Testimony of Charter Communications, Inc.

SB 4: An Act Concerning Data Privacy, Net Neutrality, Cyber Security and Fairness in Data Usage in the New Age of a Digital Workforce

March 9, 2021

Good morning Chairs Needleman and Arconti, Vice Chairs Winfield and Allie-Brennan, Ranking Members Formica and Ferraro and Members of the Energy & Technology Committee. My name is Michael A. Chowaniec, Vice President of Government Affairs for Charter Communications. Charter appreciates the opportunity to submit written testimony today on SB 4, An Act Concerning Data Privacy, Net Neutrality, Cyber Security and Fairness in Data Usage in the New Age of a Digital Workforce.

Charter values and relies on the trust and loyalty of its more than 31 million residential and business customers. Our network provides competitively priced high-speed broadband, video, voice and mobile 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.

Ensuring that the privacy of our customers is protected is very important to us and Charter appreciates the Committee holding this hearing to focus on these issues. We also appreciate the developing dialogue among businesses and 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

As you know, continuing advances in technology are changing the online privacy landscape. Despite Americans' daily reliance on websites, apps and social media, it can be difficult for consumers to understand and appreciate how companies are collecting, analyzing, using and selling information about them.

An increasingly critical aspect of ensuring that consumers will continue to use our services and the multitude of offerings on the internet is making sure they have confidence that their online personal information is protected. While Charter strives to give our customers confidence with our current policies and practices, we recognize that there is still more to do.

As our Chairman and 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 consumers since it threatens the internet's future as an engine of economic growth. That is why he has called for the creation of a new comprehensive federal privacy framework based on opt-in consent to

give consumers better tools to control their information online. Importantly, for such a framework to be effective it must be applied consistently across the entire internet ecosystem. 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 device.

This is why an ISP-specific privacy bill like Senate bill 4 is the wrong approach. Applying one set of laws to data-handling by ISPs and another set of laws to handling the exact same data by a search engine or a social media site is a recipe for consumer confusion and could, in fact, lead consumers to exercise less care over their data disclosures. Should this bill become law, Connecticut residents could be more willing to share data with all manner of online services on the mistaken belief that state law protects against the collection and use of customer data by all Internet services.

Furthermore, there is nothing unique about ISP access to consumer data such that ISPs should be singled out for special privacy laws. As shown in a study by Professor Peter Swire, "ISPs have neither comprehensive nor unique access to information about users' online activity" and "non-ISPs often have access to more and a wider range of user information than ISPs."[1] The study shows that as consumers access the Internet over multiple devices, on multiple networks in and outside the home, and continue to increase their use of encryption and virtual private networks, ISPs' ability to collect consumer data has been decreasing. At the same time, as users log into and visit the same websites regardless of the device or network, those websites' ability to track and collect data on consumers has increased.

As Charter has expressed in testimony before the United States Congress and in state houses across the country, a comprehensive privacy framework should seek to empower and inform consumers through rules based on five core principles – control, transparency, uniformity, parity and security. We believe a federal solution would best accomplish these objectives by ensuring consumers are protected by a nationally consistent framework across the online ecosystem regardless of where they live or work.

We recognize that several states, not only Connecticut, are seriously considering enacting their own state-level privacy regimes. A few, like California, Nevada, and Virginia have already passed legislation to do so. As you consider this legislation, we respectfully urge you to approach it from a similar place we do – based on the principles of parity, transparency and consumer control. Such an approach enables consumers to decide how their data is used, allows companies to innovate, and places the same responsibilities to protect consumer data on all companies.

Five Principles for Protecting Consumers Online
These are the five core principles that are critical to an effective privacy framework.

The first principle is control. Consumers should be empowered to have meaningful choice regarding the collection and use of their data. The best way to ensure consumer

[1] Peter Swire, Justin Hemmings, and Alana Kirkland, *Online Privacy and ISPs* (2016), available at https://iisp.gatech.edu/working-paper-online-privacy-and-isps.

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. Additionally, consent should be renewed with reasonable frequency and any use of personal data should be reasonably limited to what the consumer understood at the time consent was provided.

The second principle is transparency. Consumers should be given the information they need to provide informed consent. Explanations about how companies collect, use and maintain consumers' data should be clear, concise, easy-to-understand and readily available. Privacy policies also should be separate from other terms and conditions of service. If all online companies provide this type of transparency, consumers will have a greater ability to weigh the potential benefits and harms of the collection and use of their personal data.

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 what type of service is being offered. Consumer data should be protected equally 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.

The fourth principle is uniformity. For online consumer protections to be effective there should be a single national standard. A patchwork of state laws would be confusing for consumers, difficult for businesses to implement, and hinder continued innovation. Yet, Charter realizes that in the absence of a uniform, federal solution, states may be likely to act on their own. In doing so, it will be critical that the states understand what each of the others is doing so as to avoid an inconsistent or worse, contradictory, set of online protections. A system filled with inconsistency or contradictions will not serve consumers, and will stifle technological innovation.

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 also believe that agency enforcement is the appropriate mechanism to ensure online data privacy. Agencies of the state, who have individuals who are subject matter experts, and who know how to investigate and implement existing rules, laws and regulations, offer the most cost-effective manner to enforce online privacy laws. Instituting a private right of action benefits the plaintiff's bar more than consumers and does not actually result in the implementation or development of new or revised safeguards for data. Costly litigation creates greater uncertainty and may have the effect of stifling technological developments and service improvements.

Conclusion

We are now engaged in 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 wherever they go online.

Charter supports a comprehensive privacy approach. ISP-only privacy regimes are the wrong approach and do not reflect the direction of other states that are considering addressing consumer privacy. Connecticut residents deserve better than a non-comprehensive approach to protecting consumer privacy that applies to a limited amount of data collected and used by only ISPs.

We thank the Members of the Committee for the opportunity to submit written testimony, and look forward to continuing to work with you as you consider the right privacy regime to protect personal data for consumers in Connecticut.