Testimony of Kimberly McCullough, Policy Director
In Support of ISP Privacy Amendments to HB 2813
House Committee on Rules
May 4, 2017

Chair Williamson and Members of the Committee:

The American Civil Liberties Union of Oregon[1] supports amending HB 2813 to protect the privacy of the privacy of Internet subscribers in the state of Oregon.

Using the internet is a fundamental part of living in our society, participating in our democracy, and exercising our constitutional rights, including those around speech, expression, religion, and association. It is particularly important to preserve an equal playing field in this space, and protect individuals who may not have the same power as corporations to understand, influence, and control the dissemination of their information.

A person should not have to sacrifice their privacy rights and give up a rich trove of personal information to ISPs in order to access those rights via the internet. Yet that is exactly the scenario we are in—most people have little or no choice in their ISP provider (it's an oligopoly), and most of the ISPs are trying to monetize the data that consumers are forced to give them by virtue of the nature of providing broadband services. Corporations should not be given this kind of power over individuals' ability to associate.

A person's right to associate and engage in protest is on the line here. Simply by providing information required to receive broadband service, a person's political, religious and social connections could be determined through the rich trove of meta-data that companies are now free to buy and sell. They could also be assigned a threat score based on that data, which could result in their being targeted as political organizers and activists, as participants in protest, or as belonging to a particular religion. These rights are critical to preserve in the face of corporate encroachment.

There should be no additional charge for privacy—even if that charge is obfuscated by being presented as just regular pricing, while those who surrender privacy get a discount. This would disproportionately impact low-income people and people of color, who aren't in a position to pay more for privacy. And this kind of scheme is also prone to abuse—it is extremely difficult for a customer to enforce agreements around their data. A lack of consumer education also undermines the efficacy of such schemes. It is better to ensure meaningful consent at the front end, with no penalty for those who don't consent.

Thank you, and please feel free to contact me with any questions, comments or concerns.

---

[1] The ACLU of Oregon is a nonpartisan, nonprofit organization dedicated to the preservation and enhancement of civil liberties and civil rights with over 40,000 members across the state of Oregon.

GEORGETOWN LAW
Center on Privacy & Technology

Statement of Laura Moy, Deputy Director
Center on Privacy & Technology at Georgetown Law

Respectfully submitted to the

Washington State Legislature

Regarding

Privacy and Security of Internet Users

April 18, 2017

Laura M. Moy
Deputy Director | Center on Privacy & Technology
Georgetown University Law Center
600 New Jersey Avenue, NW
Washington, DC 20001
(202) 662-9547 | laura.moy@georgetown.edu

Introduction and Summary

Thank you for working to address the privacy of Internet subscribers in the state of Washington. I was one of the leading advocates in support of strong broadband privacy rules at the federal level—rules that were adopted last October, but recently eliminated under the Congressional Review Act. I present my views in this statement as a consumer and privacy advocate.

Policymakers can probably agree that they want everyone to get connected to the Internet. In the modern era, it is difficult or even impossible to get an education, apply for a job, run a business, or conduct one's banking without an Internet connection. To get connected, consumers have no choice but to go through an Internet service provider (ISP).

Because of their position as the consumer's gateway to the Internet, ISPs then have broad, unfettered access into nearly everything the consumer does online. Like a mail carrier must be able to read addresses on envelopes in order to route the mail, an ISP must be able to read addresses on bundles of data in order to route a consumer's Internet traffic.

That information can be incredibly revealing. It's not difficult to imagine how a complete record of the websites a consumer visits and the applications they use, especially in combination with details about the timing, duration, and volume of traffic, can be used to determine their medical conditions, employment status, family status, political leanings, romantic and sexual preferences, sleep habits, and more.

But that information doesn't belong to the companies that supply Internet connections—it rightfully belongs to consumers. Consumers are already paying for their Internet connections in dollars—handsomely. They do not also need to pay through their personal data. They only share such deeply private information about themselves with ISPs so that their traffic can be routed to the right place. They do not expect ISPs to collect, retain, and use that information to make money off of them.

