Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, D.C. 20230

In re:

Developing the Administration's Approach to Consumer Privacy
Docket No. 180821780-8780-01

COMMENTS OF CHARTER COMMUNICATIONS, INC.

Charter Communications, Inc. ("Charter") hereby submits its comments in response to the Notice and Request for Comment ("RFC") in the above-captioned matter.[1]

I. Executive Summary

As a leading provider of broadband internet services, Charter values and relies on the trust and loyalty of its over 26 million residential and business customers. Charter's network provides competitively-priced high-speed broadband, video, and voice services to neighborhoods of all types, from large cities to small towns and rural areas, from Fortune 100 customers to small businesses across the country.

One of Charter's key business objectives is to provide customers with a superior broadband experience that they use and value. To that end, Charter has invested more than $27 billion in broadband infrastructure and technology since 2014. Charter has boosted starting speeds to 200 Mbps in roughly 40 percent of the markets it serves and 100 Mbps in most of its remaining markets, with no data caps, modem fees, annual contracts, or early termination fees. Charter is also rolling out Spectrum Internet Gig, which delivers a one gigabit connection to homes and businesses. The company is on track to offer this service across nearly its entire footprint by the end of this year.

An increasingly important aspect of ensuring that consumers continue to utilize all the services the internet has to offer is making sure that they are confident that their personal information online is protected. That is why, last April, Charter CEO Tom Rutledge called for uniform privacy protections that would provide more meaningful consent for the use of their online information for all Americans no matter where they go on the internet.[2] We believe that a uniform national framework establishing strong online privacy protections and data security is needed to give all consumers confidence that their privacy is protected. This framework should seek to empower and inform consumers through rules that address five core principles—control, transparency, parity, uniformity, and security.

Charter therefore strongly supports NTIA's call for a framework that protects individual privacy and fosters technological innovation, particularly NTIA's focus on a privacy framework that "reduces fragmentation nationally and increases harmonization and interoperability nationally and

---

[1] *See* Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600 (Sept. 26, 2018).

[2] Tom Rutledge, Charter Chairman and Chief Executive Officer, *Charter Urges Congress to Pass Legislation Protecting Privacy Everywhere on the Internet*, BLOG, Apr. 8, 2018, available at https://policy.charter.com/blog/charter-urges-congress-pass-legislation-protecting-privacy-everywhere-internet/.

globally." Charter also appreciates the dialogue among stakeholders, consumer groups, and think tanks who have begun to examine potential approaches to protecting the privacy and security of consumers' personal information online—an outcome which will benefit both consumers and businesses.

II. A Strong Internet Privacy Policy Is Essential for Protecting Consumers and Encouraging Innovation

The internet has been a vibrant engine of economic growth and innovation over the last 20 years. Consumers in the United States and around the world increasingly rely on the internet to conduct their daily lives. Consumers use websites and mobile applications to find jobs, shop for groceries, take classes, manage their finances, connect with their loved ones, plan travel, arrange dates, and entertain themselves. Exciting new applications and use cases, such as telemedicine, offer tremendous potential to disrupt the U.S. economy and create new American jobs. For the internet to deliver on this promise, however, consumers must feel confident in their ability to control their personal information when using online services.

Unfortunately, according to data collected for NTIA by the U.S. Census Bureau, nearly half of internet users in the United States refrained from online activities due to privacy and security concerns.[3] Businesses collect, analyze, and share consumers' personal online information in unprecedented volumes; oftentimes without consumers having a clear understanding about these practices or why they are necessary. While there are legal protections for certain categories of particularly sensitive information, such as financial information and health-related data, vast amounts of other personal data are being collected, shared, tracked, and even sold online without specific protections.

Moreover, much of this online data collection happens without consumers' knowledge. Most websites embed tracking and advertising links throughout their pages, which direct the consumer's web browser to make requests to many unrelated sites instead of requesting content only from the intended destination. These sites collect user information and insert cookies into consumers' web browsers, which in turn enables third parties to track users' online activities and use this information to build comprehensive, highly individualized profiles.

Advertising networks and online data brokers are likewise often invisible to consumers, but these businesses collect, analyze, and share consumers' personal online information in unprecedented volumes. These entities often collect, use and share consumers' personal data for advertising purposes without providing meaningful notice to, or obtaining any form of consent from, consumers.

Rapid changes in technology have also made it more difficult for consumers to protect themselves. While some consumers can take steps to try to prevent certain collection activities—such as by disabling cookies on their web browsers or disabling location services on their mobile device—they may not be aware of opaque data collection practices when they are online or when they start using a new online device or app. Some online entities now identify consumers via device fingerprinting, "a

[3] *See* National Telecommunications and Information Administration, "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities" (May 13, 2016), https://www ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

technique for identifying a computing device (*e.g.*, desktop, laptop, tablet, or smartphone) based on its unique configuration."[4] This permits companies to associate online activity and behavior with a particular consumer even when a consumer's web browser has been set to reject cookies. The constant evolution of technology and data collection practices can further impede consumers' efforts to protect themselves.

