Promoting Responsible ISP Values and Improving Subscriber Privacy (PRIV-ISP) Act of 2018

Joe Cavanaugh, Craig Cheney, Jeff Gary, and Sharon Kim

April 2018

Promoting Responsible ISP Values and Improving Subscriber Privacy (PRIV-ISP) Act of 2018

Table of Contents

1 Executive Summary

2 ISPs collect sensitive consumer information with no meaningful restraints on privacy, data collection, or use.

2.1 ISPs completely control user access to the Internet.

2.2 Because of their unique position in the Internet ecosystem, ISPs have detailed access to the online activities of their users.

2.3 Mobile and Internet of Things (IoT) devices provide ISPs with more, not less, information

2.4 Users cannot avoid ISP data collection practices and cannot easily switch providers

3 The PRIV-ISP Act would protect consumers by providing choice on who gets data, what data is given, and how that data is used.

3.1 The current state of the law insufficiently anticipates and resolves the problems consumers face with ISPs.

3.2 Providing clear disclosures and opt-in consent would allow consumers to have meaningful choice over how ISPs collect, use, and share their information

3.3 Unbundling the local loop would increase ISP competition and benefit consumers.

3.4 Prohibiting ISPs from offering incentives to influence consumers' consent would protect consumers from being unfairly coerced into foregoing their privacy.

4 Conclusion

1 Executive Summary

Imagine one person could comb through all your Internet activity. That person knows what websites you visit, the music you listen to, and the shows you watch. That person knows when you wake up, where you are, and how long you take to brush your teeth. That person wants to sell your information.

That person is your ISP, the mostly invisible company you pay monthly to connect you to the Internet. ISPs—companies such as Comcast, Verizon, and AT&T—see virtually everything you do online. They own the wires that go from your house to the rest of the web, and they see the information you put on those wires. Unlike every other web service, which only see you when you visit their sites, ISPs see every request you make on the Internet. Further, because ISPs invest significantly in building their physical networks, most consumers have little or no choice of which ISP gets their most private information.[1] Put simply, your ISP sees virtually everything you do on the Internet and you have very little control over how it uses that information.

While ISPs have traditionally operated as the simple conduit to the Internet, they are increasingly leveraging their unique and privileged position to monetize information about their users by selling targeted advertising. Some seek to push the cost onto consumers, such as AT&T, which in 2013 forced users to choose: pay more, or allow us to sell all of that information to advertisers.[2] Some take a more direct route, and simply buy advertising companies that can make use of the constant stream of personal information ISPs collect.[3] Despite these clear changes in ISPs' business and their increased power in the Internet ecosystem, consumers are left with little, if any, meaningful protection against ISPs selling their data.

The Promoting Responsible ISP Values and Improving Subscriber Privacy (PRIV-ISP) Act of 2018 responds to the uniquely powerful place ISPs occupy in the Internet ecosystem and their recent changes in how they treat that model. To provide consumers with meaningful control over their personal information, therefore, the PRIV-ISP Act would enact three concurrent concurrent: First, it requires ISPs to provide competitors with access to their local infrastructure. Second, it requires ISPs to obtain affirmative and informed consent from their users before collecting and using personal information. Last the Act prohibits ISPs from withholding or modifying service based on those consumer choices. Taken together, these provisions provide a comprehensive remedy to consumers and allow them to control which ISP gets their information, what information that ISP gets, and how the ISP can use it.

---

[1] Kate Cox, *Here's What the Lack of Broadband Competition Looks Like on a Map*, Consumerist (Mar. 7, 2014).
[2] Jon Brodkin, *AT&T to End Targeted Ads Program, Give All Users Lowest Available Price*, Ars Technica (Sept. 30, 2016).
[3] Todd C. Frankel, Brian Fung & Hayley Tsukayama, Why Verizon Wants to Buy an Ailing Yahoo in $4.8B Deal, Wash. Post (July 25, 2016).

