Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

In re:	)	
	)	
Competition and Consumer Protection	)	Project No. P181201
in the 21st Century	)	
	)	

COMMENTS OF CHARTER COMMUNICATIONS, INC.

Charter Communications, Inc. ("Charter") hereby submits its comments in connection with the upcoming hearings announced by the Federal Trade Commission (the "Commission") on the subject of competition and consumer protection in the 21st Century.

I. EXECUTIVE SUMMARY

Charter appreciates the Commission undertaking these hearings to examine the implications of technological changes on competition and consumer protection enforcement inspired by the Commission's 1995 "Global Competition and Innovation Hearings" under the leadership of then-Chairman Robert Pitofsky, especially in light of technology's enormous impact on the privacy and security of online data. Charter will focus its comments on questions 4, 5 and 10 raised in the Commission's Notice.[1]

Rapid advances in technology continue to radically change the privacy landscape. Businesses now collect, analyze and share consumers' personal data in unprecedented volumes. As a leading provider of broadband internet services, Charter values and relies on the trust and loyalty of its approximately 24 million residential and business broadband customers across 41 states. Charter's network provides competitively priced high-speed broadband services to

---

[1] *See* Hearings on Competition and Consumer Protection in the 21st Century, 83 Fed. Reg. 38307 (Aug. 6, 2018). Charter recognizes that the Commission has requested comments on additional topics, and it supports the comments of the National Cable & Telecommunications Association (NCTA) addressing those other topics.

neighborhoods of all types, from large cities to small towns and rural areas, from Fortune 100 companies to small businesses across the country. Charter's key business objective therefore is to provide its 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. The company has boosted starting speeds to 200 Mbps in roughly 40% of the markets it serves and 100 Mbps in the remaining 60%—all with no data caps, early termination fees or modem fees. A critical part of that superior broadband experience is customers feeling their privacy and information are secure when they are online. Indeed, in light of its ongoing relationships with its customers and because Charter does not require annual contracts, the Company is accountable to its customers every day.

Given changes in technology use and consumers' expectations around the protection of personal online information, earlier this year Charter called for a national legal framework establishing uniform online privacy protections for all Americans no matter where they go on the internet. Charter believes such a framework should focus on the following core principles:

> Consumer Control and Meaningful Consent: Consumers should be empowered with meaningful control of their personal data online such as by requiring consumers be given a choice—an "opt-in"—for the collection, use and disclosure of such data.
>
> Transparency: In order to exercise control effectively over their online personal data, consumers should be given clear, concise, meaningful and readily available information about how their information is collected, used and disclosed. Without transparency, consumers cannot make informed decisions about how and when to protect their online personal data.
>
> Parity: A comprehensive and consistent approach to privacy that applies to all entities in the online ecosystem is necessary to give consumers confidence that their personal information is protected anywhere they go online and to reduce consumer confusion about when, where and how their personal data is being used. Consumers are best served by such a single framework that is applied consistently and based on the type of data being collected and how it will be used, and not based on the entity that is collecting and using the data.

Uniformity: The internet is inherently a borderless technology. Therefore, a federal framework is critical to protecting consumers, fostering innovation and ensuring competition among businesses. A patchwork of inconsistent online privacy laws is unworkable and will only lead to confusion for consumers and businesses alike.

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.

Each of these core principles is discussed in more detail below.

II. DATA PROTECTION IS A KEY TO CONSUMER CONFIDENCE AND A STRONG ECONOMY

Charter strongly believes that the entire online ecosystem benefits when consumers feel confident that their privacy is protected throughout their online experience. But it is difficult for this trust to be established and maintained without a consistent legal framework regarding the collection, use, disclosure and security of consumers' personal data online. According to data collected for NTIA by the U.S. Census Bureau, nearly half of internet users in the U.S. refrained from online activities due to privacy and security concerns.[2] Accordingly, Charter believes that a 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 our entire economy in the digital age. Consumers in the U.S. and around the globe rely more and more on the internet to conduct their daily lives. Websites and apps are used to find a job, shop for groceries, access healthcare, take a class, connect with loved ones and be entertained. If consumers lose confidence in their online experience, the impact would be widespread.

