August 3, 2018

VIA ELECTRONIC MAIL

Ryan Kriger
Assistant Attorney General of Vermont
109 State St.
Montpelier, VT 05609

Re: Hearings on Protecting the Privacy of Vermonters

Dear Mr. Kriger:

As a Vermont native, I care deeply about ensuring that Vermonters are granted the privacy protections they deserve, particularly from their internet service providers (ISPs). The Vermont Attorney General's office has the opportunity to be a leader in this space, especially if it enacts strong requirements that provide Vermonters with real choice, control, and security over the data their ISPs collect about them. In this letter, I will explain why ISPs need separate privacy rules, what happened with the FCC's rule, and why my organization's model bill (included with this letter along with an explainer) is the best approach.

Consumers need strong privacy protections over how ISPs treat their data. As purveyors of the network and gatekeepers to the internet, ISPs are in a privileged position with nearly-comprehensive access to data about their customers.[1] To receive internet access service, consumers must choose an ISP, pay a significant monthly fee to that ISP, and then by virtue of accessing the internet, they have to disclose a vast array of data to their ISP. The data ISPs collect and see is highly personal and detailed, including web browsing records, geolocation data, financial and health information, and in some cases the content of communications. This universe of data can reveal, for instance, a customer's race or nationality, sexual preference, religion, physical location, presence at home, personal banking details, and physical ailments.

Armed with such comprehensive and revealing data, ISPs can and likely do create intricate profiles of their individual subscribers. Further, they are able to use, sell, or provide access to

[1] Eric Null, *ISPs Know All*, Slate (June 21, 2016), http://www.slate.com/articles/technology/future_tense/2016/06/you_deserve_more_privacy_from_your_broadband_provider.html.

that data for a variety of purposes, including targeting digital advertisements for products such as payday loans or expensive and unnecessary medications.

To make matters worse, the ISP market lacks robust competition. In the 2017 Restoring Internet Freedom Order, the FCC shared data that showed nearly 50% of the US population has either zero or one option for broadband at 25 mbps download or faster, the FCC's defined threshold for high-speed internet access.[2] In Vermont, access (and therefore competition) remains a problem. According to the Vermont Department of Public Service's most recent broadband map, nearly 27% of Vermont remains *unserved* by a single provider offering 25 mbps download speeds.[3] And even in areas that are served, robust competition is unlikely to exist.

Thus, ISP customers in most cases cannot switch providers, as they often can with providers of online services (such as Amazon), to avoid problematic ISP privacy practices. As such, consumers should have the right to choose, through opt-in consent, whether and how their ISPs can use their personal information for purposes other than providing internet access service.

Recognizing these concerns, the FCC passed strong broadband privacy rules in October 2016 that gave consumers the protections they needed. After years of debating and vetting what requirements were most appropriate, the FCC gave consumers choice, transparency, and security over how ISPs use customer data—primarily through requiring opt-in consent for most uses of data.

The broadband privacy rule was hailed as a victory for consumers, who have long been in favor of stronger privacy protections in general. For instance, a recent Pew Research Center study found that 91% of adults agree that "consumers have lost control over how personal information is collected and used by companies," and that 64% of Americans believe government should issue regulations to protect their data from indiscriminate use for digital advertising purposes.[4] Bain & Company surveyed over 900 U.S. consumers and similarly found that "91 percent of respondents do not want companies selling their data, even if they are compensated for it."[5]

---

[2] Restoring Internet Freedom Order, 33 FCC Rcd 311, ¶ 125 (Dec. 2017), https://docs.fcc.gov/public/attachments/FCC-17-166A1_Rcd.pdf (showing nearly 50% of US population has between zero and one option for 25 mbps download speeds).

[3] Broadband Availability by Road Segment at 25 Mbps Down / 3 Mbps Up or Better, http://publicservice.vermont.gov/sites/dps/files/documents/Connectivity/BroadbandReports/2018/BroadbandAvailability25_3_20180112.pdf.

[4] Lee Rainie, *The State of Privacy in Post-Snowden America*, Pew Research Center (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america.

[5] Press Release, Bain & Co., How Can Companies Acquire Customer Data While Building Customer Loyalty at the Same Time? Ask Permission, May 11, 2015, http://bain.com/about/press/press-releases/Digital-privacy-survey-2015-press-release.aspx.

