Issue Brief: State Broadband Privacy Legislation

August 2019

Table of Contents

Executive Summary 3

I. Introduction 4

II. Policy Background 6

III. The Rationale for State Broadband Privacy Legislation 7

A. ISPs Occupy a Unique Role in Consumers' Lives 7

B. Consumers Care About Their Privacy 9

C. Non-Competitive Market Prevents Consumer Agency 10

D. The Federal Trade Commission's Protections are Insufficient 11

E. Low-Implementation Costs of State Broadband Rules 12

F. Broadband Privacy Continues to Allow ISPs to Compete in the Edge Provider Market 12

IV. Broadband Privacy Rules Should Not Allow ISPs to Penalize Consumers 13

V. Specific Elements of State Broadband Privacy Proposals 15

VI. Contact Details and More Information 17

Executive Summary: What is Broadband Privacy and Why Do Your Constituents Need It?

In the same way phone companies cannot listen in on your phone calls and mail carriers cannot read your mail or open your packages, internet service providers (ISPs) should not be able to snoop on and profit off of your internet traffic. Period. Consumers already pay steep monthly subscription charges to their ISP; they should be entitled to a reasonable expectation of privacy in the use of these services.

That is broadband privacy. But it does not exist today because Congress repealed comprehensive broadband privacy protections issued by the Federal Communications Commission in 2016. In response, several states have introduced broadband privacy bills to protect their residents. As a state or local lawmaker, you can protect the online privacy of your constituents by introducing and passing strong broadband privacy protections.

Because all of a consumer's online activities flows through them, ISPs have access to **enormous amounts of highly sensitive personal and business data**, and they can see nearly everywhere their customers go online and what they do.

Some of the personal information that ISPs have access to includes:

- geolocation data, which can be used to determine precisely where you live and travel to, and when;
- details about your health and financial status;
- your web browsing and app usage history; and
- your Social Security number.

ISPs can even delve into and extract information from the contents of your communications, including email, social media postings, and instant messages if they are not encrypted.

ISPs have the ability to assemble a detailed and highly personal dossier of your life. Communications with doctors or lawyers, political activities, job inquiries, dating site history—**essentially anything you do or express on the internet that you would like to keep private**, could all be examined and used by your ISP.

Consumers have **no choice** but to use an ISP to access the internet and thus share personal data with that provider.

We urge state and local lawmakers to protect the privacy of their constituents, as well as their own, by introducing and passing strong broadband privacy rules.

Consumer Reports[1] developed this issue brief to help state legislatures enact broadband privacy legislation to protect the confidentiality of Americans' internet usage and online communications. This brief will:

- explain what broadband privacy legislation would do;
- describe how the federal government has abdicated responsibility to the states;
- demonstrate why such protections are needed; and
- recommend specific elements that should be included in any broadband privacy proposal.

I. Introduction

Americans have a fundamental right to privacy. Every day they rely on local, state, and federal laws to protect that right when it comes to the security of their correspondence through the mail, telegram, and telephone. But, despite the fact that Americans now depend on the internet for online banking, accessing employment and health information, social networking, directions, and myriad other tasks,they do not have the same protections for their online information and activities.

Consumers should not have less privacy and security just because our systems of communication have evolved to include the internet. However, the repeal of the Federal Communications Commission's (FCC) broadband privacy rules has resulted in a system where online communications are afforded less privacy protection than traditional telephonic or paper communications.

Although a comprehensive federal data privacy law and the implementation of state-level privacy laws are critical, some industries, like internet service providers (ISPs), merit stronger protections. ISPs have unique insight into customer activity because they provide internet service—for which they charge customers a substantial subscription fee—giving them access to a vast amount of data from and about their consumers. While it may be possible for some consumers to take action to reduce their privacy risks once they are online, they have no choice but to use an ISP to access the internet and thus to subject all of their online data to snooping from the ISP. And consumers often have little or no choice over which ISP to use. All of an individual's traffic flows over that internet connection, traffic which can convey very personal information such as personal banking details, presence at home, physical ailments, physical location, race or nationality, religion, and sexual

[1] Consumer Reports is the world's largest independent product-testing organization. It conducts its advocacy work in the areas of privacy, telecommunications, financial services, food and product safety, health care, among other areas. Using its dozens of labs, auto test center, and survey research department, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

preference.[2] Even when traffic is encrypted, ISPs still know the sites and services their customers use. Due to the unfettered access ISPs have to consumer information and the sensitive nature of that information, a broadband privacy law should restrict ISPs' secondary use of consumers' data absent clear and affirmative permission from the individual.

