

**Before the
Federal Trade Commission
Washington, D.C. 20580**

In the Matter of)
)
Competition and Consumer Protection) Docket No. FTC-2019-0032
in the 21st Century Hearings)

COMMENTS OF USTELECOM – THE BROADBAND ASSOCIATION

USTelecom – The Broadband Association (USTelecom)¹ applauds the Federal Trade Commission (FTC) on the successful completion of its series of public hearings on competition and consumer protection.² The hearings have provided a timely and important examination of the modern communications marketplace and the appropriate roles and responsibilities of government and industry to ensure all Americans have access to the opportunities made possible by broadband. Further, the FTC in these hearings has reviewed existing regulatory structures and explored a modernization of current rules and regulations to meet the communications and connectivity needs of consumers, businesses, government, and industry in the 21st Century.³ Throughout the course of the fourteen hearings and in comments filed in the record, ensuring provider transparency and protecting consumer privacy have emerged as recurring themes—

¹ USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives – all providing advanced communications service to both urban and rural markets.

² Hearings on Competition and Consumer Protection in the 21st Century, Notice, 83 FR 38307 (Aug. 6, 2018) (Notice), <https://www.ftc.gov/policy/hearings-competition-consumer-protection>.

³ See Comments of USTelecom on Competition and Consumer Protection in the 21st Century Hearings Topic 2, (filed Aug. 20, 2019).

specifically during Hearing #10: Competition and Consumer Protection Issues in Broadband Markets and Hearing #12: The FTC's Approach to Consumer Privacy.⁴

As this process made clear, consumers and businesses are increasingly benefiting from robust and increasing broadband competition for high-speed broadband service. With such connectivity comes a massive increase in the amount and types of data being produced. Broadband networks, the services they enable, and the data produced, offer substantial consumer benefits and are the engine of a significant portion of the U.S. economy. At the same time, without sufficient protections and transparency, that same data can also be used in harmful ways. The fundamental challenge for government is to create the optimal environment and regulatory certainty for industry to invest and innovate while ensuring that consumers are empowered with information they need to clearly understand the parameters of the services they are purchasing/using. Thus, consistent with these objectives, USTelecom supports the establishment of a single national privacy framework governing all stakeholders in the internet ecosystem and the continued promotion of competition and choice through transparency.

A National Privacy Framework Governing All Stakeholders in the Internet Ecosystem Is Essential. USTelecom supports the adoption of a strong national privacy framework governing all stakeholders in the internet ecosystem.⁵ The importance of a consistent national framework was appropriately an area of focus in discussions on consumer privacy during a number of the hearings, including the multi-day privacy hearings that contributed to a robust

⁴ Hearing #10: Competition and Consumer Protection Issues in Broadband Markets, FTC, (Mar. 20, 2019), <https://www.ftc.gov/news-events/events-calendar/ftc-hearing-10-competition-consumer-protection-21st-century>; Hearing #12: The FTC's Approach to Consumer Privacy, FTC, (April 9, 2019) <https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-february-2019>.

⁵ USTelecom also continues to support uniform national net neutrality legislation, rather than a state-by-state approach.

discussion on the optimal approach to privacy regulation in the United States. The discussion also reflected the importance of balancing the need for clear and strong protections for all American consumers with an approach that continues to allow for the unparalleled innovation that has driven the Internet economy thus far.

In order to provide the greatest legal certainty to consumers and businesses, any changes to United States policy must be implemented through *federal* legislation. The existing and expanding patchwork of state and sectoral-specific federal privacy laws is creating fragmented and inconsistent privacy protections for consumers. Federal legislation that establishes a strong national privacy law will provide uniform protections to American consumers regardless of where they live or how they access the Internet and avoid conflicting requirements. It will also reduce the burdens on companies of all sizes, including broadband providers large and small that serve every corner of the country who will be able to focus on compliance with a single national standard. Additionally, legislation would serve as an opportunity to further clarify and enhance the FTC's authority to police privacy practices and protect consumers, while preventing duplicative and inconsistent regulations.

State laws that apply to only one sector of the economy create inconsistent protections.⁶ The adoption of federal legislation is the clearest method to establish consistent privacy protections that are technologically neutral, ensure consistent data protection that individuals and companies can rely upon, and apply uniformly to companies that collect, use, or share consumers' online personal data. Further, national privacy legislation that preempts state

⁶ See e.g., Kate Patrick, *Maine's New Privacy Law Won't Crack Down on Big Tech's Data-Sharing Practices*, Inside Sources (June 10, 2019), <https://www.insidesources.com/maines-new-privacy-law-wont-crack-down-on-big-techs-data-sharing-practices/> (discussing the shortcomings in Maine's new privacy law that neglects to include companies other than ISPs in state privacy legislation).

privacy laws would avoid a patchwork of federal and state privacy laws that would provide consumers with uneven protections and force them to navigate a complicated menu of diverging state-specific privacy choices and controls.⁷

USTelecom supports federal legislation giving the FTC additional tools necessary to continue to enforce consumer privacy laws, in addition to its existing authority to enforce voluntary commitments by providers. The FTC has a proven history of privacy enforcement and for decades has been the nation's lead privacy and consumer protection cop on the beat. The FTC has brought more than 500 enforcement actions for privacy and data security violations, including cases involving major internet companies. Once Congress establishes a core set of privacy requirements in legislation, the FTC can evolve enforcement to address changing practices, business models, technologies, and consumer preferences through its long-standing and effective case-by-case enforcement authority. With the FTC as the exclusive federal authority to enforce the law, it would allow for the flexibility necessary in this changing landscape while also avoiding duplication and inconsistent outcomes. But such authority need not limit state Attorneys General from continuing to do they great they have done for years. Congress can empower state Attorneys General to enforce a new federal law. A new federal privacy law, however, should not include a private right of action which will result in company resources being diverted away from compliance which is the ultimate goal of any legislation.

