STATE PRIVACY AND SECURITY COALITION

TESTIMONY OF ANDREW KINGMAN
BEFORE THE JOINT COMMITTEE ON ENERGY AND TECHNOLOGY
IN OPPOSITION TO SB 6

February 19, 2019

Dear Chairmen Needlemen and Arconti, Vice Chairs Fonfara and Allie-Brennan, and Members of the Joint Committee:

On behalf of the State Privacy & Security Coalition, which is comprised of 23 major technology, media, communications and retail companies and six trade associations in these sectors, I appear today in opposition to SB 6.

The bill would impose unreasonable and unwarranted obligations, such as requiring express approval from a consumer before an Internet service provider could provide even basic services or perform functions that are well within the consumer's expectations. We oppose this legislation because ISP privacy legislation by an individual state is unnecessary, as this issue is addressed by both federal and state law. In fact, bills like this have been considered in over half of the states, and many multiple times (including this state), since 2016. Not a single state endorsed the imposition of regulations on a service that transcends state boundaries. The bill would not meaningfully benefit Connecticut consumers and in fact would cause consumer frustration.

The Existing Privacy Regulatory Framework Already Protects Consumers

The original justification for state ISP-targeted privacy legislation was that there was some sort of "federal regulatory gap." In fact, no such gap ever has existed. Before the Federal Communications Commission (FCC) reclassified broadband internet access services (BIAS) as a telecommunications service, the Federal Trade Commission (FTC) had authority to police ISP's privacy practices. When the FCC imposed common carrier regulation on ISPs, it made clear it would use its statutory authority to oversee those companies' privacy practices. Now that the FCC has restored its prior, long-standing classification of BIAS as an lightly regulated information service,[1] and the 9th Circuit has determined that the FTC has authority over common

[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.

carriers' ISP services,[2] the Federal Trade Commission (FTC) will reassert its oversight and enforcement authority over ISP consumer privacy practices.

Claims that the Congressional action preventing the FCC broadband privacy rules from taking effect freed ISPs to sell or misuse customer personal information are simply false. ISP customers are already protected from the sale or any surprising use of their data, such as their personal web browsing history. All major ISPs have designed their privacy practices based on the FTC's robust privacy framework, which includes guidance on transparency and choice and requires opt-in consent for use or disclosure of sensitive categories of data. Long before the FCC's December Order, ISPs committed to enforceable ISP Privacy Principles, which are consistent with the FTC's robust privacy framework. Moreover, in an attempt to address misleading news stories, many ISPs have publicly affirmed that they do not sell their customers' personal web browsing histories.

Like most other states, Connecticut has a state-level consumer protection act[3] to police unfair and deceptive business practices. It gives the Department of Consumer Protection authority to take action against entities for violating promises made in consumer privacy policies and public privacy commitments. The FTC exercises similar authority to bring the same kinds of privacy and data security enforcement actions against ISPs and other companies.

Because broadband service is critical to e-commerce, creating new and different standards in Connecticut risks disrupting a significant portion of the state's innovation economy and would have major unintended consequences for consumers and businesses as ISPs are forced to adjust their investment and technology deployment plans based on a singular set of rules for the state.

An unworkable opt-in consent bill risks stifling investment and innovation by existing ISP providers and new entrants, both of whom would be restricted by the bill from, for example, developing new and innovative ways of making the Internet, content, and online services accessible to consumers.

With the recent FCC order, the FTC once again has jurisdiction over ISP privacy practices (which had been taken away by the FCC for only a few years). The FTC is the recognized expert agency on consumer privacy and has a long history of bringing enforcement actions against all types of business in the Internet ecosystem. What is more, the elimination of the FCC's privacy rules applicable to ISPs has not changed anything as these rules had not gone into effect.

Moreover, there are a number of other relevant federal privacy laws and regulations that protect specific types of consumer data, including ECPA (privacy of communications and customer

---

[2] *FTC v. AT&T Mobility LLC,* 883 F.3d 848 (9th Cir. Feb. 28, 2018) (recognizing that the common carrier exception in the FTC Act applies only to common carrier activities).

[3] Connecticut Unfair Trade Practices Act (CUTPA), Conn. Gen. Stat. Ann. §§ 42-110a *et seq.*, 42-110b ("No person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce.").

account information), CAN-SPAM (commercial email), TCPA (text and telemarketing), COPPA (children's online privacy), GLBA (financial privacy), in addition to the FCC enforcement promise described earlier.

Federal Regulators Have Acted to Ensure Uniform Application of Privacy Rules

- **FTC Privacy Framework**

The FTC is the established expert agency on consumer privacy and a strong enforcer of consumer privacy interests. Using its authority under Section 5 of the FTC Act to enforce consumer protection issues for the rest of the Internet, just as they enforced ISP consumer protection issues before the FCC took that authority away. The FTC has brought over 500 cases protecting the privacy and security of consumer information and has a staff of 40+ privacy experts (made up of lawyers and technologists) who police Internet privacy and data security and provide guidance to businesses and consumers. The FTC will again apply the same, effective regulatory framework to ISPs that it applies to the rest of the internet ecosystem - a technology and industry neutral framework that provides meaningful consumer privacy protections without unnecessarily stifling innovation and commerce.

In developing its privacy framework, the FTC engaged in a thoughtful, multi-year process that solicited and took into account input from many stakeholders and was praised by privacy and consumer groups. And in the meantime, the FCC continues to enforce ISP privacy commitments through its statutory authority.

State Legislation is Unnecessary

- **There is no gap in privacy protections relating to ISP privacy practices**

As explained above, there is no gap in existing federal or state law that would permit ISPs to violate their customers' privacy.

- **State regulation would not lead to meaningful consumer benefits, would conflict with federal policy and be preempted, and raise serious First Amendment questions**

Because consumers are already protected under both federal law and state law, as well as by ISPs' commitments in their respective privacy policies and under self-regulatory principles (which could be enforced against them), action taken by an individual state to regulate ISP privacy would not meaningfully benefit consumers.

In the case of SB 6, the bill overlooks the fact that the Internet is an intrinsically interstate service, the core nature of which is to collect and to transmit information. It is impossible for an ISP to provide service without collecting information sent by an end user, and yet the bill would require the ISP to get customer consent even to provide the service. As a result, the bill could require every ISP to obtain meaningless consent for the collection of information. If customers

refused consent, it would be impossible to provide the service to them, and the result would be serious disruptions in Internet service with no benefit to consumers.

More generally, any action taken by an individual state on privacy in the context of ISPs could lead to consumer confusion, as well as disparate legal regimes and uncertainty, and would, further, not meaningfully benefit consumers, who are already protected from having data such as their personal web browsing history sold by ISPs without consent as noted above.

State Activity Since 2016

Despite the introduction of bills in over half the states amidst a campaign that falsely alleged that ISPs were suddenly free to sell customer information without restriction, **not a single state** has passed ISP privacy legislation. Moreover, these proposals have been rejected in a string of states, including Connecticut, as well as California, Vermont, Maryland, Minnesota, Oregon, Hawaii and Washington. There is increasing recognition of the unintended consequences that could result from legislation of this kind, as well as the lack of any regulatory gap

Thank you for your consideration.

Andrew A. Kingman
Counsel, State Privacy & Security Coalition