Consumers should not bear the burden of understanding the complex array of entities that operate online and collect, use, and share personal information. Practices that fuel consumer uncertainty are detrimental to economic growth. A comprehensive and technology-neutral legal framework for online privacy that applies to all entities in the internet ecosystem will not only help instill consumer confidence but also enable businesses and consumers to take full advantage of the possibilities presented by technological advances.

III. The Legal Framework for Online Privacy and Data Security Policy Should Be Clear and Comprehensive

For the foregoing reasons, Charter believes that a national legal framework with strong online privacy and data security protections is critical both to maintaining its relationships with its customers, and ensuring that the internet continues to function as a powerful economic engine for the entire economy in the digital age. Charter agrees that privacy outcomes must be "user-centric."[5] Consumer empowerment must be the cornerstone of any policy or framework that protects consumer online privacy, and the framework must establish uniform online privacy protections for all Americans, no matter where they go on the internet or how they interact with online services.

Charter believes that such a comprehensive framework should focus on the following core principles:

(1) **Consumer Control.** As NTIA acknowledges in its RFC, providing consumers with control over their personal information is a key aspect of an effective privacy regime. Consumers should be empowered to have meaningful choice for each use of their data. Charter believes that the best way to ensure consumers have control over their data is through opt-in consent. Any legal framework that is ultimately adopted should ensure consumer consent is purposeful, clear, and meaningful. In addition, the use of personal data should be reasonably limited to what the consumer understood at the time consent was provided. Companies also should ensure that consent is renewed with reasonable frequency.

Charter has concerns about the use of "context" to ascertain whether a consumer has consented to the collection and use of personal data.[6] Any exceptions to consumer control mechanisms should

---

[4] Bernard Marr, *How Businesses Use Controversial Device Fingerprinting to Identify and Track Consumers*, Forbes.com (June 23, 2017), https://www.forbes.com/sites/bernardmarr/2017/06/23/how-businesses-use-controversial-device-fingerprinting-to-identify-and-track-customers/#3775b34e3d46.

[5] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600, 48601 (Sept. 26, 2018).

[6] *See* 83 Fed. Reg. at 48601.

be clear and limited. Charter believes that a strong consumer-centric privacy framework should ensure that consumers are in the best position to make informed decisions about how their information is used. Entities providing online services would also benefit from the certainty of having clear obligations regarding consumer consent. To the extent that NTIA includes the context concept in its privacy framework, considerable effort needs to be undertaken to clarify exactly what context means (and doesn't mean) to ensure consumers are empowered to control their personal online data.[7]

(2) **Transparency.** Charter agrees with NTIA's statement in the RFC that transparency is a desired outcome of any comprehensive framework[8] and that users should be able to easily understand how organizations collect, store, use, and share their personal information. Consumers should be given the information they need to make an informed decision. Explanations about how companies collect, use, and maintain consumers' data should be clear, concise, easy-to-understand, and readily available. Privacy policies should be separate from other terms and conditions of service. If all online entities provide transparency, consumers will have the ability to weigh the potential benefits and harms of the collection and use of their personal data. As NTIA acknowledges, lengthy notices provided to consumers when they first interact with a service often do not achieve this goal.

(3) **Parity.** Consumers are best served by a framework that is applied consistently across the entire internet ecosystem not based on who is collecting it, or whether a service is free or paid. From a consumer standpoint, they want their online data protected whether they are using an ISP like Charter, a search engine, an e-commerce site, a streaming service, a social network, or a mobile carrier or device. Consumers should know that their personal information is being treated with the same level of protections wherever they go on the internet.

(4) **Uniformity.** For these protections to be effective there should be a single national standard to protect consumers' online privacy regardless of where they live, work, or travel. Where a consumer's information is adequately protected should not differ based on which state he or she is logging in from. A patchwork of state laws is confusing for consumers, difficult for businesses to implement, and hinders continued innovation on the internet—which is a borderless technology.

(5) **Security.** Strong data security practices should include administrative, technical, and physical safeguards to protect against unauthorized access to personal data, and ensure that these safeguards keep pace with technological development.

---

[7] Even seemingly straightforward contextual exceptions such as for first party marketing, which can be beneficial for consumers, could undermine the goal of consumer control if they are not subject to clear guardrails. Any exception for first-party marketing, for instance, should take account of the fact that the entity collecting the information may operate an extensive array of affiliates, many of which may not have any direct interaction with the consumer or may not be co-branded with the collecting entity and thus may not be readily identifiable to the consumer as related to the collecting entity.

[8] 83 Fed. Reg. at 48601.