2 ISPs collect sensitive consumer information with no meaningful restraints on privacy, data collection, or use.

2.1 ISPs completely control user access to the Internet.

Internet Service Providers ("ISPs") occupy a privileged and unique place on the Internet. Because ISPs provide the technical means for a user to connect to web services (such as social media or search engines), ISPs see virtually all traffic from their users.[4] This favorable vantage point that ISPs occupy gives them broad access to consumer information: ISPs are able to see at least part of every single packet—or piece of information—sent and received by every device from every ISP customer.[5] No other entity in the Internet ecosystem possesses that level of access.[6]

ISPs can maintain this privileged position because they own and operate the physical infrastructure that users require to connect to the Internet.[7] Because this infrastructure is costly to build, competition is scarce between ISPs, and most consumers have little, if any, choice between ISPs.[8] Indeed, nearly 50% of American households are only served by a single ISP.[9] Moreover, even when consumers do have choice, switching costs may be prohibitively high.[10] ISPs essential role in Internet service and the lack of competition in the market gives each ISP tremendous power over its users.

2.2 Because of their unique position in the Internet ecosystem, ISPs have detailed access to the online activities of their users.

Users send an immense amount of information over the Internet. One of the most common actions is a user visiting a website. To load a webpage (i.e. "www.mit.edu"), a user must request it through their ISP, and in response, receive the desired website, which is displayed in the user's browser. In order for the website to load correctly, the user must send information from her computer to the ISP; for example, languages, location, browser preferences, and other online configurations.[11] Because all of this information is routed through the Internet and because the

---

[4] Aaron Rieke, et al., What ISPs Can See, (Upturn, 2016).
[5] *Id.*
[6] Statement of Paul Ohm Professor, Georgetown University Law Center and Faculty Director, Georgetown Center on Privacy and Technology Before the Subcommittee on Communications and Technology Committee on Energy and Commerce U.S. House of Representatives June 14, 2016, http://docs.house.gov/meetings/IF/IF16/20160614/105057/HHRG-114-IF16-Wstate-OhmP-20160614-U1.pdf.
[7] Jon Brodkin, *One Big Reason We Lack Internet Competition: Start an ISP is Really Expensive*, Consumerist (April 6, 2014).
[8] *Id.*
[9] FCC 2016 Broadband Progress Report ("Approximately 51 percent of Americans have one option for a provider of 25 Mbps/3 Mbps fixed broadband service."); Hal Singer, et al., Assessing the Impact of Removing Regulatory Barriers on Next Generation Wireless and Wireline Broadband Infrastructure Investment (Economists Incorporated, 2017); Kate Cox, *Here's What the Lack of Broadband Competition Looks Like on a Map*, Consumerist (Mar. 7, 2014).
[10] Prepared Remarks of FCC Chairman Tom Wheeler, The Facts and Future of Broadband Competition, 1776 Headquarters, Washington, D.C., Sept. 4, 2014
[11] Annie Edmunson, *Oblivious DNS: Plugging the Internet's Biggest Privacy Hole*, Freedom to Tinker (Apr. 2, 2018).

ISP provides the Internet connection, the websites a user requests are, more or less, viewable to the ISP. Significantly, ISPs are the only entity in the Internet ecosystem that see all of each user's traffic in this manner.

The technical information sent by users provides ISPs with incredible insight into user activity. Information on the user's computer and personal preferences can be read and collected by the user's ISP as requests are made. This information *about* the communications—collectively referred to as "metadata"—can provide significant information about users. An ISP could learn, for instance, that a user is a Spanish-speaker from New York who reads the *Huffington Post* and enjoys basketball. In aggregate, metadata, which is rarely encrypted, can even provide highly sensitive information about a user's sexual preferences, medical condition, financial affairs, or religion.[12] ISPs can even use metadata to make inferences about content they may not otherwise have access to. For instance, an ISP can see the size of information being sent to and from a user's browser. From this, an ISP can determine how users are interacting with particular websites (i.e. a heavy movie viewer), and create profiles around those traits.[13]

ISPs can use this comprehensive information to create personal, detailed profiles about its users. Unlike online advertisers, which may only know that a person with particular tastes is visiting their website, ISPs can tie that information directly to a user, and connect that information to the user's plan type, payment history, personal identification information, and even address. The combined access to browsing information and personal identifiers gives ISPs the unique ability to create detailed and persistent behavioral profiles on each of their users that other companies simply do not have. Startlingly, ISPs have already demonstrated a willingness to create exactly this type of information. In 2012, Verizon's notorious "supercookie" tied customer browsing information to billing and account information and sold it to advertisers.[14]

