Testimony of
GERARD KEEGAN
CTIA

In Opposition to Connecticut Senate Bill 4

Before the
Connecticut Joint Committee on Energy and Technology

March 9, 2021

Co-Chairs, Vice-Chairs, and members of the committee, on behalf of CTIA®, the trade association for the wireless communications industry, I testify in opposition to Sections 1, 2, and 4 of Senate Bill 4.

CTIA and its member companies support an open internet. To further that goal, we support a bipartisan federal legislative solution to enshrine open internet principles to resolve this issue once and for all and provide certainty for U.S. consumers and broadband providers. CTIA, however, respectfully opposes piecemeal state regulation of the borderless internet and mobile wireless broadband - a truly interstate service - like this legislation. The Federal Communications Commission (FCC) will likely address the issue of net neutrality in the near term. Thus, CTIA urges the Connecticut General Assembly to refrain from taking action on this legislation. In addition, the Federal Trade Commission (FTC) has reasserted its well-established oversight and enforcement authority over Internet Service Provider (ISP) consumer privacy practices making state ISP privacy laws unnecessary.

On Section 1, the mobile wireless broadband marketplace is highly competitive and has been an engine of continual innovation, attracting billions of dollars in network investment each year. From the beginning of the Internet Age in the 1990s through the start of the 21st century, the FCC, acting on a bipartisan basis, carefully and purposefully applied a national regulatory framework to internet service

that allowed providers to invest, experiment, and innovate while maintaining an open internet. In that time, an entire internet-based economy grew at unprecedented levels. But in 2015, the FCC dramatically changed course, applying for the first time ill-fitting and misplaced 80-year-old common-carrier mandates meant for traditional monopoly public utilities, such as landline phone service, to broadband internet access.

In 2018, the FCC restored the same national regulatory framework that applied before 2015, which is credited with facilitating the internet-based economy we have today. Under that framework, mobile wireless broadband providers have every incentive to invest in and deliver the open internet services that consumers demand.

The FCC's *Restoring Internet Freedom* Order reversed its 2015 decision, finding that application of 1930s utility-style rules to the internet services of today actually harmed American consumers. The FCC cited extensive evidence showing a decline in broadband infrastructure investment – an unprecedented occurrence during an era of economic expansion. In the mobile broadband market alone, annual capital expenditures fell from $32.1 billion in 2014 to $26.4 billion in 2016. This slowdown affected mobile providers of all sizes and serving all markets. For example, small rural wireless providers noted that the 2015 decision burdened them with unnecessary and costly obligations and inhibited their ability to build and operate networks in rural America.

Under the 2018 Order, consumers continue to have legal protections that complement the competitive forces in play. First, the FCC's current regulations include rigorous "transparency" rules that were adopted under President Obama's first FCC Chairman in 2010 and maintained in the 2018 decision, which require broadband providers to publicly disclose extensive information to consumers

and internet entrepreneurs about their service performance, commercial terms of service, and network management practices. Second, consistent with the FCC's pre-2015 framework, and unlike with the 2015 decision, the FTC once again has ample authority to police broadband offerings and has publicly committed to engage in active enforcement. This extends to any unfair and deceptive practices, including but not limited to, any violation of the transparency rules and ISP public commitments. The FTC also has authority to act against anticompetitive ISP practices. The FCC's 2015 Order actually removed the FTC from its longstanding enforcement role. Moreover, the U.S. Department of Justice enforces federal antitrust laws, which preclude anticompetitive network management practices.

The FCC made clear in its 2018 Order that generally applicable state laws relating to fraud, taxation, and general commercial dealings apply to broadband providers just as they would to any other entity doing business in a state, so long as such laws do not regulate broadband providers in a way that conflicts with the national regulatory framework for broadband internet access services.

Any attempt to apply multiple states' requirements would be harmful to consumers for the same reasons the FCC's 2015 rules were harmful, in addition to the fact that those requirements will be at best different and at worst contradictory. Problems multiply in the case of mobile broadband: questions will arise over whether a mobile wireless broadband transmission is subject to the laws of the state where users purchased service, where they are presently located, or even where the antenna transmitting the signal is located. State-by-state regulation even raises the prospect that different laws will apply as the user moves between states. For example, a mobile broadband user could travel through multiple states during a long train ride, even the morning commute, subjecting that rider's service to multiple different legal regimes even if the rider spent that trip watching a single movie. Such

a patchwork quilt of disparate regulation is untenable for the future success of the internet economy. In the mobile environment, state-by-state rules would be especially burdensome, difficult to comply with, costly, and subject providers to differing state interpretations and enforcement of facially similar net neutrality requirements – creating further business uncertainty.