---

[2] *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.

Parity across every step of a consumer's online experience is particularly important to maintain consumer confidence. If certain entities are exempt from the online data privacy requirements or held to a lower standard, those entities will be able to collect and use personal information from consumers without their knowledge and will not be constrained by consumers' expectations regarding the privacy and security of personal data—a result that will only sow consumer doubt and confusion. For these reasons, it is essential that consumers have confidence that all entities in the internet ecosystem adhere to the same requirements governing the collection, use, disclosure and security of online personal data.

With the adoption of the General Data Protection Regulation (GDPR) in Europe, along with individual U.S. states adopting (or looking to adopt) their own approaches to privacy regulation, the time is right for the Commission to initiate these hearings and examine the current approach to protecting online privacy and data security in order to determine whether more guidance is needed to provide certainty and clarity for consumers, industry and our economy. Given its longstanding and well-regarded work in the area of online privacy, as well as its expertise in consumer protection and competition, the Commission is uniquely qualified to provide important guidance to Congress, consumers and businesses on this important subject. Through these hearings, the Commission can ensure that the U.S. remains a leader in online privacy and data security.

III. CONSUMER PROTECTION MUST KEEP PACE WITH RAPID ADVANCES IN TECHNOLOGY

Today, consumers can be tracked online, and their data can be collected, collated, analyzed and used in ways they may not be aware of, expect or understand. Consumers are right to be concerned, given the intrusive nature of some of the data collection and use that goes on. For instance, a consumer accessing a website from home may be tracked by: the ISP providing

the consumer's connection to the internet and access to the site; the search engine that directed the consumer to the site; the web browser; the site itself; the advertisers posting ads on the site; and social networks connected to the site.

Consumers are even less aware of the tracking often done in the background by entities that are not visible to consumers as they surf the web. Third-party ad networks and online data brokers are likewise invisible to consumers.[3] For instance, if a consumer reads a newspaper through its website, third-party advertising networks are present in the background, using "cookies" (small text files that these ad networks drop on consumers' browsers) to track and collect information about the reader's activity not only on that website but also on other sites the reader visits.[4] These entities sell the personal data that they collect for advertising purposes, but without providing meaningful notice to, or obtaining any form of consent from, consumers.[5] Consumers have few, if any, mechanisms to learn about these hidden entities that are collecting and using their personal data.

While consumers can take steps to try to prevent the collection and use of their online personal data (such as disabling cookies on their web browsers or disabling location services), technology and data collection practices continue to evolve, which can impede consumers' efforts to protect themselves. For example, some online entities now are identifying consumers by using device fingerprinting, which is "a technique for identifying a computing device (*e.g.*,

---

[3] Jessica Rich, *Keeping Up with the Online Advertising Industry*, Federal Trade Commission, Apr. 21, 2016 (noting that many of the online advertising companies "are [collecting information about consumers' online activity] behind the scenes, completely invisible to most of us"), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry.

[4] The Wall Street Journal, *Privacy Policy* (May 5, 2015) ("Third parties that support the Dow Jones Online Services by serving advertisements … may also use [tracking technologies] to … collect Other Information on the Dow Jones Online Services and on other websites."), https://www.wsj.com/policy/privacy-policy.

[5] Arvind Narayanan and Dillon Reisman, *The Princeton Web Transparency and Accountability Project* (2017) at 1, 5 (explaining how pervasive online tracking by "hidden" third parties is and how these third parties identify and develop profiles about internet users), http://randomwalker.info/publications/webtap-chapter.pdf.

desktop, laptop, tablet or smartphone) based on its unique configurations."[6] Thus, even if a consumer configures his or her browser to reject cookies, companies can use device fingerprinting to associate online activity and behavior with that particular customer, defeating his or her attempt to remain anonymous. A similar problem exists in connection with the use of so-called "location services." Some consumers prefer not to use such services due to concerns about others being able to monitor their whereabouts and want clear control over when and how their location information is collected, used and shared.