2.3 Mobile and Internet of Things (IoT) devices provide ISPs with more, not less, information

Rather than increasing privacy, the adoption of mobile devices is likely to further enable ISP data collection. The number of households who connect to the Internet solely through their mobile devices is growing and expected to continue increasing.[15] Despite this, over 95% of all unencrypted web traffic comes from mobile devices, many of which cannot support updates enabling greater security.[16] Compounding this issue, ISPs can see traffic from all devices connected to their network, and in some cases, monitor traffic irrespective of which network is used.[17] In users' homes, ISPs can observe browsing patterns across multiple devices and determine which devices are used, how often, and for what.[18] Outside the home, the increasing

---

[12] Aaron Rieke, et al., What ISPs Can See, (Upturn, 2016).
[13] Narayanan, Arvind, and Dillon Reisman. *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*. June 27, 2016.
[14] Consent Decree: Verizon Wireless re: Supercookie (Mar. 27, 2016), https://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0307/DA-16-242A1.pdf.
[15] *Mobile Factsheet,* Pew Res. Ctr. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/.
[16] Google Transparency Report, 2018.
[17] Jacob Kastrenakes, *FCC Fines Verizon $1.35 Million over 'Supercookie' Tracking*, Verge (Mar. 7, 2016), https://www.theverge.com/2016/3/7/11173010/verizon-supercookie-fine-1-3-million-fcc.
[18] Nick Feamster, *What Your ISP (Probably) Knows About You*, Freedom to Tinker (Mar. 4, 2016).

availability of WiFi hotspots gives ISPs unprecedented insight into mobile subscribers as they travel.[19] The rise of mobile, far from stifling ISP's data collection, is enabling it like never before.

The ubiquity and increasing sensitivity of "Internet of Things" (IoT) devices also enables ISP data collection. IoT devices, which typically connect to the which now include a range of products like lightbulbs, coffee makers, children's toys, TVs, toothbrushes, sex toys, and even beds,[20] have further enabled ISPs to gain sensitive in-home activities about their customers. ISPs can see, for example, when a light bulb is on or off, when a smart speaker is playing music, what TV show is on, and when you brush your teeth.[21] The enormous amount of data sent to ISPs about household tasks and activities allows ISPs access into the most private reaches of American life.

2.4 Users cannot avoid ISP data collection practices and cannot easily switch providers

Despite the immense amount of information ISPs can extract from their customers on their computers, their mobile devices, and even their light bulbs, consumers have little—if any—ability to avoid having their information collected. Collection, use, and sharing practices are largely governed by "take it or leave it" contracts, and when ISPs do have opt-out mechanisms, they do not fully stop ISPs from collecting and using sensitive data.[22] In some cases, ambiguous language in privacy policies provides ISPs with room to sell information on their customers despite opt outs.[23] Customers do not have the ability to negotiate these terms or—in many cases—to avoid the collection and retention of the data their ISP compels them to provide.

Even if customers are deeply unsatisfied with the privacy options presented by their ISP, they may not be able to switch easily or at all. The physical infrastructure owned and operated by ISPs is expensive and time-consuming to build: once one ISP has buried its wires in a neighborhood, others are unlikely to follow suit. This leaves many Americans underserved and with few or no alternatives to their ISP.[24]

To remedy consumer's lack of control over their data and inability to choose between ISPs, legislation should mandate robust disclosure and affirmative consent requirements, and stimulate competition between ISPs by requiring incumbent ISPs to lease their physical infrastructure to potential competitors.

---

[19] As of 2015, Comcast offered 10 million WiFi hotspots; users connect to them over 3.6 billion times. Nick Feamster, *What Your ISP (Probably) Knows About You*, Freedom to Tinker (Mar. 4, 2016).
[20] Kashmir Hill & Surya Mattu, *The House that Spied on Me*, Gizmodo (Feb. 7, 2018), https://gizmodo.com/the-house-that-spied-on-me-1822429852.
[21] *House that Spied on Me*; *see also* Noah Apthorpe et al., *Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic*, https://arxiv.org/pdf/1708.05044.pdf
[22] Libby Watson, *Want to Stop Your Internet Provider From Selling Your Browsing Data? It Ain't Easy*, Gizmodo (Apr. 5, 2017), https://gizmodo.com/want-to-stop-your-internet-provider-from-selling-your-b-1793902371.
[23] *Want to Stop Your Internet Provider From Selling Your Browsing Data?*
[24] Hal Singer Report.