Making matters worse, many consumers cannot switch providers if they dislike the privacy practices of their ISP. In many areas, consumers have only one option when it comes to high-speed broadband. Even when there are two or three possible providers, switching costs—contract termination fees, installation fees, the time investment necessary to research and adopt an alternative—can make it very difficult for a subscriber of one provider to switch to another.

Nor is there much that the average consumer can do to hide their online activities from their ISP. The few things consumers can do to protect their own privacy from their ISPs add up to a handful of weak tools that are at best suboptimal and at worst horribly insufficient.

For these reasons, state legislation to protect consumer privacy from ISPs is needed, and it is needed swiftly.

1. Consumers have no choice but to share highly personal information with an Internet service provider.

Virtually every single consumer shares information about everything they do online with an ISP. Consumers share this information not because they want to, but because they must. At one time Internet connectivity may have been a mere luxury, but today most Americans consider it to be a necessity. In the words of major ISP Comcast, "Internet service has become essential for success."[1]

The essential nature of Internet service in the modern economy sets ISPs apart from other kinds of companies that operate online. A consumer may choose whether or not to join a particular social network, use a particular email provider, conduct searches through a particular search engine, or purchase goods through a particular Internet retailer. But sharing information with an ISP is an unavoidable part of going online.

Making matters worse, many consumers cannot switch providers if they dislike the privacy practices of their ISP. In many areas, consumers have only one option when it comes to high-speed broadband. Even when there are two or three possible providers, switching costs—contract termination fees, installation fees, the time investment necessary to research and adopt an alternative—can make it very difficult for a subscriber of one provider to switch to another.

2. The information that consumers must share with their Internet service provider reveals details about their private lives.

From their privileged position as gatekeepers to the Internet, ISPs have tremendous visibility into nearly everything their clients do online, and

---

[1] Comcast, Internet Essentials Flyer, *available at* http://www.gaithersburgmd.gov/~/media/city/documents/services/community/comcast_internet_essentials_flyer.pdf (last visited Apr. 6, 2017).

can learn detailed information about consumers' private lives. An ISP can see what websites its subscribers visit and when they visit them, and can make inferences based on that information. As explained in a 2016 paper on broadband privacy published by New America's Open Technology Institute,

> Domain names, of course, can expose intimate details about the subscriber's health (plannedparenthood.org), finances (acecashexpress.com, particularly if accessed before each payday), political views (joinnra.nra.org), and many other sensitive attributes. A subscriber's history of domain name lookups could also be used to more accurately predict certain attributes about a subscriber like gender, age, race, income range, and employment status. Without appropriate regulatory safeguards for broadband traffic data such as DNS queries, these inferences could be made available on the open market, without specific notice or affirmative consent from the subscribers whose lives are being examined.[2]

In addition, even when consumers' online activities have been purged of personal identifiers, such as name or a subscriber identifier, browsing histories can still be linked back to specific individuals. As explained this week by anonymization experts Sharad Goel and Arvind Narayanan, who this week presented a paper on the challenges of anonymizing web histories, "'anonymous' web browsing records often contain an indelible mark of one's identity. We recruited nearly 400 users to send us their web browsing data

[2] The FCC's Role in Protecting Online Privacy (Jan. 21, 2016) at 5, *available at* https://www.newamerica.org/oti/policy-papers/the-fccs-role-in-protecting-online-privacy/.

stripped of any overt personal identifiers. In 70 percent of cases we could identify the individual from their web history alone."[3]

No other type of actor in the Internet ecosystem has access to as rich and reliable a stream of private information about individual users as ISPs. As noted privacy scholar Paul Ohm explained before the United States Senate Commerce Committee last year,

