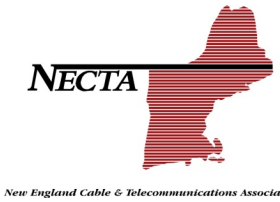


*New England Cable & Telecommunications Association, Inc.*
*Ten Forbes Road ● Suite 440W ● Braintree, MA 02184*
*TEL: 781.843.3418 ● FAX: 781.849.6267*

**STATEMENT OF THE NEW ENGLAND CABLE & TELECOMMUNICATIONS ASSOCIATION, INC. IN OPPOSITION TO SENATE BILL 6 AN ACT CONCERNING NET NEUTRALITY PRINCIPLES AND INTERNET PRIVACY.**

**February 19, 2019**

Good morning, Chairs Needleman and Arconti, Vice Chairs Fonfara and Allie-Brennan, Ranking Members Formica and Ferraro, and esteemed Members of the Energy & Technology Committee. My name is Tim Wilkerson, and I am Vice President and General Counsel for the New England Cable and Telecommunications Association ("NECTA").

**I. Introduction**

NECTA is a five-state regional trade association representing substantially all private cable telecommunications companies in Connecticut, Massachusetts, New Hampshire, Rhode Island, and Vermont. All NECTA cable members have a physical presence in Connecticut, including two Fortune® 100 companies, Charter Communications, which is headquartered in Stamford, and Comcast with a Regional New England headquarters in Berlin and a subsidiary, NBC Sports, headquartered in Stamford, as well as privately held Cox Communications and Atlantic Broadband. NECTA's cable members have collectively invested $2 billion over the past seven years developing state of the art networks in Connecticut, and in 2019, the cable industry expects to employing over six thousand Connecticut residents.

I appreciate the opportunity to testify on SB6 and detail our members' concerns with this legislation. In short, there will be serious unintended consequences if this legislation passes; it is unworkable and would be devastating to the Internet economy in Connecticut and beyond. In the case of both net neutrality and privacy, federal bi-partisan legislation is the right way forward.

**II. Connecticut's Vibrant and Competitive Internet Ecosystem and the Disruptive Risks and Unintended Consequences of State Regulation of Internet Service Providers**

Over the past decade, NECTA members' maximum Internet speeds have increased dramatically. Residential Internet speeds, delivered through approximately thousands of miles of fiber networks, reach speeds of up to two Gigabits. For business services, NECTA members provide top Internet speeds that any retailer, university research and development facility, financial services company, or hospital could demand. Importantly, Connecticut cable providers have actively deployed what is known as DOCSIS 3.1 technology to provide even faster, more reliable data speeds and features (DOCSIS 3.1 can deliver 1 to 10 gigabit speed levels). This investment

is reflected in Connecticut's impressive broadband performance, in Ookla's recent *2018 Speedtest Fixed U.S. Broadband Performance Report* the state's mean download speed was 93.68 Mbps in excess of the national average. Because of the predictable regulatory environment and Internet Service Providers ("ISPs") multi-billion-dollar investments in the state's broadband infrastructure, Connecticut's overall innovation ecosystem— life sciences, aerospace, advanced precision manufacturing, and beyond— is world class. `

Today NECTA members' advanced networks and operating systems have the capacity to not only meet but exceed consumer demand. Our members' network superiority is highlighted by the most recent *Netflix ISP Speed Index* ranking Comcast as one of the top two ISPs for prime-time Netflix performance in the world. As ISPs' product offerings evolve to increasingly include mobile services, Internet of Things ("IoT") products, telehealth options, and other transformative business lines, the consumer experience is becoming hyper personal. These innovations have been powered by the delivery of broadband services under predictable and national and state regulatory schemes. By enacting legislation like SB6 the Connecticut legislature will disrupt two decades of regulatory certainty and contribute to the creation of a disjointed patchwork of inconsistent state Internet laws. Policing the Internet on a state-by-state basis is fraught with risk, costly to both state governments, consumers, and the private sector.

**III. Existing State and Federal Oversight and Enforcement**

Today, the Federal Trade Commission ("FTC"), the FCC, the United States Justice Department ("DOJ"), and the State Attorneys General have well established authority to protect consumers and preserve the open Internet and protect consumer privacy. At the state level, Attorneys General can sue ISPs who engage in unfair or deceptive trade practices under existing state consumer protection laws.

To ensure an open Internet and protect consumer privacy, the FTC is once again the principle agency with regulatory oversight over ISPs. The FCC's 2017 *Restoring Internet Freedom Order* ("*RIF Order")* returned online consumer protection authority to the FTC, the "top federal cop on the beat" for the past twenty years. The FTC has a long history of vigorously pursuing investigations and enforcement actions against any company in the online environment for unfair, deceptive, and anticompetitive practices. Additionally, the FCC, in coordination with the FTC, continues to require ISPs to publicly disclose information about their practices to consumers. Finally, the DOJ can enforce antitrust laws if ISPs act in an anticompetitive manner or illegally reach agreements that unfairly interfere with the lawful online content or conduct of consumers or companies.