In addition to their unique role, ISPs deserve unique treatment due to their status as a necessary utility. Consumers depend on the internet to conduct myriad tasks and should be protected by higher requirements for ISPs based on this unique role, the lack of market competition and consumer choice, and their status as a necessary utility.

Furthermore, ISPs have a track record of taking advantage of the lack of controls on their activities to violate consumers' expectations of privacy in a number of ways. For instance, ISPs have placed undeletable, undetectable cookies[3] or pre-installed software on consumers' phones in order to track their activity on the device,[4] sold consumer data to marketers,[5] hijacked searches in order to direct traffic to business partners,[6] and snooped through individuals' web traffic in order to deliver ads.[7]

---

[2] *See What ISPs Can See*, UPTURN (Mar. 2016), https://www.teamupturn.com/reports/2016/what-isps-can-see.

[3] AT&T and Verizon used undetectable, undeletable "supercookies" to track all of a mobile customer's traffic and activity on their device. Consumers were unable to opt-out of this collection (at least initially) and could not delete these trackers. Jacob Hoffman-Andrews, *Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls*, ELEC. FRONTIER FOUND. (Nov. 3, 2014), https://www.eff.org/deeplinks/2014/11/verizon-x-uidh; Elizabeth Weise, *AT&T Ends Tracking of Customers by "Supercookie"*, USA TODAY (Nov. 14, 214), https://www.usatoday.com/story/tech/2014/11/14/att-supercookies-tracking/19041911/.

[4] AT&T, Sprint, and T-Mobile all used pre-installed software in order to record users' traffic and activities on their mobile devices. The use of these trackers also allowed the ISP to see encrypted traffic as well. Trevor Eckhart, *What is Carrier IQ?*, ANDROID SEC. TEST (2011), http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/.

[5] ISPs are now building out their own advertising networks in order to use the detailed data they have on users in-house. However, there's evidence that ISPs can and have sold location, demographic, and browsing history data to marketers. Kate Kaye, *The $24 Billion Data Business that Telcos Don't Want to Talk About*, ADAGE (Oct. 26, 2015), http://adage.com/article/datadriven-marketing/24-billion-data-business-telcos-discuss/301058/.

[6] "The hijacking seems to target searches for certain well-known brand names only. Users entering the term "apple" into their browser's search bar, for example, would normally get a page of results from their search engine of choice. The ISPs involved in the scheme intercept such requests before they reach a search engine, however. They pass the search to an online marketing company, which directs the user straight to Apple's online retail website.
More than 10 ISPs in the US, which together have several million subscribers, are redirecting queries in this way." All the ISPs cited by this report have halted this practice. Although the ISPs continued to intercept "some queries—those from Bing and Yahoo—but [passed] those searchers onto the relevant search engine rather than redirecting them." Jim Giles, *US Internet Providers Hijacking Users' Search Queries*, NEWSCIENTIST (Aug. 9, 2011), https://www.newscientist.com/article/dn20768-us-internet-providers-hijacking-users-search-queries/.