There are benefits that flow from the collection and use of consumers' personal data online, including the ability to more effectively tailor services to individual consumers, whether by retaining login credentials, making recommendations or otherwise providing a more relevant consumer experience. However, consumers should be informed and have the ability to consent to such collection and use, as well as any disclosure to third parties. In many instances, consumers are unable to exercise control over their personal information because they are uninformed or unaware of what online personal data is being collected, by whom and how that data is being used and shared.

Companies that offer subscription-based services must balance the benefit of collecting data with the potential loss of customers should a consumer decide to stop purchasing their products or services. Entities with a more transitory relationship or no direct consumer relationship, and a business model built primarily around the monetization of consumers' personal information, may have less incentive to provide consumers meaningful control over their data. These entities may resist giving users the ability to opt-in to the collection, use and

---

[6] 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.

disclosure of personal online data, or obscure even the option of opt-out consent through opaque privacy policies, because of the nature of their business model.

Consumers cannot be expected to adequately protect themselves, as many do not fully understand how data collection technology works, and do not yet have settled expectations about what is acceptable data collection and use by the entities they interact with directly or indirectly online. Consumers should not bear the burden of understanding the complex array of entities that operate online and collect, use and share personal information. Further, practices that fuel consumer uncertainty are detrimental to economic growth. A comprehensive and competitively neutral legal framework for online privacy that applies to all entities operating online will help instill consumer confidence and enable businesses and consumers to take full advantage of the possibilities presented by technological advances.

IV. PRIVACY AND DATA SECURITY ENFORCEMENT AND POLICY SHOULD BE CONSUMER-CENTRIC

As the Commission examines whether changes in the economy, evolving business practices and new technologies require adjustments to competition and consumer protection law, its enforcement priorities and its policy approach, a consumer-centric approach will ensure that consumers have confidence in using online services and that businesses have the incentives necessary to develop new products and services that benefit consumers and earn their trust. Charter respectfully submits that privacy and data security enforcement and policy should be guided by the following core principles:

A. Consumers Should Be Empowered with Control and Meaningful Consent Over Their Data

Charter believes that the cornerstone of any policy or framework protecting online consumer privacy must be the empowerment of consumers. Any legal framework should ensure

consumer consent is purposeful, clear and meaningful. Businesses should be required to obtain affirmative "opt-in" consent from their customers prior to collecting, using or sharing their personal online data. Implied consent should be permitted only in limited circumstances that are consistent with their expectations. For example, it is reasonable to infer that a consumer consents to the use of his or her personal data when it is essential to provide the service requested or to collect unpaid bills to the provider. There may be other circumstances where implied consent would be reasonable, but the Commission should carefully examine how best to limit any exception to reflect consumers' reasonable expectations.

While Charter believes that this opt-in approach is in the best interests of consumers and economic growth, it also recognizes that there may be other equally effective ways to empower consumers and to address the issues surrounding the collection, use and disclosure of personal data online, while at the same time preserving innovation and competition in the marketplace. Charter is prepared to work with the Commission, lawmakers, consumer groups, academic experts and other players in the industry to consider a range of alternatives. Charter firmly believes, however, that legal and enforcement efforts should empower consumers to control how their online personal data is collected, used and shared with third parties.

B. Companies Should Be Transparent About What Personal Data They Are Collecting and How They Are Using It

Privacy practices also should be transparent to consumers. Companies collecting personal data online should be required to provide clear, concise and easy-to-understand privacy policies to their consumers. Those policies should be provided before personal data is collected; they should be separate from the company's standard terms of use and written in plain language that is easy-to-understand; and they should continue to be readily accessible to consumers at any time. Consumers also should be notified of any material changes to a company's privacy policy.