**IV. NECTA Members Ongoing Commitment to Net Neutrality Principles**

NECTA members do not block, throttle, or otherwise interfere with the lawful online activity of our customers and have consistently agreed to these commitments since the Federal Communications Commission ("FCC") first issued them in the Transparency Rule as part of the 2010 *Open Internet Order*. It is important to underscore that these commitments are more than a mere pledge. They have been an ongoing part of our companies' operating DNA.

With the FCC memorializing the Transparency Rule in its *Restoring Internet Freedom Order* ("*RIF Order*"), ISPs' network management practices and performance and commercial terms of service are now legally enforceable by state and federal agencies. NECTA members' disclosures are robust, clear commitments to their customers to uphold an open Internet.

**V. Federal Law Preempts State Attempts to Impose Net Neutrality Requirements Through Conditions on State Procurement of Contracts or Similar Measures**

The *RIF Order* removed the overhang and uncertainty of Title II regulation and reinstated the light-touch regulatory framework that promoted substantial broadband investment, innovation, and deployment for nearly two decades. This will unleash new investment and innovation and enable us to provide our customers even better Internet service in the years to come, all while ensuring that our customers and all stakeholders are fully informed of our open Internet policies and practices.

From its inception, the Internet grew and thrived due to a light touch regulatory environment that was outlined in the bi-partisan 1996 Telecommunications Act (enacted by a Republican Congress and signed by President Bill Clinton), which treated broadband as an "information service." During this period, the Federal Trade Commission was the cop on the beat, overseeing ISPs and non-IPs alike, ensuring that consumers were well protected. In 2015, the FCC made a dramatic departure from this longstanding, successful approach when it reclassified Internet service from an "information service" to a Title II common-carrier telecommunications service, and imposed burdensome 1930s-era utility-style regulations (originally designed for old-fashioned telephone service), through its "*Title II Order*."

The *RIF Order* contains several important elements: it restores the Federal Trade Commission as the cop on the beat for the entire Internet ecosystem; it imposes enhanced transparency requirements on ISPs, which must publicly disclose information regarding their network management practices, performance, and commercial terms of service; and it broadly preempts state and local governments from imposing separate net neutrality requirements. Such state and local conditions could impair the Internet ecosystem by requiring ISPs to comply with a patchwork of likely conflicting requirements across different jurisdictions.

Some advocates will claim that state net neutrality measures are not subject to federal preemption. They are wrong. Under the Hobbs Act, states (and any federal or state trial courts that adjudicate the validity of state net neutrality bills or executive orders) are legally bound by the FCC's preemption analysis in the *RIF Order*. Only the D.C. Circuit can review the validity of the FCC's preemption in the appeal of the *RIF Order*, and that preemption analysis is highly likely to be upheld.

Also inconvenient for those promoting state-level net neutrality laws to restore the 2015 Open Internet Order are several paragraphs in that very order in which the FCC "reaffirm[s] the Commission's longstanding conclusion that broadband Internet access service is jurisdictionally interstate for regulatory purposes." And that the FCC "announce[s] our firm intention to exercise our preemption authority to preclude states from imposing obligations on broadband service that

are inconsistent with the carefully tailored regulatory scheme we adopt in this Order." Yes, the Open Internet Order *also* broadly preempted the states.

**VI. Net Neutrality Litigation**

The *2017 Restoring Internet Freedom Order* was challenged in the D.C. Circuit Court of Appeals by multiple state attorneys general, consumer groups, and other interests. Oral arguments were held just a few weeks ago on February 1, 2019. Over the course of 2018, four states passed net neutrality legislation (California, Oregon, Vermont, Washington) and six governors issued executive orders instituting net neutrality requirements in state procurement (Hawaii, Montana, New Jersey, New York, Rhode Island, Vermont).

There is now litigation in two states over these state-enacted laws – California and Vermont. Within hours of California Governor Jerry Brown signing SB822, the United States Department of Justice sued to block the law, arguing that it is invalid under both conflicting federal law and the United States Constitution. A broad set of industry participants filed amicus briefs in the case as well. Industry has also filed a suit to stop Vermont from enforcing its net neutrality law and executive order, and that process is ongoing.

Not long after the California suit was filed, California Attorney General Xavier Becerra entered into an agreement to suspend any enforcement of California's net neutrality law and to not litigate the US DOJ suit, acknowledging that until the DC Circuit Court (and likely then the United States Supreme Court) decided whether the FCC had the authority to preempt states from passing separate and conflicting laws, the State of California had no legal ability to defend its law. AG Becerra recognized this in his agreement with the US DOJ to stay any enforcement of CA's recently-passed net neutrality law until the underlying appeal of the *RIF Order* is resolved; he acknowledged that if the order is upheld, CA will necessarily fail in its effort to set state-level net neutrality regulations.