Transparency Promotes Competition and Consumer Choice. Requirements and/or national legislation that require companies to be transparent and provide users with clear and

⁷ While the hearings and this discussion focus on consumer privacy, the same principles are true for other topics, including cybersecurity and net neutrality. State level and sector specific rules in these areas are equally problematic for many of the same reasons.

comprehensible information about the services and applications they provide can benefit consumers, as the Federal Communications Commission (FCC) held in its Restoring Internet Freedom Order.⁸ Transparency empowers consumers to make informed choices when differentiating among competing products and providers of services.

USTelecom members have long supported transparency. Broadband providers have made independent commitments to provide information about their internet access services and available plans.⁹ Such public transparency commitments are not just contractual promises to customers; providers that break them can be subject to FTC enforcement penalties or to civil litigation.¹⁰

In addition to clearly disclosing information on service terms and performance capabilities, USTelecom members are also committed to transparency in how they treat consumers' information. Consistent with the FTC's privacy framework,¹¹ USTelecom members are committed to being transparent about the categories of data they collect, how consumer data is used, and the types of third parties with whom data may be shared. Any policies and/or federal legislation should ensure that consumers have easy-to-understand privacy choices based on the sensitivity of the data. In order to ensure continued innovation, policy makers should recognize that data that is pseudonymized or de-identified reduces privacy risks for consumers

⁸ See 47 C.F.R § 8.1.

⁹ See Comments of Verizon on Competition and Consumer Protection in the 21st Century Hearings Topic 2, at 7, (filed Aug. 20, 2019) (Verizon Comments); See Comments of AT&T on Competition and Consumer Protection in the 21st Century Hearings Topic 2, at 6-7 (filed Aug. 20, 2019).

¹⁰ Verizon Comments at 24.

¹¹ *Protecting Consumer Privacy in an Era of Rapid Change; Recommendations for Businesses and Policymakers*, FTC Report, pp. 35-60 (Mar. 2012).

and requirements with regard to such data should be tailored accordingly.¹² Through the implementation of best practices in the areas of data security and data de-identification and pseudonymization, risks associated with the use of personal data are reduced.

While the disclosures described above are focused on the service being offered, broadband providers are also pushing for increased transparency as to *where* broadband service is and is not available. Through its Broadband Mapping Initiative pilot, USTelecom and a diverse consortium of broadband companies and associations are leading the industry in developing a highly granular map of broadband coverage in the United States so policymakers and consumers will know exactly where broadband is, and more importantly, where broadband is not available in the United States.¹³ As part of this initiative, USTelecom launched a pilot in Virginia and Missouri where broadband companies are combining their existing service provider address information with new digital resources, databases, and crowdsourcing platforms to improve policymakers understanding of areas that are served/unserved by broadband. This unprecedented, voluntary level effort will drive broadband deployment and competition as broadband providers compete to serve areas that are not connected. It will also ensure that federal and state government broadband funding programs can target scarce government dollars to areas that need it most.

¹² See *NISTIR 8053* by Simson L. Garfinkel, Information Access Division, Information Technology Laboratory, NIST, (Oct. 2015): “De-identification removes identifying information from a dataset so that individual data cannot be linked with specific individuals. De-identification can reduce the privacy risk associated with collecting, processing, archiving, distributing or publishing information. De-identification thus attempts to balance the contradictory goals of using and sharing personal information while protecting privacy.” <https://nvlpubs.nist.gov/nistpubs/ir/2015/nist.ir.8053.pdf>.

¹³ *Mapping the Broadband Gap: Broadband Mapping Initiative Action Center*, USTelecom.org, <https://www.ustelecom.org/broadband-mapping-initiative-action-center/> (last visited June 26, 2019).

Conclusion. The key to ensuring consumers are adequately protected in the Internet ecosystem is to make sure consumers know what service options are available to them and the terms of such offerings, including what data is being collected and how it is being used. Policies must empower consumers with the opportunity to exercise choice, while at the same time balance the need not to interrupt beneficial uses of information. The imposition of restrictions on data uses that would not result in material harm to consumers will stifle innovation and eliminate everyday customer conveniences. We urge the FTC to support Congress's efforts to enact Federal legislation that achieves the goals of protecting consumers and innovation.

Respectfully submitted,

USTELECOM



By: _____

B. Lynn Follansbee
Vice President, Policy & Advocacy

Kristine Fargotstein
Vice President, Policy & Advocacy

601 New Jersey Avenue, NW, Suite 600
Washington, D.C. 20001
202-326-7300

June 28, 2019