By ensuring that all online entities provide such transparency, consumers will have the ability to weigh the potential benefits and harms related to the collection, use and disclosure of their personal data, and thus truly provide informed consent.

C. Consumer Data Should Be Protected Consistently Throughout the Online Experience

Consumers should feel confident that their online personal data is strongly protected throughout their online experience. It makes no difference to consumers whether their information is being collected by a search engine, an e-commerce site, a streaming service, a social network, a mobile carrier or device, or an ISP. A sectoral-based approach will only lead to consumer confusion and entrench the dominance of certain companies or sectors that are not subject to the same obligations as others. Moreover, guidelines that disfavor one technology or business model over another would deter market entry, thwart innovation and limit competition.

Different privacy practices should not be permitted for the same type of personal data depending on the business model of an entity, or the kind of entity collecting and using the data. These distinctions can lead to competitively harmful gamesmanship that will only reduce consumer confidence, negatively impacting the overall value of the online experience.

D. Consumer Data Should Be Protected By a Uniform Federal Approach to Enforcement and Policy

Charter believes that uniformity and consistency are critically important to reduce consumer confusion and increase consumer protection. For that reason, an effective consumer privacy framework should apply uniformly nationwide, regardless of the location of the companies or consumers at issue. At present, different states are developing and implementing different consumer privacy and data protection laws. Such a patchwork of state laws will be confusing for consumers and difficult for companies to implement. Moreover, such disparate

state laws ignore the very nature of the internet, which operates without regard to state (and international) borders. A uniform and national approach is needed to avoid uncertainty and to enable future innovation.

E. Consumer Data Should Be Protected with Strong Data Security Practices

Any legal framework should ensure all entities collecting, using and sharing such data establish strong data security practices. A recent survey by Parks Associates showed that approximately 45% of consumers are "very concerned about people accessing their devices or data without permission," and consider data security and privacy issues as "their greatest concern about connecting devices to the internet."[7] Companies should implement administrative, technical and physical safeguards to protect against unauthorized access to online personal data, and ensure that these safeguards keep pace with technological development.

V. THE FTC IS THE APPROPRIATE AGENCY TO ADDRESS ONLINE PRIVACY AND DATA SECURITY

The Commission is the appropriate agency to address the issues related to online privacy and data security. As the nation's leading Agency in this area, it has broad authority to safeguard consumers and enforce privacy and data security protections across the entire online ecosystem.[8] This authority flows from the expansive mandate granted to the Commission under the Federal Trade Commission Act, which—among other things—empowers the Commission to prevent unfair methods of competition and unfair or deceptive acts or practices in a variety of ways,

---

[7] *See* "Nearly one-half of consumers cite strong data and privacy concerns related to Internet-connected devices," Parks Associates, Sept. 26, 2017 (http://www.parksassociates.com/blog/article/ceu-2017-pr5).

[8] By contrast, the FCC's jurisdiction is limited to regulation of interstate communications by radio, television, wire, satellite and cable. *See* 47 U.S.C § 151.

including by conducting investigations, bringing enforcement actions, issuing guidelines and reports and making legislative recommendations.[9]

Consumer protection has served as a core part of the Commission's mission for many years, across both Republican and Democratic administrations. The Commission currently employs over 600 full-time equivalent employees devoted to consumer protection.[10] The Commission and its Bureau of Consumer Protection are recognized throughout the world as a leading authority on these issues.

In particular, the Commission has a strong track record with respect to online privacy related matters. The Commission can and should build off of the extensive work it already has engaged in on these issues, including the work that is memorialized in the Commission's 2012 report "Protecting Consumer Privacy in an Era of Rapid Change," which was prepared after soliciting and receiving public comments from businesses, privacy advocates, technologists and individual consumers, and which was part of a joint effort between the White House, the Department of Commerce and the Commission to push Congress to enact more robust consumer privacy laws governing the online ecosystem.[11] Other examples of the Commission's robust experience in this area include Staff Reports on Online Behavioral Advertising and Mobile Privacy Disclosures,[12] guidance for small businesses with respect to privacy and security,[13] and

---

9 15 U.S.C. § 45, 46, 57a.

