Congress directed the FTC to require parental consent for most uses of PII, including non-sensitive PII, about any child under thirteen, subject to a variety of exceptions.[30] The FCC's proposal arguably restricts even more behavior than COPPA, however. For example, it would require opt-in consent for all third party uses of non-sensitive PII, without even the exceptions COPPA contains. Given that Congress mandated a more restrictive approach for children's PII, it seems incongruous for the FCC to now mandate similar restrictions for information about adults, and only when an ISP collects that information.

Turning to a new topic. The NPRM also asks if the FCC should regulate or prohibit ISPs from offering discounts to broadband consumers in exchange for the use of personal information.[31] The NPRM states that, "the FTC and others have argued that these business models unfairly disadvantage low income or other vulnerable populations…."[32] But, as my separate statement makes clear, the FTC has never argued this. The NPRM cites the FTC Big Data Report's summary of general concerns raised *by workshop participants* – not FTC staff . Indeed, the FTC report specifically observed that, "big data can create opportunities for low-income and underserved communities," and cites a broad range of existing examples.[33]

2014.); Comment at 27-28 (conditioning support for proposed security program on change to require "reasonable security").

[30] 15 U.S.C. § 6502(b)(2) (setting out conditions under which consent is not required for use of children's personal information).

[31] NPRM ¶ 259-262. The NPRM also asks if such practices are *already* prohibited by the Communications Act. *Id.* ¶ 259.

[32] *Id.* ¶ 261.

[33] Big Data Report at 5-8; 27.

As I further noted in my separate statement, a ban on discounts for ad-supported ISPs would not only reduce consumer choice – it might eliminate one viable way to increase broadband adoption. Such a ban would prohibit even a fully informed consumer from trading some of her data for a discount on her broadband bill. Yet when would-be broadband subscribers explain why they have not adopted broadband, they primarily cite high cost, not privacy concerns.[34] Lowering the cost of broadband through ad-supported services, therefore, could increase broadband adoption, a goal which we all support.

Conclusion. The FCC's NPRM seeks to protect the privacy and data security of ISP consumers. In pursuing this laudable goal, the FCC ought to take FTC staff's critique seriously. FTC staff has offered a less restrictive alternative modeled on the FTC's highly successful approach, which properly reflects consumers' preferences about sensitive information. In addition to adopting a FTC-like approach, the FCC should also permit consumers to make well-informed choices about discounted broadband offerings. Thank you, and I would be glad to take your questions at this time.

[34] John B. Horrigan, FCC, *Broadband Adoption and Use in America* 5 (OBI Working Paper Series No. 1, Oct. 2010), https://apps.fcc.gov/edocs_public/attachmatch/DOC-296442A1.pdf