Statement of FTC Commissioner Maureen K. Ohlhausen
Regarding
Comment of the Staff of the Bureau of Consumer Protection of the
Federal Trade Commission

Protecting the Privacy of Customers of Broadband and
Other Telecommunications Services, FCC Notice of Proposed Rulemaking
WC Docket No. 16-106
May 27, 2016

The FTC has long been the nation's privacy and data security enforcement agency. We have brought over 500 enforcement actions protecting the privacy and security of consumer information, including actions against ISPs and against some of the biggest companies in the Internet ecosystem.[1] We also conduct extensive consumer and business outreach and guidance; coordinate workshops to foster discussions about emerging privacy and data security issues; coordinate on international privacy efforts; and advocate public policies that protect privacy, enhance data security, and improve consumer welfare.[2] As a result, the FTC possesses significant privacy and data security expertise.

I strongly support FTC staff's comment, which applies that expertise to analyze the FCC's privacy Notice of Proposed Rulemaking (NPRM).[3] I write separately to emphasize the differences between the FTC's approach and the proposed FCC approach to consumer privacy and to warn that the FCC's approach may not best serve consumers' interests.

I. The FTC Approach Reflects Consumer Preferences About Data, Regardless of Which Entity Holds It

The FTC has built its privacy program on the long-established legal principles of unfairness and deception.[4] This framework focuses on the sensitivity of consumer data and

[1] *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.

[2] *See, e.g.*, 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/2017/01/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.

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

[4] 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

particular promises made about data collection and use, rather than on what type of entity collects or uses that data. By contrast, 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. It does not account for the sensitivity of the consumer data involved. Thus, the FCC would require opt-in consent for many uses of non-sensitive consumer data by BIAS providers, yet would require no consent at all for certain uses of sensitive data by those providers. By contrast, 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.

The FTC 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 study – that for uses of non-sensitive data, people have widely varying privacy preferences.[5]

Exercising and obtaining consent can be burdensome for consumers and businesses. Reading a notice and making a decision takes time that, in the aggregate, can be quite substantial.[6] Regulations should impose such costs in a way that maximizes the benefits while minimizing the costs. Therefore, opt-in or opt-out defaults should match typical consumer preferences, which means they impose the time and effort of making an active decision on those who value the choice most highly. 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. As former FTC Chairman Tim Muris and former Director of the FTC's Bureau of Consumer Protection Howard Beales stated,

> "Customers rationally avoid investing in information necessary to make certain decisions … when their decision is very unlikely to have a significant impact on them … Default rules should be designed to impose those costs on consumers who think they are worth paying. An opt-out default rule means that consumers who do not think that decision making costs are worthwhile do not need to bear those costs. Consumers who care intensely, however, will face the costs of making a decision."[7]

---

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.

[5] 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/.

[6] *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/.

[7] J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 115 n.20 (2008).

If a regulation imposes defaults that do not match consumer preferences, it imposes costs on consumers without improving consumer outcomes. The burdens imposed by a broad opt-in requirement may also have negative effects on innovation and growth.[8]

II. Discounts Based On Targeted Advertising May Benefit Consumers

The NPRM mischaracterizes the FTC's findings about what the FCC labels "financial inducement practices" but which most people know as "discounts."[9] The NPRM states, "the FTC and others have argued that these business models unfairly disadvantage low income or other vulnerable populations…."[10] But the FTC did not argue this. The portion of the FTC Big Data Report cited by the NPRM merely summarizes the concerns of some workshop participants – not FTC staff – about big data uses generally. Even on that point, the FTC report observed, "big data can create opportunities for low-income and underserved communities," and cites a broad range of existing examples.[11]

A ban on discounts for ad-supported BIAS prohibits a consumer from trading some of her data for a price discount, even if the consumer is fully informed. Would-be broadband subscribers cite high cost as more important than privacy concerns for the reason why they have not adopted broadband.[12] Given that fact, such a ban may prohibit ad-supported broadband services and thereby eliminate a way to increase broadband adoption.

At the very least, any rule on "financial inducement practices" ought to account for the FTC's observation that "in markets with sufficient alternatives," where "the terms of the exchange are transparent and fairly disclosed…such choice options may result in lower prices or other consumer benefits, as companies develop new and competing ways of monetizing their business models."[13]

---

[8] *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.").

[9] NPRM ¶ 261.

[10] *Id.*

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

[12] 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.

[13] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 52 (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

III. Conclusion

The FCC's NPRM seeks to protect the privacy and data security of BIAS consumers. To meet this laudable goal most effectively, the FCC should base its requirements on consumers' preferences about sensitive information and set opt-in and opt-out defaults accordingly. It should also permit consumers to make well-informed choices about discounted broadband offerings.