Unfortunately, Congress overturned the broadband privacy rule using an expedited process under the Congressional Review Act, despite overwhelming bipartisan support for the broadband privacy rule from consumers. A March 2017 poll showed that 80% of Democrats and 75% of Republicans wanted the President to veto Congress' repeal bill and allow the FCC's rule to take effect.[6] Even fifteen House Republicans bucked party leadership and voted to retain the broadband privacy rule.[7]

In the wake of the federal government's repeal, there are no clear rules governing what ISPs can do with customer data, and jurisdiction has been ceded back to the Federal Trade Commission (FTC), a small agency with limited authority tasked with overseeing all interstate commerce. At this point, ISPs can simply set their own rules in their privacy policies and consumers are virtually powerless to protect themselves.

After Congress rescinded the broadband privacy rules, my organization drafted a model bill for states to consider enacting. The model language takes a comprehensive approach to protecting broadband privacy.[8] Rather than create separate buckets of sensitive and non-sensitive data (the approach used in the FCC rules and by the FTC in its enforcement), the model requires broadband providers to protect *all* information they collect by default. The model does that by requiring broadband providers obtain opt-in consent before using, selling, disclosing, or providing access to customer information (which includes merely de-identified data) for *any* non-service-related purpose, with some exceptions. The model also requires broadband providers to provide clear and prominent notice of its privacy practices and to use reasonable security measures to protect its customers' data.

The model bans so-called "pay for privacy" schemes, where a broadband provider will upcharge a customer who wants to protect his or her privacy—or will provide a steep discount to customers who agree to essentially no limitations on how the broadband provider can use his or her data. This practice is predatory, and is designed to coerce or, at best, induce customers into giving away their privacy rights.

Certain uses of customer data are allowed, however. For instance, exceptions include emergency situations and use for billing a customer. Also, aggregate data (that which is removed of

---

[6] Matthew Yglesias, *Republicans' Rollback of Broadband Privacy Is Hideously Unpopular*, Vox (Apr. 4, 2017), https://www.vox.com/policy-and-politics/2017/4/4/15167544/broadband-privacy-poll; *see also* Priorities USA & Civis Survey, https://www.scribd.com/document/344203409/PUSA-Civis-ISP-Crosstabs (finding 83.3% of survey respondents opposed the President signing the bill to repeal the FCC's privacy rules).

[7] Kimberly Kindy, *How Congress Dismantled Federal Internet Privacy Rules*, Wash. Post (May 30, 2017), https://www.washingtonpost.com/politics/how-congress-dismantled-federal-internet-privacy-rules/2017/05/29/7ad06e14-2f5b-11e7-8674-437ddb6e813e_story.html.

[8] Eric Null, *OTI Publishes Model State Legislation to Help States Protect Broadband Privacy*, Open Tech. Inst. (Oct. 26, 2017), https://www.newamerica.org/oti/blog/oti-publishes-model-state-legislation-help-states-protect-broadband-privacy.

identifiers and combined) is granted less protection because it is generally understood to present fewer privacy risks. This is in contrast to merely de-identified data, which which has some identifiers removed but is individualized, making it much easier for that data to be associated with an individual.[9]

I hope that the Vermont Attorney General's office will consider adopting regulations that mirror my organization's model bill and will help push for a similar law to be passed through the Vermont legislature. Strong rules, and ultimately a strong state law, could help protect Vermont residents against privacy intrusions from their ISPs.

Sincerely,

Eric Null
Senior Policy Counsel
Open Technology Institute | New America

[9] It is trivial for de-identified data to be re-identified. *See, e.g.,* Boris Lubarsky, *Re-Identification of "Anonymized" Data*, 1 Geo. Law Tech. Rev. 202 (2017), https://www.georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017; Sharad Goel & Arvind Narayanan, *Why You Shouldn't Be Comforted by Internet Service Providers' Promises to Protect Your Privacy*, Slate (Apr. 4, 2017), http://www.slate.com/blogs/future_tense/2017/04/04/don_t_be_comforted_by_internet_providers_promises_to_protect_your_privacy.html.