3 The PRIV-ISP Act would protect consumers by providing choice on who gets data, what data is given, and how that data is used.

3.1 The current state of the law insufficiently anticipates and resolves the problems consumers face with ISPs.

Due to recent restrictions on the Federal Communications Commission's (FCC) authority over ISPs, as well as the federal government's current deregulatory posture,[25] privacy protections must come from more local sources. In October 2016, the Federal Communications Commission (FCC) adopted rules limiting the extent to which ISPs could collect and use consumer information.[26] The rules required ISPs to obtain opt-in consent for certain types of information, regulated the use of consumer information based on its sensitivity, and provided other safeguards for consumers.[27] These rules, which marked the strongest-yet push to regulate the collection and use practices of ISPs, were overturned by Congress in March 2017[28] under authority of the Congressional Review Act,[29] which allows Congress to overturn agency rules through a majority vote in each chamber.[30] The law also forbids the affected agency from promulgating any rules "substantially similar" to those overturned by Congress in this manner unless specifically authorized by Congress to do so.[31] This incident, coupled with the historically low passage rate of legislation in the current Congress[32] and its legislative inaction on other pressing Internet issues, suggests that federal legislation to protect consumers will not be forthcoming.

The Promoting Responsible ISP Values and Improving Subscriber Privacy (PRIV-ISP) Act of 2018 is a state legislative proposal designed to proactively address the aforementioned privacy issues and improve consumers' privacy controls at the local level. States and municipalities have demonstrated their interest and willingness to regulate commercial behavior by ISPs. Following the repeal of the FCC's Net Neutrality rules, several states, including Washington and New York, enacted their own rules despite claims from the FCC that states were precluded from doing so.[33] Given this activism at the state level, the PRIV-ISP Act presents a model for how states can continue their role in improving consumers' Internet privacy.

---

[25] *See* Jim Puzzanghera, *FCC Clears Way for Big TV Mergers, Eases Broadband Price Limits*, L.A. Times (Apr. 20, 2017), http://www.latimes.com/business/la-fi-fcc-deregulation-20170420-story.html; Brian Fung, *The FCC Just Voted To Repeal Its Net Neutrality Rules, In a Sweeping Act of Deregulation*, Wash. Post (Dec. 14, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/12/14/the-fcc-is-expected-to-repeal-its-net-neutrality-rules-today-in-a-sweeping-act-of-deregulation/?utm_term=.0f4ad55c2ec2.

[26] Fed. Communications Comm'n, *FCC Adopts Broadband Privacy Rules* (Oct 27, 2016), https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules.

[27] *See* FCC Fact Sheet.

[28] Senate Joint Resolution 34 (Public Law 115-22).

[29] https://www.npr.org/2017/03/28/521831393/congress-overturns-internet-privacy-regulation

[30] 5 U.S.C § 801, Congressional Review. https://www.law.cornell.edu/uscode/text/5/part-I/chapter-8.

[31] *Id.*

[32] GovTrack, Statistics and Historical Information: Bills by Final Status. https://www.govtrack.us/congress/bills/statistics.

[33] Ceclia Kang, *Washington Governor Signs First State Net Neutrality Bill*, N.Y. Times (Mar. 5, 2018), https://www.nytimes.com/2018/03/05/business/net-neutrality-washington-state.html; Executive Order, New York State (Gov. Cuomo), https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/EO_175.pdf.

3.2 Providing clear disclosures and opt-in consent would allow consumers to have meaningful choice over how ISPs collect, use, and share their information

The PRIV-ISP Act of 2018 presents a two-part legislative solution to addressing consumer privacy concerns regarding ISPs, beginning with a mandate that ISPs provide an opt-in consent mechanism to customers, coupled with a robust disclosure policy. Under the Act, ISPs will be required to disclose to customers exactly what data will be collected, the duration over which the data will be gather and stored, who has access to the collected data, and how the data will be used. Furthermore, the PRIV-ISP Act stipulates that the information must be clearly presented in the customer's language of choice (to a reasonable extent), and use simple terms that can be understood by customers regardless of their technical background. When provided this information, customers have a reasonable ability to make an informed decision as to how their personal information is used by the ISP.