10 *See* Federal Trade Commission, Fiscal Year 2019 Congressional Budget Justification at p. 2.

11 *See* Edward Wyatt, *F.T.C. and White House Push for Online Privacy Laws*, The Washington Post, (May 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.

12 *See* Self Regulatory Principles for Online Behavioral Advertising, Federal Trade Commission Staff Report (Feb. 2009); Mobile Privacy Disclosures: Building Trust Through Transparency, Federal Trade Commission Staff Report (Feb. 2013);

13 *See, e.g.*, Protecting Personal Information: A Guide for Business (https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business); Start with Security: A Guide for Business (https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business).

numerous privacy and security workshops and industry outreach programs,[14] all of which further affirm the same fundamental principles of consumer empowerment and transparency that should apply here.

The Commission also should continue to be the lead enforcer with respect to online consumer privacy protection. The Commission's record in this respect is unparalleled; it has protected consumers by bringing over 500 privacy and data security cases under its Section 5 authority, including enforcement actions involving the misuse of personal information across various sectors of the online ecosystem.[15]

The Commission's prior work in this area demonstrates its commitment to striking the proper balance between innovation and privacy as technology and consumer expectations continue to evolve. Moreover, by continuing to take the lead in protecting consumers in this arena, the Commission 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.

As the Commission's broad mandate and past experience make clear, it has a wide range of tools at its disposal to navigate these extraordinarily complex and rapidly changing issues. These tools include the ability to develop and implement guidelines, similar to those that the

---

[14] *See, e.g.*, https://www.ftc.gov/news-events/events-calendar/2018/02/privacycon-2018; https://www.ftc.gov/news-events/events-calendar/2010/03/exploring-privacy-roundtable-series; https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

[15] *See generally* 163 Cong. Rec. at H2493 (Mar. 28, 201) (statement of Rep. Flores) (noting that the FTC's framework has generated "over 500 cases protecting consumer information [and] ensuring their online privacy"); *see also, e.g., United States* v. *VTech Electronics*, Case No. 1:18-cv-00014 (N.D. Ill.); *FTC* v. *Uber Technologies, Inc.*, Case No. 3:17-cv-00261 (N.D. Cal.); FTC, *In the Matter of Snapchat, Inc.*, Docket No. C-4501; *FTC* v. *Ruby Corp et al.*, Case No. 1:16-cv-02438 (D.D.C.); *United States* v. *InMobi Pte Ltd*, Case No. 3:16-cv-3474 (N.D. Cal.); *FTC* v. *MaxTheater, Inc.*, 2005 WL 3724918 (E.D. Wash. Dec. 6, 2005).

Commission has developed and implemented in other contexts.[16] Additionally, the Commission can, as it has in the past, issue a report, take enforcement action against individual entities, or promote legislation. At this stage of the inquiry, Charter remains open to considering a wide range of different proposals about the best way to manage this complex ecosystem.

VI. CONCLUSION

Charter fully supports the Commission's efforts to examine the complex issues related to online privacy and data security raised in its Notice. The Company looks forward to the opportunity to participate in the upcoming public hearings and to discuss these issues in greater detail. While Charter is prepared to consider a range of different alternatives to protect online privacy and data security, Charter believes that the core principles listed above—control and consent, transparency, parity, uniformity and security—should form the foundation of the Commission's analysis.

Should the Commission have any questions in relation to these comments or the upcoming hearings, please contact Rachel C. Welch, Senior Vice President, Policy and External Affairs (Rachel.Welch@charter.com), or Marc A. Paul, Vice President, Policy and External Affairs (Marc.Paul@charter.com), or by telephone on +1 (202) 370-4280.

---

[16] 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.