[7] Three ISPs have been known to do this: AT&T, Charter, and CMA. AT&T snooped on web traffic for some of their paid WIFI hotspots and then inserted ads based on the browsing data. Jonathan Mayer, *AT&T Hotspots: Now with Advertising Injection*, WEBPOLICY (Aug. 25, 2015), http://webpolicy.org/2015/08/25/att-hotspots-now-with-advertising-injection/. Charter also snooped and placed ads but did so for some of its broadband customers. Nate Anderson, Charter "Enhances" Internet Service with Targeted Ads, ARSTECHNICA (May 13, 2008), https://arstechnica.com/uncategorized/2008/05/charter-enhances-internet-service-with-targeted-ads/.And the smaller ISP, CMA, also served ads in this fashion. Phillip Dampier, *ISP Crams Its Own Ads All Over Your Capped Internet Connection; Banners Block Your View*, STOP THE CAP! (Apr. 3, 2013), http://stopthecap.com/2013/04/03/isp-crams-its-own-ads-all-over-your-capped-internet-connection-banners-block-your-view/.

Consumers should feel confident that their ISPs are not rifling through their internet behavior to build up behavioral profiles about them. In addition, consumers desire the consumer protections the FCC rules would have provided. For these reasons, state and local governments should reinstate broadband privacy rules for their residents in order to protect their privacy and security.

II. Policy Background

In October 2016, the FCC passed rules to protect consumers' broadband privacy. These rules required ISPs to obtain their customers' affirmative consent before using and disclosing their web browsing history, application usage data, and other sensitive information for marketing purposes and with third parties. Historically, ISPs had not snooped on user behavior to target ads, but some were starting to explore this business model due to ambiguity in the law's protections.[8] In addition to giving consumers control over their personal information, the rules required ISPs to be transparent about their privacy practices in a simple and comprehensible way. The rules also created a breach notification regime that would have required ISPs to inform their customers when their information has been accessed by unauthorized parties and could cause harm.[9]

> "Internet service providers like Comcast and AT&T have been trying to get rid of these rules since the day they were approved, and the Senate just handed them a big victory...Consumers have a fundamental right to privacy. This move by the Senate is a huge step in the wrong direction, and it completely ignores the needs and concerns of consumers."
>
> *—Jonathan Schwantes on the rollback of the FCC Broadband Privacy Rules by the U.S. Senate, March 23, 2017*

Despite Americans' desire for these protections,[10] in March 2017, the US Congress voted to repeal the rules with a resolution of disapproval under the Congressional Review Act (CRA)—thereby preventing the FCC from ever passing a rule in "substantially the same form" in the future.[11]

---

[8] Timothy B. Lee, *Congressional Republicans Just Voted to Let ISPs Sell Your Browsing History to Advertisers*, VOX (Mar. 28, 2017), https://www.vox.com/new-money/2017/3/28/15089396/house-republican-privacy-bill.

[9] Historically, ISPs had not used subscriber data for advertising purposes, but in recent years many of the large ISPs began to build the capacity to monetize personal user data. Matt Keiser, *For Telecoms, The Adtech Opportunity is Massive*, EMARKETER (Jan. 18, 2017), https://www.emarketer.com/Article/Telecoms-Ad-Tech-Opportunity-Massive/1015052; *see* Anthony Ha, *Verizon Reportedly Closes in on a Yahoo Acquisition with a $250M Discount*, TECHCRUNCH (Feb. 15 2017), https://beta.techcrunch.com/2017/02/15/verizon-yahoo-250-million/.

[10] *See infra* § Consumers Care About Their Privacy.

[11] 5 U.S.C. § 801(b)(2).

Despite industry claims to the contrary, the roll back of these broadband privacy protections under the CRA is a significant loss for all Americans.[12] Under the rules, consumers would have had control over what happens to their private information. Now they do not.

III. The Rationale for State Broadband Privacy Legislation

Due to the repeal of the FCC's broadband privacy rules, there is no federal authority that is acting, or can act, to enact rules to limit ISP surveillance of customer communications for marketing or other commercial purposes. In the wake of the repeal, 24 states and the District of Columbia introduced legislation concerning residents' online privacy[13] and at least 19 states and the District of Columbia introduced bills that reinstate some or all of the protections contained within the FCC rules[14] in the 2017-18 legislative session. In 2019, 14 states and the District of Columbia are considering proposals to restrict how ISPs can collect and share consumer data.[15] In addition, Maine passed one of the strongest privacy laws in the country in July 2019 when they enacted their broadband privacy measure: An Act to Protect the Privacy of Online Customer Information.[16] Not only does this bill reinstate the protections that consumers would have had under the FCC's broadband privacy rules, but it also prohibits pay-for-privacy plans that the FCC rules would have allowed.

