STATE PRIVACY AND SECURITY COALITION

Legislative Commission on Data Practices
Minnesota House of Representatives
10 State Office Building
St. Paul, MN 55155

November 28, 2017

Re: Internet Security and Privacy Hearing

Chair Scott and Members of the Committee:

Thank you for the opportunity to testify about Internet security and privacy. My name is Ryan Sulkin and I am here on behalf of the State Privacy & Security Coalition, which is comprised of 27 major technology, media, communications and retail companies and six trade associations in these sectors. Our Coalition opposes state action on this issue because it is already well-addressed by both federal and state law. Twenty-eight states have considered and rejected Internet Service Provider (ISP) privacy legislation this year, and for very good reasons.

Overview

ISP customer privacy is already protected under existing state and federal law, including through the enforceable promises of ISPs. All major ISPs have designed their privacy practices based on the FTC's robust and successful privacy framework which includes guidance on transparency and choice. ISPs have also committed to the ISP Privacy Principles, which are consistent with the FTC privacy framework. Moreover, a number of ISPs have publicly affirmed that they do not sell their customers' personal web browsing histories and have privacy policies that would prevent such behavior.

In addition to there being no need for yet another law overseeing ISP privacy practices, creating new and different standards in Minnesota risks disrupting a significant portion of the state's innovation economy and creating major unintended, harmful consequences for consumers and businesses, alike. ISPs would be forced to adjust their investment, technology deployment plans, and product and service offerings based on a singular set of rules for the state.

Arguments that the Congressional action preventing the FCC broadband privacy rules from taking effect has freed ISPs to sell customer personal information without limitation are simply false. The elimination of the FCC's privacy rules applicable to ISPs has not changed consumers' protections, since these rules had not yet gone into effect prior to their elimination, and the underlying FCC privacy statute continues to apply.

Minnesota already has an ISP law that protects subscribers.[1] The statute prohibits ISPs from divulging personal information, including consumer identity, web browsing activity and stored computer data information, without a customer's authorization. Moreover, Minnesota Unlawful Trade Practices Act and its Consumer Protection Act both prohibit businesses from making misrepresentations about their products and services.[2] These existing laws give the Minnesota Attorney General – and consumers themselves –vehicles to take action against ISPs and other companies for violating promises made in consumer privacy policies and public privacy commitments.[3]

The Existing Privacy Regulatory Framework Already Protects Consumers

The privacy practices of ISPs are already subject to several layers of laws, regulations, and other enforceable restrictions. Nothing about Congress's decision to rescind the FCC's flawed broadband privacy rules has freed ISPs to sell customer personal information without limitation – assertions to the contrary are simply false. Congress' action simply rejected rules had not even gone into effect because of the siloed, piece meal nature of the FCC's 2016 decision. There is no gap in the law that would permit ISPs to violate their customers' privacy.

On December 14th, the FCC plans to vote to reclassify the broadband Internet service back to a Title I service. As FCC Chairman Pai recognized in his announcement of the upcoming release of the draft order, "my proposal will put the federal government's most experienced privacy cop, the FTC, back on the beat to protect consumers' online privacy."[4] And FTC Acting Chair Maureen Ohlhausen has lauded the FCC's decision and reiterated that "[t]he FTC stands ready to protect broadband subscribers from anticompetitive, unfair, or deceptive acts and practices just as we protect consumers in the rest of the Internet ecosystem."[5]

The FTC has not only the authority, but also the right experience to protect consumers' online privacy. 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 received high praise from privacy and consumer groups. The agency has been a strong enforcer of consumer privacy interests and has brought over 500 cases protecting the privacy and security of consumer information. When the FCC's "Restoring Internet Freedom" order is final, ISPs will be subject to the same effective regulatory framework that applies to the rest of the Internet ecosystem -- a technology- and industry-neutral

[1] Minn. Stat. § 325M.01-.02 (2016).
[2] See Minn. Stat. § 325D.09 (2016) and Minn. Stat. § 325F.67 (2016).
[3] See Minn. Stat. § 8.31, subd. 1 and subd. 3a (2016); Minn. Stat. § 325D.15 (2016).
[4] http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db1121/DOC-347868A1.pdf.
[5] https://www.ftc.gov/news-events/press-releases/2017/11/statement-acting-ftc-chairman-maureen-k-ohlhausen-restoring.

framework that provides meaningful consumer privacy protections without unnecessarily stifling innovation and commerce.

Until such move is made, however, the FCC retains the ability to enforce Section 222 against ISPs even without its former flawed rules – or any rules – in place. Since 2015, the FCC under both Chairman Wheeler and Chairman Pai has asserted its authority under Section 222 to enforce consumer privacy, regardless of the existence of any rules.[6] Section 222 imposes a duty of confidentiality and duty of care that applies to broadband ISPs.

Additional federal privacy laws and regulations

In addition to the enforcement authority granted to the FTC and FCC, there are a number of other relevant federal privacy laws and regulations, including the Children's Online Privacy Protection Act (protecting children's information collected through websites or online services), the Electronic Communications Privacy Act (protecting the privacy of communications and customer records), CAN-SPAM (protecting consumers from unwanted commercial email), and the Telephone Consumer Protection Act (protecting consumers from unwanted texts and telemarketing). A violation of any of those laws could lead to enforcement by state regulators through the state's consumer protection ("mini-FTC") laws, and, in many instances, by consumers through private rights of action.

State Regulation Would Not Lead to Meaningful Consumer Benefits

Because consumers are already protected under *existing* 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.

What is more, hastily-developed ISP-focused privacy legislation taken by an individual state would be premature and could lead to consumer confusion, as well as disparate legal regimes and uncertainty. The FCC has recognized that "broadband Internet access service should be governed principally by a uniform set of federal regulations, rather than by a patchwork of separate state and local requirements,"[7] because conflicting state rules can impair provision of broadband service. This is the case with broadband privacy rules, which can inflate the cost of deploying broadband service by adding significant state-specific compliance costs and bar innovative business models that benefit consumers.

[6] In particular, in 2015 the FCC issued an enforcement advisory regarding its intent to enforce Section 222 against broadband ISPs, stating: "By examining whether a broadband provider's acts or practices are reasonable and whether such a provider is acting in good faith to comply with Section 222, the Enforcement Bureau intends that broadband providers should employ effective privacy protections in line with their privacy policies and core tenets of basic privacy protections." And in an order adopted on June 26, 2017, the Commission reminded ISPs of their obligations to protect consumer privacy under Section 222 and reiterated the FCC's commitment to enforce these protections in accordance with the guidance in that enforcement advisory. http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0629/FCC-17-82A1.pdf.
[7] Cite Restoring Internet Freedom Order.

Consumers are already protected from having data such as their personal web browsing history sold by ISPs without consent, as noted above. And a comprehensive approach to privacy is consistent with consumer expectations – according to a survey by Peter Hart, 94 percent of consumers want the same protections to apply to their online information regardless of the entity collecting such information.

Conclusion

Despite the introduction this spring of bills in more than half the states amidst a campaign that falsely alleged that ISPs are suddenly free to sell customer information without restriction, no state has passed ISP privacy legislation this year. The proposal has been rejected in a string of states, including California, Connecticut, Vermont, Maryland, Massachusetts, Hawaii, and Washington, as well as in other, western states such as Montana. The consistent rejection of these proposals highlights that this issue is less about politics, and more about an increasing recognition of the potential unintended consequences and negative repercussions that could result from this kind of legislation.

For these reasons, we oppose action by an individual state on this issue.

Thank you for your consideration.

Ryan Sulkin

DLA Piper LLP (US)
www.dlapiper.com