Testimony of
GERARD KEEGAN
CTIA

In Opposition to Connecticut Senate Bill 6

Before the Connecticut Joint Committee on Energy and Technology

February 19, 2019

Chairs, Vice Chairs, and members of the committee, on behalf of CTIA, the trade association for the wireless communications industry, I am here in opposition to Senate Bill 6. CTIA and its member companies support an open internet. We support a federal legislative solution to enshrine open internet principles and to enact a uniform and comprehensive privacy framework for the United States. In addition, the Federal Trade Commission (FTC) has reasserted its well-established oversight and enforcement authority over internet service provider (ISP) broadband services and consumer privacy practices making net neutrality and state ISP privacy legislation unworkable and unnecessary.

State Net Neutrality Legislation is Unnecessary

The mobile wireless broadband marketplace is competitive and continuously changing. It is an engine of innovation, attracting billions of dollars in network investment each year, and generating intense competition to the benefit of consumers. From the beginning of the Internet Age in the 1990s, the Federal Communications Commission (FCC) applied a regulatory framework to internet service that allowed providers to invest, experiment, and innovate. In that time, an entire internet-based economy grew. But in 2015, the FCC took a much different approach, applying 80-year-old common-carrier mandates meant for traditional monopoly public utilities, despite the fact that internet

services are nothing like public utility offerings such as water or electricity or even landline telephone service.

In 2017, the FCC's *Restoring Internet Freedom Order* reversed that 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.

The FCC's overbroad prohibitions on broadband providers harmed consumers in other ways, too—particularly with respect to innovation. For example, after the 2015 Order, the FCC launched a yearlong investigation of wireless providers' free data offerings, which allow subscribers to consume more data without incurring additional costs. The risk of FCC enforcement and its vague "general conduct" standard cast a shadow on mobile carriers' ability to innovate, compete and deliver compelling and valuable services that consumers demanded. In addition, the inflexible ban on paid prioritization precluded broadband providers from offering one level of service quality to highly sensitive real-time medical applications and a differentiated quality of service to email messages. The FCC's 2017 *Restoring Internet Freedom Order* took a different path –

one that benefits consumers and enables new offerings that support untold varieties of technological innovations in health care, commerce, education, and entertainment.

Based on the way some people have talked about the *Restoring Internet Freedom Order*, you might think the FCC eliminated federal rules that had always applied to internet services and that the federal government left consumers without any protections. But that is just not the case. The internet was not broken before 2015, and the internet as we knew it did not end because of the FCC's 2017 decision.

With its action in 2017, 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 national regulatory framework, mobile wireless broadband providers have every incentive to invest in and deliver the internet services that consumers demand. The truth is that, in a competitive market like wireless, mobile broadband providers have no incentive to block, degrade, or impair access to lawful internet services, and if they did, their customers would simply switch providers.

Under the current – and pre-2015 – regulatory landscape, consumers continue to have legal protections that complement the rigorous competitive forces in play in the internet marketplace. First, the FCC's current regulations include a "transparency" rule that was adopted under President Obama's first FCC Chairman in 2010 and maintained in the 2017 decision, which requires broadband providers to publicly disclose extensive information about their performance, commercial terms of service, and network management practices to consumers and internet entrepreneurs. Second, consistent with the FCC's pre-2015 framework, the FTC once again has ample authority to police

broadband offerings in applicable cases 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.

Third, the U.S. Department of Justice enforces federal antitrust laws, which preclude anticompetitive network management practices. Finally, the FCC made clear in its 2017 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. The 2017 Order reaffirmed the FCC's 2015 decision that states and localities may not impose requirements that conflict with federal law or policy, but may otherwise enforce generally applicable laws. Thus, Connecticut remains empowered to act under its Unfair and Deceptive Acts and Practices law.

In short, Connecticut consumers are well protected against anti-competitive or anti-consumer practices. They enjoy protections provided by the FCC, the FTC, federal antitrust law, and – importantly – existing Connecticut state law. On the other hand, state-specific net neutrality rules imposed on broadband providers would harm consumers, and would – along with other state and local mandates – create a complex "patchwork quilt" of requirements that would be unlawful.

In its 2017 *Restoring Internet Freedom Order*, the FCC explained that broadband internet access is an inherently interstate and global offering. Internet communications delivered through broadband services almost invariably cross state lines, and users pull content from around the country and around the world – often from multiple jurisdictions in one internet session. Any attempt to apply multiple states' requirements would therefore 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.

These 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 net neutrality requirements to differing state interpretations and enforcement – creating further business uncertainty.

