



**Testimony of
Gerry Keegan
CTIA
In Opposition to Connecticut Senate Bill 335**

Before the Connecticut Joint Committee on Energy and Technology

March 8, 2018

Chairs, Vice Chairs, and members of the committee, on behalf of CTIA, the trade association for the wireless communications industry, I am here to testify in opposition to Connecticut Senate Bill 335, which would restrict how internet service providers (ISPs) operate in Connecticut.

First and foremost, it is important to note that there is no gap in privacy protections that must be filled at the state level. The 2017 Congressional action did not change privacy protections for consumers. The Federal Communications Commission (FCC) rules had not taken effect, so the 2017 CRA changed nothing from the regulatory framework that has existed since 2015.

The FCC's recently adopted *Restoring Internet Freedom Order* means that the Federal Trade Commission (FTC) will reassert its well-established oversight and enforcement authority over ISP consumer privacy practices.¹ Over 20 years, the FTC has developed and enforced an effective privacy framework that applies to all players in the internet ecosystem. Restoring FTC jurisdiction subjects ISPs to the same, effective regulatory framework that applies to the rest of the internet ecosystem. It is also consistent with the framework advocated for by the Obama Administration, which noted

¹ See FCC Restoring Internet Freedom Report & Order ¶ 194 (adopted Dec. 14, 2017; issued Jan. 4, 2018), http://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0104/FCC-17-166A1.pdf.



that, “uniform consumer data privacy rules are necessary to create certainty for companies and consistent protections for consumers.”² This legislation deviates from the privacy framework and standards that have been in place for decades and imposes unjustified restrictions on ISPs alone. Even during the brief period of time during which the FCC, and not the FTC, asserted jurisdiction over ISPs, consumers’ privacy remained protected. The FCC’s statutory authority applied, and ISPs including CTIA members, committed to principles that maintained privacy protections consistent with the FTC’s effective privacy framework, covering transparency, consumer choice, security, and data breach notifications.³

Second, any suggestions that ISPs, including CTIA members, have unique access to consumer data online are unfounded. A comprehensive study by veteran Clinton and Obama Administration privacy expert Peter Swire showed that ISPs actually have limited insight into the online activity of consumers.⁴ SB 335 unnecessarily targets one set of providers - ISPs - and treats them differently than others operating in the internet ecosystem.

By creating two sets of rules that are different for various entities within the internet ecosystem, SB 335 would harm competition and create consumer uncertainty about

² “Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy,” <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1096&context=jpc>, last accessed 3/7/2018.

³ “Protecting Consumer Privacy Online,” <http://www.ctia.org/docs/default-source/default-document-library/final--protecting-consumer-privacy-online.pdf>, last accessed 3/7/2018.

⁴ “Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others,” http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf, Swire, Peter, last accessed 2/9/2018: “ISP access to user data is not comprehensive – technological developments place substantial limits on ISPs’ visibility. [And] ISP access to user data is not unique – other companies often have access to more information and a wider range of user information than ISPs.”



which rules apply to their data. Survey results submitted to the FCC last year showed that 94 percent of internet users believe all companies touching their online data should follow the same privacy rules.⁵ These findings indicate that SB 335, which targets only ISPs, would in fact be a contravention to what consumers actually want. The bill's prohibition of the transfer of a broad set of personally identifiable information without express consent would also make it very difficult – if not impossible - for ISPs to operate in Connecticut and could have a host of unintended consequences.

Additionally, in recognition that the internet is not defined by state lines, the recent FCC order includes preemption language to avoid a patchwork of state laws regulating internet service. The FCC has recognized that “broadband Internet access service should be governed by a uniform set of federal regulations, rather than by a patchwork of separate state and local requirements.” Conflicting state rules could hamper the provision of broadband service, lead to increase compliance costs, and inhibit providing new and innovative products and services – all to the detriment of consumers.

The wireless industry takes a proactive approach to protect consumer privacy. Our members provide consumers with detailed privacy policies, which clearly describe how providers protect consumer data. Current federal and state statutes also provide additional layers of protection for sensitive consumer information.

⁵ The Progressive Policy Institute, “Consumers Want One Set of Rules Protecting Their Information,” <http://www.progressivepolicy.org/press/press-releases/press-release-consumers-want-one-set-rules-protecting-information/>, last accessed 3/7/2018.



CTIA member companies have long recognized the importance of protecting consumer data and respecting consumer privacy. In 2003, CTIA and the wireless carriers that are signatories to the "Consumer Code for Wireless Service," including AT&T, Sprint, T-Mobile, and Verizon Wireless, made a commitment to help consumers make informed choices.⁶ The tenth point of the Code provides that signatory carriers agree to abide by policies for the protection of customer privacy. As part of that commitment, carriers follow policies regarding the privacy of customer information in accordance with applicable federal and state laws and make available privacy policies concerning information collected online. The wireless industry recognizes the importance of customer privacy and takes strong measures to protect customer data.

Finally, no state has passed a bill on ISP privacy, despite the introduction of such bills in over 20 states in 2017, because states increasingly recognize the unintended consequences and negative repercussions that could result from legislation of this kind. In October of last year, this legislature mandated the creation of a working group to examine ISP privacy. The working group has not yet been convened, and the report that this legislature commissioned has never been produced and added to the record. Given that this legislature decided that it needed more information on this subject and that that information has not yet been received, it is premature to legislate in this area.

In closing, CTIA members are absolutely committed to protecting consumer information as they value consumer trust. Existing federal and state laws and protections

⁶ CTIA Consumer Code for Wireless Service, <http://www.ctia.org/initiatives/voluntary-guidelines/consumer-code-for-wireless-service>, last accessed 3/7/2018.



remain intact today rendering SB 335 unnecessary. Moreover, CTIA members have committed to a framework to protect consumer information and privacy. For these reasons, we respectfully ask that you not move SB 335.