States have historically taken the lead on safeguarding individual privacy. For instance, since 2002, every state and the District of Columbia have enacted data breach notification laws while comparable bills have consistently stalled at the federal level.[17] The states should continue to lead in the area of broadband privacy as well.

A. ISPs Occupy a Unique Role in Consumers' Lives

With storage costs shrinking and their all-encompassing window into Americans' online behavior, ISPs can save indefinitely all of the data they collect, amassing year upon year of wide-ranging

---

[12] *Setting the Record Straight on Broadband Privacy*, CTR. FOR DEMOCRACY & TECH. (June 19, 2017), https://cdt.org/files/2017/06/2017-06-19-Broadband-Privacy-Myths-Facts.pdf.

[13] *Privacy Legislation Related to Internet Service Providers*, NAT'L CONFERENCE OF STATE LEGISLATURES (May 8, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers-2018.aspx.

[14] *Id.*; James K. Wilcox, *States Push Their Own Internet Privacy Rules*, CONSUMER REPORTS (Apr. 20, 2017), https://www.consumerreports.org/privacy/states-push-their-own-internet-privacy-rules/.

[15] *2019: Privacy Legislation Related to Internet Service Providers*, NAT'L CONFERENCE OF STATE LEGISLATURES (June 17, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/2019-privacy-legislation-related-to-internet-service-providers.aspx.

[16] *An Act to Protect the Privacy of Online Customer Information*, 35-A M.R.S. c. 94 (2019), *available at* https://mainelegislature.org/legis/bills/getPDF.asp?paper=SP0275&item=9&snum=129.

[17] *Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Mar. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.x; Tracy P. Marshall & Sheila A. Millar, *State Data Breach Notification Laws*, NAT'L LAW REV. (Apr. 28, 2017), https://www.natlawreview.com/article/state-data-breach-notification-laws-overview-requirements-responding-to-data-0.

intimate, personal, and sensitive information about millions and millions of captive broadband customers. This personal information includes all the websites a user visits as they traverse the web, even if the content of the website is encrypted. Home ISP use, in particular, can reveal a great deal of information about the residence's internet users and their behavior. By observing internet traffic patterns, an ISP (or a researcher, foreign government, or others with access the same information) could determine the types of devices that users had in their homes, as well as how often these devices are used, and the same traffic could reveal when the user would likely be in their home.[18] Mobile ISP use reveals even more detail about a user since mobile internet service providers have access to precise location data, in addition to the depth of detail they have about a home-ISP user. This precise location data can allow the ISP to track users as they conduct their daily activities, detect health information by viewing what symptoms and illnesses they use the internet to search for, and draw assumptions about the user's finances, sexuality, political views, and other highly personal characteristics based on a user's web traffic.

> The fridge, Wheeler said, collects information about what's stored inside and shares it via the internet. "Now even when that data only goes to the refrigerator owner's mobile device…It is known by AT&T or Comcast or whoever the ISP is" that consumer subscribes to. "So the ISP knows what goes in and out of a refrigerator!"
>
> *—then-FCC Chairman Tom Wheeler's response to a smart refrigerator seen in the Consumer Reports labs, October 19, 2016*[19]

An ISP's access to precise location data is especially concerning since 20 percent of the US adult population depends on smartphones for their personal internet access.[20] Therefore, ISPs not only have detailed browsing information on these consumers, but they can also combine that data with location information that may reveal sensitive information. Such sensitive information could contain associational affiliations, like an individual's attendance of Alcoholics Anonymous meetings or their religious and leisure activities. The ISP could also deduce health information, such as whether someone has a specific disease, by correlating an online search for the disease with location data that shows the user also made in-person visit to a local clinic, followed by a trip to a local pharmacy.