Adoption of a Connecticut net neutrality law at this moment is premature. With three lawsuits over the viability of such laws pending and before any state has attempted to enforce its own laws due to that litigation, Connecticut's taxpayers are best served by waiting until those lawsuits are resolved before moving forward.

**VII. State-level privacy laws could harm legitimate and desirable business activities.**

We recognize and appreciate the concerns that policymakers have regarding privacy and understand the desire to seek legislation which is broad in its scope. We caution the committee that despite the bill's specific application to ISPs, virtually all information and the entire Internet based economy will be impacted. It is not hyperbole to suggest that this legislation's impacts would cascade throughout the Internet ecosystem and fundamentally alter our economy in harmful ways. Today's economy is built on a web of interconnectedness featuring specialized companies providing services such as marketing, billing, order fulfillment and support. The requirement that consumers opt-in every time virtually any information is shared is impractical. This overly broad nature legislation will discourage and not encourage Connecticut businesses from investing and innovating.

**VIII. Internet service providers protect their customers' sensitive personal data.**

NECTA members do not and will not sell their customers' sensitive personal data. Some have speculated that ISPs have access to customers' digital lives including search and browsing histories along with visibility in to their activities on individual websites. In fact, ISPs have limited - and increasingly less - visibility into consumer activities and online information due to numerous factors such as encryption of Internet traffic. Today, the vast majority of all web traffic is encrypted preventing any entity without permission, including ISPs, from observing a consumer's activity on a particular website.

The 2017 RIF Order did not change current ISP practices or diminish their obligations under the established federal privacy framework. Instead, the order now requires enhanced transparency which ensures consumers and regulators have access to and awareness of providers policies and conduct. Broadband companies have long complied with privacy rules related to data collected online that are consistent with the FTC privacy regulations.

NECTA's members place great emphasis on ensuring the protection of their customers' privacy. Consistent with that priority, major ISPs — including all Connecticut NECTA members — have publicly pledged that they will not sell or share their customers' browsing histories to third parties, and have publicly committed to extensive and legally enforceable privacy promises, including not to sell customers' sensitive information (such as banking, children's, and health information) without their affirmative, opt-in consent. These privacy statements are clear, transparent, and conspicuous for all NECTA members' customers.

**IX. State and federal law protects consumer privacy**

This bill is not necessary to protect privacy— existing federal and state law already protects consumer privacy, and gives regulators and individual consumers the tools to hold providers accountable if they do not adhere to their privacy commitments. This bill is also affirmatively harmful — to both consumers, who will be confused and frustrated when they are unable to use Internet services in the ways they expect and rely on, and to the larger Internet ecosystem, which will be subject to different, sometimes conflicting laws.

Under the existing authority of the FTC and state laws – including Connecticut's consumer protection laws– these privacy commitments by ISPs are legally enforceable. This privacy protection regime has applied for more than 20 years to the entire Internet ecosystem to the benefit of consumers and providers alike. When businesses violate privacy commitments or behave in a manner which is unfair or deceptive the FTC has punished bad behavior and will certainly continue to do so. As the nation's leading privacy regulator, the FTC has filed over 500 privacy enforcement cases. This successful approach has been endorsed and adopted by both Democratic and Republican federal policy makers in Congress and at the regulatory agencies which oversee ISPs and others.

SB6 violates these principles. It is the kind of state imposed regulatory scheme that Congress expressly rejected. This legislation will directly conflict with and frustrate the clear federal preference for a uniform, national privacy framework, administered and enforced by the FTC, for ISPs and other Internet companies.

## X. Conclusion

Deleted: ¶
¶

NECTA members strongly support and adhere to the principles of net neutrality, including no blocking, throttling, discriminating or otherwise interfering with the lawful online activity of our customers. We believe the best way to achieve lasting consumer protections, an open Internet, and strong consumer privacy is through a national policy framework that is established through bipartisan federal legislation. Codifying these protections under a clear, modern, and enduring law along with existing state and federal enforcement authority, will prevent unnecessary disruptions and the unintended consequences that would ensue from a patchwork of state regulation of the Internet.

On the other hand, if the legislature passes SB6, it would create disruption and uncertainty for consumers' experience by upending what should be a uniform, national set of rules under which our businesses and other Internet based companies operate. There is real potential for dramatic confusion as well as unintended consequences for consumers and businesses alike.

For all of the above reasons, NECTA respectfully opposes SB6.

Respectfully,

Dated: February 19, 2019

_____
Timothy O. Wilkerson
Vice President & General Counsel