> No other entity on the Internet possesses the same ability to see. If you are a habitual user of the Google search engine, Google can watch you while you search, and it can follow you on the first step you take away from the search engine. After that, it loses sight of you, unless you happen to visit other websites or use apps or services that share information with Google. If you are a habitual Amazon shopper, Amazon can watch you browse and purchase products, but it loses sight of you as soon as you shop with a competitor. Habitual Facebook users are watched by the company when they visit Facebook or use websites, apps or services that share information with Facebook, but they are not visible to Facebook at any other times.[4]

In contrast to services like Google, Amazon, and Facebook, ISPs can see at least some information about everything its subscribers do online, using their connection.

---

[3] Sharad Goel & Arvind Narayanan, *Why You Shouldn't Be Comforted by Internet Providers' Promises to Protect Your Privacy*, Future Tense (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 (referring to Jessica Su, Ansh Shukla, Sharad Goel, & Arvind Narayanan, *Anonymizing Web Browsing Data with Social Networks*, *available at* https://5harad.com/papers/twivacy.pdf).

[4] Testimony of Paul Ohm Before the Senate Commerce Committee, July 12, 2016, at 3, http://paulohm.com/projects/testimony/PaulOhm20160712FCCPrivacyRulesSenate.pdf.

3. Consumers cannot keep their online activities private from their Internet service provider on their own.

The threat to consumer privacy posed by ISPs is not a threat that consumers can address on their own. As I explained in a recent op-ed, none of the potential privacy protecting tools that consumers could use to hide their online activities from their ISP are perfect.[5]

Consumers may start with the privacy options offered by their ISP, but as a privacy self-help tool, consumer-facing privacy options are weak at best. Consumer-facing notices associated with privacy options are often difficult to locate and even more difficult to understand. Options are often provided on what companies consider to be a voluntary basis—which means they could disappear or change at any time. Indeed, privacy options are likely to change in some ways as the regulatory landscape changes.

Tech-savvy consumers who can afford an additional monthly fee on top of what they already pay their ISP may consider signing up for a "virtual private network," or VPN service. As I explained, however,

> [I]t's not as easy as it sounds: You have to have a bit of geek know-how to properly configure your VPN, and (annoyingly) you'll also have to remember to turn on your VPN every single time you connect to the internet. Not only that, but tunneling all of your traffic through a VPN will substantially slow down your internet experience. And if that wasn't bad enough, it might not even address your privacy concerns: Just like your internet provider, your VPN provider could also track and sell your online activities. Needless to say, VPNs are not a magic cure for internet privacy.

---

[5] Laura Moy, *Think You Can Protect Your Privacy from Internet Providers Without FCC Rules? Good Luck.*, The Daily Dot (Mar. 28, 2017), https://www.dailydot.com/layer8/congress-kill-isp-privacy-protections/.

Finally, consumers who know how to install browser extensions can install a free extension that will automatically take the consumer to the encrypted version of a website whenever one is available. Unfortunately, however, many websites do *not* have encryption available, and even when encryption is available, it does not hide all private information from the ISP.

The bottom line when it comes to privacy self-help options is that the tools available to consumers do not come close to offering consumers the same level of protection that the law can offer.

4. The best way to protect consumers' privacy from their Internet service providers is with legal protections, and right now we need more.

Because consumers have no choice but to share such highly private information with an ISP in order to get connected, because connectivity is crucially important in the modern era, and because consumers really cannot protect their own privacy from their provider, the best way to protect privacy vis-à-vis ISPs is through legal protections. Unfortunately, federal legislation under the Congressional Review Act recently wiped out the rules we had on the books on this issue—rules that would have made clear that ISPs must ask their customers' permission *before* using highly private information, such as browsing history or app usage history, for purposes other than to provide the service their customers pay for.

