Before the Energy, Utilities and Technology Committee

Testimony of Gigi Sohn

Distinguished Fellow, Georgetown Law Institute for Technology Law & Policy

L.D. 946, An Act to Protect Privacy of Online Customer Personal Information

April 24, 2019

Chairman Lawrence, Chairman Berry, members of the Joint Standing Committee on Energy, Utilities and Technology, my name is Gigi Sohn. I'm a Distinguished Fellow at the Georgetown Law Institute for Technology Law and Policy and a Benton Senior Fellow. I have been an advocate for open, affordable, and democratic networks for over 30 years. As Counselor to former FCC Chairman Tom Wheeler, I worked on the FCC's 2016 Broadband Privacy Rules, upon which L.D. 946 is based.[1]

I urge the Joint Committee and the legislature to pass L.D. 946 without delay. It is common sense legislation that would require broadband Internet access providers ("broadband providers" or "ISPs") operating in the state to protect the privacy of their customers. L.D. 946 would ensure that broadband customers have meaningful control over their personal information and choice about how it's used. The bill also ensures that broadband providers offer a degree of transparency over how they use information and protect customer's personal information from outside harms. Finally, the bill encourages broadband providers to innovate by allowing them to continue to use and share customer information.

These are not controversial provisions. Broadband providers receive, store and use a vast amount of consumer information, including sensitive information. As the FCC found in 2016, broadband providers "sit[] at a privileged place in the network, the bottleneck between the customer and the rest of the network…."[2] This gatekeeper position means that broadband providers see every single piece of information—every "packet"—that a customer sends and receives over the Internet

[1] I'd like to thank Jeff Gary, Institute Associate for the Georgetown Law Institute for Technology Law and Policy for his assistance with this testimony.

[2] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd 13911, 13920 (2016)

while on the network, including the contents of those packets. While broadband providers protest that they see less than other online actors, the FCC record shows that only three online "edge" companies have 3rd party tracking capabilities across more than ten percent of the top one million websites, and that none of those can access more than approximately twenty-five percent of web pages. In contrast, a broadband provider sees 100 percent of a customer's unencrypted Internet traffic, no matter what web page or app that person uses.

Beyond having perfect visibility into a customer's unencrypted web traffic, broadband providers also see all the encrypted traffic over their networks. While the providers cannot see the contents of these packets, the encrypted traffic itself can still reveal incredibly sensitive information about customer's lifestyles and habits. For instance, an ISP can still see the domains a customer visits.[3] Taken together, users' traffic online—such as visits to https://hiv.gov or https://aidsinfo.nih.gov—paint a detailed picture. Similarly, broadband providers also see the activities of any "smart home" devices connected to their networks. The providers see when their customer turns their lights on and off, when they watch TV and for how long, when they have friends over, and more.[4] Taken together, broadband providers see a large amount of both the content their users view and the activities their users engage in.

[3] UPTURN, WHAT ISPS CAN SEE (2016), https://www.upturn.org/reports/2016/what-isps-can-see.
[4] *See* Kashmir Hill & Surya Mattu, *The House that Spied on Me*, GIZMODO (Feb. 7, 2018), https://gizmodo.com/the-house-that-spied-on-me-1822429852. Indeed, due to the proliferation of devices connected to the internet (lights, baby monitors, toothbrushes, sex toys, and beds, among others), it is possible for ISPs to have enormous insight into even the most intimate of details of a person's life.

Unlike edge providers, who may only be able to link behavioral information to a pseudonym on anonymous account,[5] broadband providers link their cache of customer information directly to real, verified subscriber accounts. Broadband providers possess their customers' real names, addresses, phone numbers, credit histories, and billing histories.[6] Broadband providers, unlike any other online provider, therefore can create uniquely detailed and comprehensive profiles on their customers, currently with little to no restrictions on how they use, sell, or share those profiles.

