STATEMENT OF RACHEL WELCH,
SENIOR VICE PRESIDENT POLICY AND EXTERNAL AFFAIRS, CHARTER COMMUNICATIONS
ON
"EXAMINING SAFEGUARDS FOR CONSUMER DATA PRIVACY"
BEFORE THE
SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

September 26, 2018

Introduction

Good morning, Chairman Thune, Ranking Member Nelson, and distinguished members of the Committee. Thank you for the opportunity to appear today.

I am Rachel Welch, Senior Vice President, Policy and External Affairs at Charter Communications. I lead the team that develops our public policy positions here in Washington and across the 41 states we serve.

As a leading provider of broadband internet services, Charter values and relies on the trust and loyalty of its more than 26 million residential and business customers. Our 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.

Fundamentally, one of our key business objectives is to provide our customers with a superior broadband experience that they value and use. To that end, we have 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 we serve and 100 Mbps nearly everywhere else, with no data caps, no modem fees, no annual contracts and no early termination fees. We are also rolling out Spectrum Internet Gig which delivers a one gigabit connection to homes and businesses and we are on track to offer this service across virtually our entire footprint by the end of the year.

Charter appreciates the Committee holding this hearing and focusing on the complex issues that impact consumers' online privacy. We also appreciate the developing dialogue among stakeholders – including those seated next to me here today – as well as consumer groups, think tanks and others who have begun to examine potential approaches to protecting the privacy and security of consumers' personal information online.

Consumers Need a Comprehensive Online Privacy Framework

Advances in technology have radically changed the privacy landscape. Despite Americans' daily reliance on websites, apps, and social media, it is difficult for consumers to understand and appreciate how companies are collecting, analyzing, sharing and selling a tremendous amount of information about them.

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. While we strive to give our customers confidence with our current policies and practices such as not selling any information that personally identifies our customers to third parties, we recognize that there is still more to do.

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. We believe that a uniform national framework establishing strong online privacy protections and data security is needed to give all consumers, including our customers, confidence that their privacy is protected. We believe that this framework should seek to empower and inform consumers through rules that address five core principles – control, transparency, uniformity, parity and security.

Businesses now collect, analyze, and share consumers' personal online information in unprecedented volumes. 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.

Threats to privacy and security are pervasive on the Internet today. Consumers' personal data is exposed to more entities than ever before and much of this data collection happens without their knowledge. For example, most web sites embed tracking and advertising links throughout their pages. The consumer's web browser is directed by the destination site 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 their browser. This enables third parties to track where the user goes online and stitch together their online behavior to build a comprehensive, highly individualized profile about him or her.

Rapid changes in technology have also made it more difficult for consumers to protect their online data. While some consumers can take steps to try to prevent certain collection activities that may be more well-known—such as by disabling cookies on their web browsers or disabling location services—they may not be aware of other practices that are not visible when they surf the web or fire up the latest new device or app. For instance, third-party ad networks and online data brokers are often invisible to consumers. Moreover, technology and data collection

practices are constantly evolving, which can further impede consumers' efforts to protect themselves.

Online Privacy is A Critical Part of Ensuring Economic Security

The internet has been a vibrant engine of economic growth and innovation for the last 20 years. Consumers in the United States and around the world rely more and more on the internet to conduct their daily lives. Websites and apps are used to find jobs, shop for groceries, take classes, manage finances, connect with loved ones, plan travel, find dates, and be entertained. Exciting new applications and use cases, such as telehealth and telemedicine, offer tremendous potential to bring similar disruption to other sectors of the U.S. economy and create thousands of new American jobs. For the internet to continue to deliver on this promise, however, users must continue to feel confident in their ability to control their online data.

Unfortunately, according to data collected for the National Telecommunications and Information Administration (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. Similarly, 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 privacy and security issues to be "their greatest concern about connecting devices to the internet."

A comprehensive legal framework for online privacy that empowers and informs consumers will increase consumer confidence in online services. If the framework is competitively neutral and reflects the principle of parity, it would not impede businesses from developing new technologies or business models that will encourage market entry, innovation, and robust competition. Instead, it would ensure that businesses have the necessary incentives to develop new products and services that both benefit consumers and earn their trust.

It's on all of us to develop a comprehensive framework that will help Americans avoid uncertainty and enable continued innovation economic growth in the future. We believe that a federal framework is the best path forward.

Five Principles for Protecting Consumers Online

We appreciate that Congress is taking up the issue of online privacy and data security and recognize that there are a range of ideas and methods for protecting online data. We believe that a national online privacy framework should start with the consumer and be grounded in the concept of empowering and informing consumers to control the personal information that is collected about them online.

Charter believes such a framework should focus on the following core principles.

The first principle is control. Consumers should be empowered to have meaningful choice for each use of their data. We believe 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. That means no more pre-ticked "boxes," take-it-or-leave-it offers, or other default consents. It also means that 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.

The second principle is transparency. 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 such transparency, consumers will have the ability to weigh the potential benefits and harms of the collection and use of their personal data, and truly provide informed consent.

The third principle is parity. Consumers are best served by a uniform 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. Quite simply, we believe consumers should know that their personal information is being treated with the same level of protections wherever they go on the Internet.

The fourth principle is uniformity. For these protections to be effective there should be a single national standard that protects consumers' online privacy regardless of where they live, work or travel. Whether 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 would be confusing for consumers, difficult for businesses to implement, and hinder continued innovation on the internet—which is a borderless technology.

The final principle is security. At Charter we believe privacy is security and security is privacy. 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.

We support the adoption of legislation that is based on these principles. We also believe that the Federal Trade Commission is the appropriate agency to oversee and enforce online privacy and data security. The FTC is the nation's leading agency when it comes to privacy enforcement, having brought hundreds of privacy and data security cases. Importantly, it has broad authority to safeguard consumers and enforce privacy protections across the entire online ecosystem. As

a result we believe that the FTC is the right agency to oversee and implement any legislative framework.

Conclusion

Revelations of data misuse in recent years have led to a long-overdue public conversation about what happens to data online and the vulnerabilities that develop when online data goes unprotected. Consumers today and in the future deserve to have the ability to control how their information is collected and used whenever they use the internet, and wherever they go online.

As our CEO Tom Rutledge has said, different policies that lead to inconsistent protections sow confusion and erode consumers' confidence in their interactions online; this is bad for business and bad for America since it threatens the Internet's future as an engine of economic growth.

Charter looks forward to the opportunity to work with Members of Congress, industry partners, consumer groups and other stakeholders to develop legislation that protects consumers, and makes them feel more confident taking advantage of all that the Internet has to offer.

I thank the Members of the Committee for the opportunity to appear before you today on this important issue, and I would be happy to answer any questions you might have.