Alongside of the disclosure policy is an opt-in consent policy, whereby users must give affirmative consent before any of the practices described in the disclosure can take effect. Favoring an opt-in consent policy over an opt-out consent policy provides stronger privacy protections to customers. By default, an opt-in policy leaves the customer protected when no customer action is taken, whereas customer intervention is required to gain privacy protections with an opt-out policy. Additionally, with an opt-in policy, when requiring customers to take action before any data is stored, there exists a higher chance that customers will actually read the disclosures of the privacy policy, and be aware of details of the policy. In an opt-out situation, not only is action required by the customer to obtain privacy protection, but action is also required by the customer to gain insight into the details of how their data is being used. In this sense, an opt-out policy is, by default, signing customer up without them knowing what they are signing up for. It is clear to see from this, that an opt-in consent policy affords more protections "out of the box" to users.

Additionally, under the PRIV-ISP Act, ISPs are prohibited from withholding or changing services, charging additional fees, or offering discounts, based on whether or not a customer has consented to the private data usage policy. This prevents ISPs from structuring their service plans such that customers who have not consented are discriminated against.

3.3 Unbundling the local loop would increase ISP competition and benefit consumers.

The second major provision of the PRIV-ISP Act is a requirement that ISPs open up their physical infrastructure to competing ISPs at a fair market value. This practice is colloquially known as "unbundling the local loop".

ISPs must route physical cables, or the "local loop", to end-users in order to provide internet services. In most cases in the US, the ISP that is providing a customer with internet service also owns the physical infrastructure.[34] If the company that provides the internet routing services also owns the physical infrastructure it is referred to as a "bundled local loop." Due to the significant financial burden of laying down the physical infrastructure associated with internet connections,

[34] Kate Cox, *Here's What the Lack of Broadband Competition Looks Like on a Map*, Consumerist (Mar. 7, 2014).

such as fiber optic lines, it often does not make sense for two ISPs to lay down wires to the same building. The result of this is that consumers have only one, or perhaps two, choices when it comes to ISPs. When consumers have no meaningful choice when it comes to picking an ISP, the ISPs significant leverage over their customers when it comes to business practices, especially those related to privacy. If a customer does not like the privacy practices of an edge provider, they can simple not use the service or switch to another provider. The same recourse does not exist with ISPs. Unbundling the local loop forces ISPs to lease out their physical infrastructure to competitors at a fair market value so the company that owns the cables is not necessarily the same company that provides internet routing services.

The PRIV-ISP Act allows states to the their contracting and leasing power with ISPs to require ISPs to unbundle the local loop and allow competitors to share infrastructure where practicable. A competitive marketplace for broadband could foster competition in privacy terms and use[35], so long as there is sufficient user demand. Unbundling also addresses the primary disagreement festering between those in favor of heightened regulations for ISPs and those opposed: that ISPs are different than edge providers. If ISPs were unbundled, the main barrier to consumer choice—physical unavailability of service—would be removed, closing the divide between ISPs and other online providers.

3.4 Prohibiting ISPs from offering incentives to influence consumers' consent would protect consumers from being unfairly coerced into foregoing their privacy.

Unlike edge providers such as Facebook, Twitter, and Google, gathering personal data about consumers is not part of the ISPs' core business model. Further, unlike these same edge providers, going through an ISP to obtain an Internet connection is a must, not a choice, for the typical American consumer. ISPs should therefore be prohibited from forcing customers to choose between their privacy and paying additional fees for this essential service they provide.

This provision would protect consumers from being forced to divulge personal details about themselves to ISPs that they would otherwise not like to provide, while simultaneously allowing them to keep their access to the Internet. Therefore, a consumer could choose to keep their access to their Internet without sacrificing their privacy.

4 Conclusion

ISPs have outsized control over the private information of virtually every American. Technical fixes and market solutions have failed to remedy this imbalance and are likely to continue to do so. Legislative solutions provide the pathway forward. The PRIV-ISP Act, geared towards the technical realities of the Internet and the ISP market, would implement two commonsense principles: First, ISPs should ask consumers before collecting and using their private information. Second, ISPs should compete for consumers' business by providing the best service possible. These two shifts would provide consumers with meaningful choice on who handles their sensitive information and how it is used.

---

[35] Jeff Dunn, *American Has an Internet Problem—But a Radical Change Could Save It*, Bus. Insider (April 23, 2017)