Charter believes that a federal framework which incorporates these principles will produce the best outcomes for both consumers and businesses and that it is possible to construct such a framework while preserving the necessary flexibility to promote competition and innovation.

IV. The FTC Is the Appropriate Agency to Address Online Consumer Privacy Concerns

Charter strongly believes that the Federal Trade Commission ("FTC" or "Commission") should serve as the Federal consumer privacy enforcement agency with regard to the national online privacy and security framework.[9] The Federal Trade Commission Act grants an expansive mandate to the Commission and empowers it to combat unfair methods of competition and unfair or deceptive acts or practices through a variety of tools, including conducting investigations, bringing enforcement actions, issuing guidelines and reports, and making legislative recommendations. As the nation's leading agency in this area, the Commission has broad authority to safeguard consumers and enforce privacy and data security protections across the entire online ecosystem. The Commission and its Bureau of Consumer Protection are recognized throughout the world as a leading authority on these issues.

The Commission's record with respect to online consumer privacy protection is unparalleled; it has protected consumers by bringing hundreds of privacy and data security cases under the authority conferred by Section 5 of the Federal Trade Commission Act, including enforcement actions involving the misuse of personal information across various sectors of the online ecosystem. The Commission's prior work in this area, including its enforcement actions as well as the work memorialized in its 2012 report "Protecting Consumer Privacy in an Era of Rapid Change,"[10] demonstrates its commitment to striking the proper balance between innovation and privacy as technology and consumer expectations continue to evolve. Designating the Commission as the agency that will continue to take the lead in protecting consumers in this arena will avoid a situation in which regulation of these issues is fragmented across multiple agencies, which would risk disruption, uncertainty, and divergence of oversight for similarly situated companies.

---

[9] *See* 83 Fed. Reg. 48603 (stating the "high-level end-state goal[]" of having the FTC "continue as the Federal consumer privacy enforcement agency, outside of sectoral exceptions beyond the FTC's jurisdiction"). Among providers of video services, only cable and satellite companies are subject to sector-specific privacy framework codified in the Communications Act. *See* 47 U.S.C. §§ 338(i) (satellite); 551 (cable). In today's marketplace, however, consumers are increasingly turning to over-the-top providers and virtual multichannel video programming distributors for their video programming. As consumers "cut the cord" in favor of "virtual" MVPDs like Hulu and Sling, and online video distributors like Netflix and Amazon Prime Video, the total number of traditional MVPD customers dropped in the last quarter of 2017 by 3.4% compared to a year earlier—the highest rate of decline since the trend of cord cutting emerged in 2010. *See* Aaron Pressman, "Cord Cutting Hits Another Record, Bashing Cable and Telecom Stocks," Fortune, Mar. 1, 2018, http://fortune.com/2018/03/01/cord-cutting-record-internet-tv/. In fact, a quarter of U.S. households do not have cable *or* satellite service. *See* Press Release, Gfk, *One-Quarter of US Households Live Without Cable, Satellite TV Reception – New Gfk Study* (July 13, 2016), https://www.gfk.com/en-us/insights/press-release/one-quarter-of-us-households-live-without-cable-satellite-tv-reception-new-gfk-study/.

[10] Federal Trade Commission, FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, Mar. 2012.

NTIA asks whether, in order to achieve the goals of the RFC, any changes would be necessary with regard to the FTC's resources, processes, and/or statutory authority.[11] As the Commission's broad mandate and past experience make clear, it currently has a wide range of tools at its disposal to navigate these extraordinarily complex and rapidly changing issues. In addition to enforcement actions against individual entities, these tools include the development and implementation of guidelines, similar to those that the Commission has developed and implemented in other contexts;[12] issuing reports, and promoting legislation. Charter remains open to further discussions with government and other stakeholders on how the Commission can best address privacy-related issues in the future.

V. Conclusion

Charter strongly supports NTIA's focus on protecting consumer privacy while fostering innovation. We believe the five core principles outlined in these comments—control, transparency, parity, uniformity, and security—should form the foundation of the framework for achieving these goals. We appreciate this opportunity to participate in the development of the Administration's approach to consumer privacy.

Respectfully submitted,

Rachel C. Welch
Senior Vice President
Policy and External Affairs
Charter Communications, Inc.

Rachel.Welch@charter.com

Marc A. Paul
Vice President
Policy and External Affairs
Charter Communications, Inc.

Marc.Paul@charter.com

+1 (202) 370-4280

[11] 83 Fed. Reg. at 48603.

[12] For example, the Horizontal Merger Guidelines promulgated by the Commission in conjunction with the DOJ have had an enormous influence not just on how U.S. antitrust agencies conduct merger policy but also on how courts and antitrust agencies throughout the world make decisions about the antitrust consequences of mergers. The Merger Guidelines set expectations for the Agencies and for businesses; and assist businesses to understand the state of the law in practical terms and allow them to structure their affairs with greater confidence.