ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

February 17, 2020

Members of the House Corporations Committee
Wyoming State Legislature
200 West 24th Street
Cheyenne, WY 82002

Re: HOUSE BILL NO. HB0101: Protection and privacy of online customer information.

Dear Members of the House Corporations Committee,

The Information Technology and Innovation Foundation (ITIF) wishes to comment on the recently introduced HB0101 regarding the protection and privacy of online customer information.[1] Founded in 2006, ITIF is an independent 501(c)(3) nonprofit, nonpartisan research and educational institute—a think tank. Its mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. ITIF's goal is to provide policymakers around the world with high-quality information, analysis, and recommendations they can trust.[2] We have been alarmed by recent initiatives by state legislatures to write rules affecting the Internet ecosystem, particularly state rules affecting broadband privacy, such as House Bill 0101.

This bill is flawed for three main reasons: first, there is no justification for narrow privacy laws that apply only to broadband providers. Second, the bill appears intended to simply maximize user privacy without balancing other interests and would have a negative impact on potential innovative uses of data. Third, privacy regulation should be a uniform endeavor across all fifty states. Even if one is not happy with the current oversight of privacy best practices by the Federal Trade Commission, we should avoid a privacy Frankenstein that would result from numerous state laws and prefer a single law at the federal level.

BROADBAND PROVIDER ACCESS TO DATA DOES NOT JUSTIFY SECTOR-SPECIFIC LAWS

The bill introduced by Representative Yin proposes very strict data privacy regulations that would apply only to broadband Internet access providers (also referred to as Internet Service Providers or ISPs), and not other

[1] Legislation 2020, "HB0101 - Protection and privacy of online customer information." State of Wyoming 65th Legislature, https://www.wyoleg.gov/Legislation/2020/HB0101.
[2] *See* About ITIF: A Champion for Innovation, https://itif.org/about.

actors in the online ecosystem.[3] In order to justify sector-specific privacy rules, one would expect an unusually high risk of consumer harm from broadband data being shared or used inappropriately. Today, the only sector-specific privacy rules are for areas of the economy where there exists a heightened risk of harm from the disclosure of sensitive personal information, such as healthcare or financial services. As a factual matter, that heightened risk does not exist with regard to broadband providers: their access to data is neither unique nor comprehensive.

In his report, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, Professor Peter Swire lays out a number of ways in which broadband providers generally have less visibility into users' online activity compared to other actors in the Internet ecosystem.[4] Broadband providers do not have anything near comprehensive access to consumer data for several reasons. One of the most prominent limitations on broadband providers' access to data is the growing use of encryption online. When websites use encrypted protocols, the broadband provider is unable to access the content of consumer activity online. Because of encryption, ISPs are generally only able to access high-level metadata, which inherently has a lower risk of harm from being used or shared compared to the contents of emails, social media history, or specific search queries, for example. All of the top 10 websites now encrypt their traffic by default or on user log-in, and 42 of the top 50 do as of 2016.[5] And encryption adoption on the web is on a sharp, recent rise: At the start of 2019, 87 percent of Web traffic was encrypted, compared to just 53 percent in 2016.[6]

Encryption functionally obscures most content (and virtually all sensitive content) from ISPs, meaning the case for heightened rules applied only to broadband providers is tenuous at best. The fact that consumers spread their Internet use over multiple broadband connections at home, work, and at various WiFi hotspots further reduces the risk of harm from any one provider's collection of information.

---

[3] The draft legislation applies only to providers of Broadband Internet Access Services. In other words, it applies only to those who provide the on-ramp to the Internet, and not the companies that provide Internet services that are accessed via the Internet, such as search, social media, cloud services, or other applications.

[4] Peter Swire, et al, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others,* The Institute for Information Security & Privacy, Georgia Tech, Feb 2016, http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf.

[5] Swire report at 28.

[6] Fahmida Y. Rashid, "Encryption, Privacy in the Internet Trends Report" *Duo Decipher* (Jun 2019) (reporting on Mary Meeker's "Internet Trends" report), https://duo.com/decipher/encryption-privacy-in-the-internet-trends-report.

Engineers have pointed out there is a significant gap between what information is technically available to Internet Service Providers (ISPs) and what is practically useful. Richard Bennett, a consultant with a thirty-year background in network engineering, points out that because of the numerous, diverse connections opened when a typical web page loads, "all the ISP can do with the all that information is guess what the important parts are…. As a practical matter, converting the raw information that ISPs can harvest from web requests … is a very difficult task."[7]

Internet service provider access to data is also not unique. As Jules Polonetsky, head of the Future of Privacy Forum, has put it, "[t]oday, data has been democratized"—large amounts of consumer data are already available to anyone with a credit card.[8] The ability to obtain data like that which broadband providers have access to is widely available and in no way unique to broadband providers. The proposed rules would lead to the strange and market-distorting result where broadband providers would not be allowed to share or use the exact same information that is readily available to others.

