Statement of

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-

CON (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

ED. 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

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

III. Conclusion

The FCC's NPRM seeks to