While broadband providers continue to claim they can simply be trusted to protect and not misuse this incredible trove of information, the facts show that is simply not true. One example makes this abundantly clear. Last year, AT&T and Verizon testified before this Committee that "no [personally identifiable customer] information is shared without customer notice and control"[7] and that "ISPs must obtain customers' permission to sell their personal web history or sensitive information."[8] Other opponents of common-sense privacy laws similarly insisted that "[t]here is no gap in federal law that would permit ISPs to violate their customers' privacy."[9] While these promises seem reassuring, we now know that at

[5] *See, e.g.*, Eric Griffith, *How to Create an Anonymous Email Account*, PC MAG (Dec. 3, 2017), https://www.pcmag.com/article/331733/how-to-create-an-anonymous-email-account; Jake Peterson, *Make an Anonymous Facebook Profile to Keep your Personal Data Private*, GADGET HACKS (Feb. 26, 2019), https://smartphones.gadgethacks.com/how-to/make-anonymous-facebook-profile-keep-your-personal-data-private-0183760.

[6] To sign up for new Internet service from Verizon, for instance, a customer must provide her real first and last name, address and ZIP code, email address, phone number, date of birth, and social security number. Few, if any, edge providers have this amount of verifiable personal information on their users.

[7] Testimony of Verizon Communications before the Energy, Utilities, and Technology Committee, May 24, 2017.

[8] Testimony of Owen Smith of AT&T before the Energy, Utilities, and Technology Committee, May 24, 2017.

[9] Memorandum from Matt Mincieli, Northeast Region Exec. Dir., TechNet to Sen. David Woodsome, Chair, Joint Standing Committee on Energy, Utilities & Technology and Rep. Seth Berry, Chair Joint Standing Committee on Energy, Utilities & Technology (May 24, 2017).

the same time broadband providers and their allies were making these claims to this Committee,[10] they were selling customers' real-time location data to bounty hunters and other criminals, who could use it, for example, to track down victims of domestic violence.[11] Despite public outcry that forced mobile broadband providers to make public assurances that they would curtail the practice,[12] they have nonetheless continued to sell this highly sensitive data well into this year.[13]

What has been the federal government's response to this report? The Federal Trade Commission just sent what's called a "6(b)" letter to broadband providers seeking details about their privacy policies, procedures and practices. Despite claims from opponents of new legislation, this marks the first major action the Commission has taken against broadband providers since it has had oversight authority. Indeed, while broadband providers insist that FTC authority is robust, they cannot point to a single instance from 2002 to 2015 (the period of FTC oversight prior to the adoption of the FCC's 2015 Open Internet Order) when the Commission brought an enforcement action against an ISP for a violation of a subscriber's privacy. Without the legal authority to make rules and with limited staff and resources, the

---

[10] *See* Letter from Anthony Russo, Vice President, Fed. Leg. Affairs, T-Mobile US, Inc. to Ron Wyden, U.S. Senator, Feb. 15, 2019 (disclosing multiple abuses of T-Mobile consumer data ranging from 2014 to 2019), https://www.documentcloud.org/documents/5767086-T-Mobile-Response-to-Wyden-on-Phone-Location.html.

[11] Letter from Ron Wyden, U.S. Senator to Ajit Pai, Chairman, Fed. Commc'ns Comm'n, May 8, 2018, https://www.wyden.senate.gov/imo/media/doc/wyden-securus-location-tracking-letter-to-fcc.pdf; Joseph Cox, *I gave a Bounty Hunter $300. Then He Located Our Phone*, MOTHERBOARD (Jan. 8, 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

[12] Brian Fung, *Verizon, AT&T, T-Mobile and Sprint Suspend Selling of Customer Location Data After Prison Officials Were Caught Misusing It*, WASH. POST (June 19, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/06/19/verizon-will-suspend-sales-of-customer-location-data-after-a-prison-phone-company-was-caught-misusing-it.

[13] Karl Bode, *Senator Wyden Hammers T-Mobile for Empty Promises on Sale of Cell Phone Location Data*, MOTHERBOARD (Jan. 18, 2019), https://motherboard.vice.com/en_us/article/d3mgkv/senator-wyden-hammers-t-mobile-for-empty-promises-on-sale-of-cell-phone-location-data.

FTC can only do so much to protect consumers from the privacy violations of broadband providers.