---

[18] Sarthak Grover et al., *Peeking Behind the NAT: An Empirical Study of Home Networks*, PROCEEDINGS OF THE 2013 CONF. ON INTERNET MEASUREMENT (Oct. 2013), http://conferences.sigcomm.org/imc/2013/papers/imc061-groverA.pdf.

[19] Kate Cox, *FCC Adopts New Privacy Rule Limiting What ISPs Can Do With Your Personal Data*, CONSUMERIST [Archives] (Oct. 28, 2016), https://consumerist.com/2016/10/27/fcc-adopts-new-privacy-rule-limiting-what-isps-can-do-with-your-personal-data/.

[20] *Internet/Broadband Fact Sheet*, PEW RESEARCH CTR. (June 12, 2019), https://www.pewinternet.org/fact-sheet/internet-broadband/.

Equally concerning is the fact, since nearly a quarter of US adults report that they are "almost constantly" online,[21] ISPs have near-constant access to an individual's minute-by-minute activities, correspondences, and behaviors. However, even without constant internet use ISPs have access to a vast array of information about the majority of all adult consumers in the US since most Americans (77 percent) go online on at least a daily basis.[22]

Furthermore, the magnitude of the vast data repositories accumulated by internet providers in their role as communications utilities is likely to only further mushroom with the onset of connected devices. The emerging "Internet of Things" (IoT) category of products—a label that covers everything from digital video recorders to home routers to 'smart' toasters—is expected to balloon to approximately 20.4 billion connected devices by 2020.[23] And, the majority of the connected devices in use will be in the hands of consumers,[24] meaning that a huge amount of detailed data on consumer activities and their interactions with these devices will have to flow through their ISP.

B. Consumers Care About Their Privacy

Consumers deeply care about their privacy and have taken steps to help protect their information while online. Recent research from Forrester shows that consumers in the US and Europe are increasingly concerned about how their data is being used online.[25] This concern has resulted in individuals trusting fewer brands.[26] Additionally, 61 percent of American adults expressed concern about the sharing of their data or online behaviors between companies.[27] And an increasing number of consumers (33 percent) block ads when online and use browser do-not-track settings (25 percent).[28] Despite these tools, the majority of Americans (61 percent) would like to do more to protect their privacy.[29]Consumers have also altered their online activity based on fears that their data may be compromised.[30] A January 2017 Consumer Reports survey found that 65 percent of

---

[21] Andrew Perrin & JingJing Jiang, *About a Quarter of U.S. Adults Say They are 'Almost Constantly' Online*, PEW RESEARCH CTR. (Mar. 14, 2018), http://www.pewresearch.org/fact-tank/2018/03/14/about-a-quarter-of-americans-report-going-online-almost-constantly/.

[22] *Id.*

[23] *Gartner Says 8.4 Billion Connected "Things" Will be in Use in 2017, Up 31 Percent from 2017*, GARTNER (Feb. 17, 2017), http://www.gartner.com/newsroom/id/3598917.

[24] "The consumer segment is the largest user of connected things with 5.2 billion units in 2017, which represents 63 percent of the overall number of applications in use." *Id.*

[25] Greg Sterling, *Survey: Chasm Exists Between Brands and Consumers on Data Privacy*, MARTECH (Apr. 6, 2018), https://martechtoday.com/survey-chasm-exists-between-brands-and-consumers-on-data-privacy-213646.