Moreover, ITIF research shows that all major broadband providers already offer consumers the ability to opt-out of existing targeted advertising programs, allowing consumers who are particularly sensitive to privacy concerns to not participate.[9] In line with existing FTC guidance, broadband providers all offer notice of the data that is collected and the option for consumers to opt out of practices they are uncomfortable with. What would change under HB0101, however, is the ability of ISPs to responsibly experiment with new ways of supporting the expensive deployment and maintenance of broadband networks.

Persistent confusion stems from the popular, but mistaken, belief that because broadband providers operate the network connecting users to the rest of the Internet, these providers have a special duty to protect consumers' online activities. But this "gatekeeper" model is the wrong way to think about broadband providers' relationship to consumer data. As the FTC explained in its 2012 Privacy Guidelines, although ISPs serve as intermediaries, giving consumers access to other services, "the Commission agrees that any privacy

---

[7] Richard Bennett, "FCC Confused About Privacy," *HighTech Forum*, http://hightechforum.org/fcc-confused-about-privacy/.
[8] Jules Polonetsky, "Broadband Privacy and the FCC: Protect Consumers from Being Deceived and from Unfair Practices," *Future of Privacy Forum* (March 2016), https://fpf.org/2016/03/11/13938/.
[9] *See* Doug Brake, Daniel Castro, & Alan McQuinn, Information Technology and Innovation Foundation, Broadband Privacy: The Folly of Sector-Specific Regulation, (2016), http://www2.itif.org/2016-broadband-privacy-folly.pdf.

framework should be technology neutral. ISPs are just one type of large platform provider" that have access to consumer data.[10]

THIS BILL DOES NOT BALANCE PRIVACY WITH OTHER INTERESTS

The proposed legislation would prevent the use, disclosure, or sale of a very broad range of ISP customer data. If we want to balance data privacy with continued innovation around data-fueled applications such as machine learning and artificial intelligence, we should prefer a more flexible regulatory model, such as that employed by the FTC today. The FTC today oversees fair competition—including all companies privacy policies—and has broad authority under Section 5 of the Fair Trade Act to take enforcement actions against unfair or deceptive trade practices.[11] The FTC also offers specific guidance when it comes to privacy, having put forth a single, comprehensive framework guided by three overarching principles: privacy by design, consumer choice, and transparency.[12]

By allowing flexibility for industry to develop best practices within these guidelines, and stepping in ex post where problems develop, the FTC does not have to predict the direction technological advancements or changes in business practices will take us. This allows firms to internalize or outsource different functions in fast-paced industries with a focus on efficiency rather than compliance. This type of privacy oversight, with rules that apply an even, light-touch approach to different actors, would be a better environment for dynamic competition to occur across platforms. A uniform oversight framework, with low regulatory barriers to entry, would not only allow carriers to explore further entry into areas like advertising, but would avoid discouraging new entrants from providing broadband services.

Representative Yin's bill, on the other hand, would severely restrict the use of data by ISPs, functionally locking them into the predominant business model today, rather than allowing for experimentation with the potential for broadband offerings that exchange use of user data for a lower subscription price, sale of high-level metadata for security analytics, or outsourced machine-learning network optimization. It would restrict

---

[10] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," at 56 (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
[11] 15 USC § 45.
[12] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," March 2012, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

the ability of ISPs to share information with third-party researchers and academics, denying a possible source of valuable information with relatively little upside.

There is likely room to improve on the FTC oversight framework in place today, but such a bill should carefully balance consumer privacy with other objectives, such as the need for sources of data that can fuel innovation or increase competition in targeted advertising. Furthermore, such a law should apply uniform rules throughout the nation.

DATA PRIVACY LAWS SHOULD BE FEDERAL, AND APPLY UNIFORMLY THROUGHOUT THE NATION

Privacy policies impact a substantial portion of the Internet economy and should be developed at a national level through Congress. A national framework for digital economy rules would ensure the same protections for all U.S. residents, minimize transaction costs for businesses, enable opportunities to innovate, and increase efficiency in the policymaking process.[13]

With the expansion of the digital economy, there is a growing disjuncture between local governance and the national and international nature of the Internet. This is obviously true with cloud-based services and web destinations. But technology is driving a reduced dependence on the particular jurisdiction of broadband networks as well, undermining justification for particularized rules for each state.[14]

States enacting unique or conflicting rules on privacy—let alone privacy rules unique to the ISP sector—would create a patchwork that unnecessarily drives up compliance costs that ultimately must be recouped from end-users. Often large regional or national companies are forced to save on compliance and conform to the most restrictive rules. States acting individually on data privacy would create a race to the bottom. I urge you to reject this bill.

---

[13] Alan McQuinn and Daniel Castro, "The Case for a U.S. Digital Single Market and Why Federal Preemption Is Key," ITIF (Oct 2019), https://itif.org/publications/2019/10/07/case-us-digital-single-market-and-why-federal-preemption-key.

[14] Doug Brake, "National Networks Need National Policies," ITIF (Nov. 2017), https://itif.org/publications/2017/11/09/national-networks-need-national-policies.

ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Sincerely,

Doug Brake
Director of Broadband and Spectrum Policy
Information Technology and Innovation Foundation