In its 2017 Order, the FCC explained that broadband internet access is inherently interstate and global and found broadband-specific state laws are unlawful and

preempted by federal law. The FCC recognized that state or local laws that impose net neutrality mandates or that interfere with the federal preference for national regulation of broadband internet access are impermissible. This is nothing new: even in its 2015 Order, the FCC had concluded that contrary state laws governing broadband internet access are preempted.

Several states have nonetheless adopted net neutrality laws and regulations, but the futility of doing so is becoming clear. California enacted a net neutrality law that was challenged in court by the U.S. Department of Justice and a group representing broadband providers, including CTIA. Before even a hearing on the law, the California Attorney General stipulated to non-enforcement of the law pending judicial review of the 2017 Order.

Likewise, when a net neutrality bill was proposed in the Vermont legislature, that state's own Public Service Department issued a memo in which it "strongly caution[ed]" that the legislation "would likely run afoul of" the FCC's rules and warned that "a federal court is likely to be highly skeptical [of] and disinclined to uphold any law that directly or indirectly seeks to legislate or regulate net-neutrality." The law was nevertheless enacted, and is now facing its own court challenge.

Ultimately, we believe that Congress should act to bring certainty and provide reasonable uniform net neutrality protections for all users. For this reason, CTIA has called on Congress to enact bipartisan legislation for the internet ecosystem that promotes an open internet while also enabling the consumer-friendly innovation and investment we need for tomorrow.

Finally, it is worth noting that this is the second time that the FCC has issued a de-regulatory classification of broadband. When the first such order reached the Supreme Court, the Court expressly upheld the FCC's authority in this regard in the Brand X case. According to the Supreme Court:

> "The questions the Commission resolved in the order under review involve a 'subject matter [that] is technical, complex, and dynamic.' . . . The Commission is in a far better position to address these questions than we are. Nothing in the Communications Act or the Administrative Procedure Act makes unlawful the Commission's use of its expert policy judgment to resolve these difficult questions."

No Gap in ISP Privacy Regulations

From the outset, 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 FCC rules had not taken effect, so the 2017 Congressional Review Act changed nothing from the privacy framework that previously existed. State-specific ISP privacy legislation deviates from that framework and imposes unjustified restrictions on ISPs.

Now that the FCC's *Restoring Internet Freedom Order* is in effect, the FTC has reasserted its well-established oversight and enforcement 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. 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 that, "uniform consumer data privacy rules are necessary to create certainty for companies and consistent protections for consumers."

The FTC is an active consumer privacy enforcer. It has brought over 500 enforcement actions protecting consumer privacy. Most recently, the FTC, with 32 state attorneys general, brought an action against a large computer manufacturer alleging that it "preinstalled software that interfered with how a user's browser interacted with websites." The Commission also brought charges against a ride sharing company alleging that it failed to "live up to its claims that it closely monitored employee access to consumer and driver data." These are just two examples of more recent FTC privacy enforcement actions. A more recent 9th Circuit U.S. Court of Appeals decision affirmed the FTC's enforcement authority over non-common carrier activities and its ability to enforce its privacy framework against all internet companies, including ISPs. State attorneys general can also bring enforcement actions against ISPs that violate state statutes such as unfair trade practices prohibitions.

If a state adopts ISP privacy legislation, it would create two sets of rules that are different for various entities within the internet ecosystem, would harm competition, and would create consumer uncertainty about which rules apply to their data. Survey results submitted to the FCC in 2016 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 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 former Clinton and Obama Administration 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 have access to more information and a wider range of user information. Consumers no longer use a single stationary device. Today consumers use many connected devices serviced by multiple ISPs. More than 50 percent of web traffic is also encrypted and that number continues to grow. Google estimates, for example, that 90 percent of traffic over Chrome is encrypted. 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.

In recognition that the internet is not defined by state lines, the 2017 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. Finally, no state has passed a bill on ISP privacy, despite the introduction of such bills in over 20 states, because states increasingly recognize the unintended consequences and negative repercussions that could result from legislation of this kind.

CTIA and its members also support the adoption of a federal law that establishes a comprehensive and uniform framework for consumer privacy. The private sector has been united in calling for a nationally unified approach. Federal legislation is the only way to achieve a uniform approach to privacy.

In closing, it is unnecessary to pass state net neutrality and ISP privacy legislation due to the strong consumer protections currently in place and because states are preempted in this area. Additionally, state-by-state laws would be especially burdensome, difficult to comply with, costly, and subject broadband providers to differing state interpretations and enforcement – creating further business uncertainty. Accordingly, we respectfully ask that you not move SB 6.