Some opponents of broadband privacy rules have argued that the Federal Trade Commission ought to be the agency in charge of overseeing the privacy obligations of all Internet companies, including ISPs. But the Federal Trade Commission cannot oversee ISPs, due to a many-decades-old carve-out in the statutory provision that gives the FTC its privacy teeth.[6]

---

[6] That carve-out, known as the "common carrier exemption," precludes the FTC from exercising its general authority to prohibit unfair and deceptive trade practices from entities designated as common carriers under a number

Nor can the federal statute governing broadband privacy be fully effective on its own. There are things left ambiguous in the statute, such as what must be in a consumer-facing privacy notice and what constitutes consumer "consent" for non-service-related use of private information like a subscriber's browsing history. It will be a long time before the Federal Communications Commission is able to research, draft, and pass new broadband privacy rules. Nor is it yet clear exactly how hamstrung the agency may be by the Congressional Review Act, which not only forbids the FCC from reinstituting its now-invalidated rule, but also prohibits the future promulgation of any rule that is similar.

To protect consumer privacy, it should be made crystal clear that broadband providers must seek and obtain their subscribers' permission *first*, before using private identities, demographic data, and web browsing history for marketing purposes. Right now, these are things that only state legislation can accomplish.

5. Effective privacy protections for consumers must require ISPs to seek permission not only to sell subscriber information, but also to use or permit access to data for non-service-related purposes.

Consumers do not expect ISPs to collect information to provide service and then use that information for any number of other purposes, marketing or otherwise. Non-consensual non-service-related uses of ISP subscribers' data may harm consumers and undermine competition. Thus, legislation that attempts to protect the privacy of internet subscribers should address not only the potential sale of consumers' private, information, but non-service-related uses of that information as well.

---

of other federal laws, including the Communications Act. Broadband providers fall into this category, and thus fall outside the FTC's privacy jurisdiction. *See* 15 U.S.C. 45(a)(2).

It is not difficult to imagine a wide variety of situations in which ISPs might use information about their subscribers' online activities unfairly, in ways their subscribers would not like. For instance, an ISP could target advertisements of weight-loss products to subscribers whose traffic reveals frequent use of a connected scale, teeth whitening products to subscribers who appear to use a connected toothbrush more than twice a day, occupational training to subscribers whose traffic patterns indicate a sudden increase in time spent at home during working hours (indicating loss of a job), and home security products to subscribers who have browsed the websites of multiple home security providers. Indeed, ISPs may even use their subscribers' data to undercut competitors in some of these markets—AT&T has said that it "uses the fact that a customer is an AT&T broadband customer to assist its marketing of other AT&T services, such as security services and technical support packages." Without restrictions on how the company may use its broadband subscribers' traffic data, the company could use information about a subscriber's online activities—such as visits to multiple home security competitors—to further inform and target its marketing.[7]

Consumers should have the important ability to avoid this type of analysis and unfair use of their private information—information they have no choice but to share in order to obtain a service that already costs them substantial monthly fees. Broadband privacy protections should require ISPs to obtain their subscribers' consent for non-service-related "use" of data.

In contrast, requiring consent only for the "sale" of information for non-service-related purposes would not fully address the actual data practices

---

[7] *See* Declaration of Brian Collins, Thomas F. Hughes and Matthew T. Haymons in Support of Motion for a Stay at ¶ 8, U.S. Telecom Ass'n v. Fed. Commc'n Comm'n, No. 15-1063 (D.D.C. led May 13, 2015), *available at https://www.publicknowledge.org/assets/uploads/blog/15.05.13_Motion_for_Stay_Exhibits.pdf*.

ISPs engage in to benefit from their customers' data. Multiple ISPs have said in consumer-facing statements that they do not sell their subscribers' individualized browsing histories. They may, however, use subscriber information, or permit others to use that information, in ways that many consumers do not and would not agree with, and should be required to obtain consent before engaging in those practices.

Conclusion

The state legislature's attention to this important issue is commendable. On behalf of consumers like myself, I urge you to consider the points presented above.