The internet does not stop at state boundaries. Consumers regularly access content from across the country and around the world making virtually all internet traffic interstate and making it impossible to make distinctions between that interstate traffic and the limited amount of internet traffic that begins and ends in a single state. The FCC's 2018 order barring common carrier regulation of broadband internet access service, including mobile broadband service, was affirmed in October 2019 by the federal Court of Appeals for the D.C. Circuit. And, although it rejected the FCC's blanket express preemption of all state laws affecting intrastate broadband internet access, the court expressly affirmed the FCC's authority to preempt on a case-by-case basis any state law that "undermines the 2018 Order," as well as the availability of conflict preemption in the courts. Indeed, courts have long recognized that interstate communications services are subject to the exclusive authority of the FCC.

On Section 2, with the FCC's *Restoring Internet Freedom* Order in effect, the FTC once again has authority over ISP consumer privacy practices. For over 20 years, the FTC has developed and enforced an effective privacy framework that applies to all players in the internet ecosystem. The FTC is an active consumer privacy enforcer. It has brought over 500 enforcement actions protecting consumer privacy. Through these enforcement actions, as well as through extensive policy guidance, the FTC has articulated a consumer privacy framework in which more sensitive personal information (e.g., biometric or genetic information, children's information, and health information) is generally subject to

heightened protections, while there is greater flexibility to collect, use, and disclose non-sensitive information. In addition, the Connecticut Attorney General already has the authority to address unfair or deceptive acts or practices relating to consumer privacy under state consumer protection laws. Because of these existing federal and state measures, and other privacy laws, there is no gap in ISP customers' privacy protections that Connecticut needs to fill.

SB 4 would create two sets of rules that are different for various entities within the internet ecosystem. This would lead to widespread consumer confusion about which rules apply to their data and work to create an uneven playing field. Internet users overwhelmingly prefer a single national standard. Survey results submitted to the FCC showed that 94 percent of internet users believe all companies touching their online data should follow the same privacy rules. These findings indicate that state legislation, like SB 4, targeting ISPs would in fact be inconsistent with what consumers actually want.

In addition, ISPs do not have unique access to consumer data. A study by noted privacy expert Peter Swire found that ISP access to consumer data is not comprehensive, that technological developments place substantial limits on ISP visibility, and ISP access to user data is not unique – other companies may have access to more information and a wider range of user information. Furthermore, consumers no longer use a single stationary device. Today consumers use many connected devices serviced by multiple ISPs.

Moreover, research indicates that more than 80 percent of web traffic is encrypted, and that number continues to grow. Google estimates, for example, that 95 percent of traffic across Google products and services is encrypted. When a website is encrypted, an ISP does not know what a user

views on that site. Additionally, a growing number of consumers use virtual private networks that block ISPs from even seeing the domain name that a user is visiting. There cannot be comprehensive ISP visibility when ISPs are prevented from seeing user activity.

Uniform federal policies work best. CTIA and its members support efforts to address the growing challenges to consumers' privacy. In particular, CTIA supports federal legislation that establishes uniform, technology-neutral consumer privacy protections. Such legislation is the only way to ensure clearer, more specific, and nationally consistent privacy protections for consumers and certainty for businesses.

SB 4 would not produce any of the benefits of a uniform federal approach. To the contrary, it would create a highly restrictive technology-specific privacy regime. This legislation would require ISPs (but not other entities) to obtain "express and affirmative permission" from consumers to sell or transfer consumers' personal identifying information. Such a sweeping and inflexible opt-in requirement is at odds with nearly every other U.S. consumer privacy law and framework. As a result, this bill would change how Connecticut consumers access information on the internet causing consumer confusion by creating different levels of privacy protections based on the type of entity that handles their personal information, something consumers would not expect.

Maine passed an ISP-only privacy law in 2019. CTIA, along with other associations representing broadband providers, filed a lawsuit in the U.S. District Court of Maine. Maine's decision to impose unique burdens on ISPs' speech — while ignoring the online and offline businesses that have and use the very same information and for the same purposes as ISPs — represents discrimination between similarly situated speakers that is impermissible under the First Amendment.

In addition, the Maine law is preempted by federal law because it directly conflicts with federal determinations about the proper way to protect consumer privacy. Among other things, the law conflicts with the FCC's decision that a combination of disclosure, competition, and FTC oversight — not prescriptive ISP-specific rules — best balances the federal policies of promoting broadband and protecting consumer privacy.

Finally, on Section 4, wireless providers already provide appropriate explanations on consumer bills related to consumer charges and make appropriate disclosures about data caps. CTIA opposes this section as the priority for industry, policymakers, and all stakeholders should be removing barriers to mobile broadband deployment and adoption and not enacting this type of provision that is unnecessary in light of what mobile providers already disclose to consumers.

The internet is inherently interstate – and even international. State-by-state legislation is both unworkable and could harm the vibrant ecosystem existing today. We must work together to ensure investment continues while protecting the flow of information consumers expect. Thus, we support federal legislation to ensure there is a uniform national framework for the open internet and consumer privacy. We welcome Connecticut calling on Congress to resolve these issues at the federal level but must oppose state-by-state legislation. Further, the FCC will likely take action on net neutrality in the near term. Connecticut should not add to any further conflict and confusion by passing this bill. Accordingly, I respectfully urge you not to move this legislation.