Similarly, the FCC has allegedly been "investigating" the geo-location matter for over a year. Had the FCC's privacy rules still been in place, the mobile broadband providers wouldn't have been able to sell the precise geo-location data unless a consumer expressly opted-in to that sale. Of course, a consumer would be extremely unlikely to do so. Clear mandates, like those embodied in L.D. 946, protect consumers ***before*** they are harmed. It is past time to take serious steps to curtail these abusive and unscrupulous practices and to close demonstrated gaps in consumer protection law.

Opponents of L.D. 946 claim it would restrict their First Amendment rights to communicate with their customers. This is simply not true. In the first instance, nothing in this bill restricts the ability of providers to market to their customers or to allow others to do so. They may continue to monetize their users' attention just like anyone else. Further, there is an explicit carve-out that allows broadband providers to use customer personal information to advertise their own products. Finally, broadband providers may continue to use the information however they please, so long as they obtain consumer consent. There is nothing in this bill that will prevent the legitimate use of data by broadband providers.

L.D. 946 would give consumers control over the wealth of data collected and used by ISPs and would place an affirmative duty on broadband providers to take reasonable measures to secure that data. Consumers deserve to be protected, and to have control over their own data, despite unfounded claims that they might become "confused" with their newfound abilities. Consumers know the difference between

their broadband provider and an online company like Amazon or Google. Shortly after Congress repealed the FCC's 2016 broadband privacy rules, consumers were up in arms and confronted members of Congress at local Town Halls. Consumers didn't care that the rules didn't apply to all actors in the Internet ecosystem; they were upset that Congress had eliminated the one law that had given them control over their data.

Providing consumers with straightforward protections is more necessary now than when this Committee heard testimony on a similar bill, L.D. 1610, in May 2017. Then, broadband providers could make a colorable argument that the FCC still retained authority over their privacy practices under Section 222 of the Communications Act of 1934. But that argument dissolved after the broadband providers successfully lobbied to have the Trump FCC abdicate its responsibility to regulate broadband markets and overturn those rules in December 2017. Since then, the same ISPs have tried to bully states that dare to introduce laws to prevent any meaningful legislation from passing.[14]

The broadband provider's shell game is clear: if every state were to pass a law, ISPs will be forced to comply with a "patchwork" of different consumer privacy protections. A federal framework is therefore preferable. This bad-faith argument would hold more water if broadband companies were not consistently the driving force in repealing federal broadband rules—whether for net neutrality or for privacy.[15] Even if this two-step passed the smell test, the reality is that companies

[14] Jon Brodkin, *AT&T/Verizon Lobbyists to "Aggressively" Sue States That Enact Net Neutrality*, ARS TECHNICA (Mar. 27, 2018), https://arstechnica.com/tech-policy/2018/03/attverizon-lobbyists-to-aggressively-sue-states-that-enact-net-neutrality.
[15] Chris Mills, *Never Forget How Much Money Comcast, Verizon and AT&T spent to Crush Net Neutrality*, BGR (July 12, 2017), https://bgr.com/2017/07/12/net-neutrality-explained-internet-day-of-

comply with different state laws all the time—including tax laws, laws governing corporations, telecommunications laws and yes, privacy and consumer laws. The solution to the alleged "patchwork" problem is for the companies to comply with the highest level of privacy protection a state requires, and the ISPs have repeatedly demonstrated their ability to do this.

Broadband providers have been incredibly successful complying with state laws *in Maine*. Many of the laws in their fearsome "patchwork" have come directly from this body. In fact, Maine is a national leader in protecting the privacy of its residents. It has passed laws protecting prescription data,[16] health data,[17] library records,[18] and data on victims of domestic violence.[19] This legislature passed one of the most comprehensive statutes requiring law enforcement to get warrants for cellphone information, including the content of messages[20] and location tracking data.[21] I urge you to continue that leadership by unanimously passing L.D. 946.

action-july-12 (telecommunications companies have spent $572 million lobbying the FCC and other agencies since 2008, more in that period than any other industry other than oil and pharmaceuticals.).
[16] 22 M.R.S. § 7245 et seq.
[17] 22 M.R.S. § 1711-C; 34 M.R.S. § 1207
[18] 27 M.R.S. § 121.
[19] 21-A M.R.S. § 122-A et seq.
[20] 16 M.R.S § 641 et seq.,
[21] 16 M.R.S. § 648 et seq.