[26] *Id.*

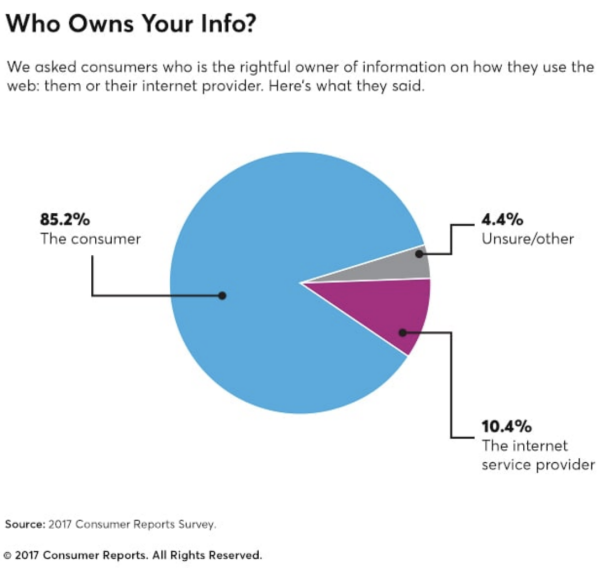
[27] *Id.*

[28] *Id.*

[29] Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RESEARCH CTR. (Mar. 27, 2018), http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

[30] Rafi Goldberg, *Lack of Trust in Internet Privacy May Deter Economic and Other Online Activities*, NAT'L TELECOM. & INFO. ADMIN. (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

Americans lack confidence that their personal information is private and secure.[31] Following the repeal of the FCC's broadband privacy rules under the CRA, however, a Consumer Reports survey found that this percentage had raised to 70 percent.[32] A March 2018 survey from Pew Research Center reported that although 74 percent of individuals say that it is very important for them to be in control of who can get information about them, only nine percent of those surveyed believe that they have "a lot of control" over the information that is collected about them.[33]



In addition, a May 2017 Consumer Reports survey found that 92 percent of Americans think companies should have to get permission before sharing or selling users' online data.[34] And, most Americans do not believe that having to give up their personal information to get basic communications service over broadband is a fair deal.[35] Consumers' privacy concerns have translated into a desire for stronger laws to help them protect their privacy while online: two-thirds of Americans say that current laws are not good enough in protecting their privacy and the majority of consumers (64 percent) support more regulation of advertisers.[36]

C. Non-Competitive Market Prevents Consumer Agency

Fixed and mobile internet access is essential to the lives of a growing number of consumers: 69 percent of Americans indicate that the lack of a home broadband connection would be a "major disadvantage to finding a job, getting health information, or accessing other key information."[37] Today, more than 84 percent of American adults use the internet, including more than 95 percent of those aged 18 to 29.[38] Seventy-seven percent of Americans own smartphones, which most use

[31] *As Trump Takes Office, What's Top of Consumers' Minds?*, CONSUMER REPORTS (Jan. 19, 2017), https://www.consumerreports.org/consumer-protection/as-trump-takes-office-what-is-top-of-consumers-minds/.
[32] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/ [hereinafter *Consumers Less Confident*].
[33] *Americans' Complicated Feelings*, *supra* note 29.
[34] *Consumers Less Confident*, *supra* note 32.
[35] Joseph Turow et al., *The Tradeoff Fallacy*, UNIV. OF PA. (June 2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.
[36] *Americans' Complicated Feelings*, *supra* note 29.
[37] John B. Horrigan & Maeve Duggan, *Home Broadband 2015*, PEW RESEARCH CTR. (Dec. 21, 2015), http://www.pewinternet.org/2015/12/21/home-broadband-2015/.
[38] Andrew Perrin & Maeve Duggan, *Americans' Internet Access: 2000-2015*, PEW RESEARCH CTR. (June 26, 2015), http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/.

for online banking, accessing employment and health information, social networking, and driving directions.[39] In addition, about 80 percent of Americans shop online.[40] Through the course of conducting these online activities, consumers share highly personal data with their ISP.

However, most consumers only have a choice of one or two high-speed broadband providers. Forty percent of all Americans are limited to one ISP.[41] The majority of the US broadband market is controlled by two providers: Comcast and Charter.[42] The market for wireless internet service, which is already not very competitive particularly in rural areas, may even shrink from four to three available providers if the Sprint/T-Mobile merger is finalized.[43] This lack of competition means that consumers cannot necessarily avoid one ISP's data policies simply by switching service providers. As consumers increasingly lack the ability to make meaningful choices or to protect their own interests, legislatures have an obligation to establish basic protections to safeguard fundamental interests and rights. Broadband privacy legislation would provide consumers with choice and agency—and protect our online activities and communications from unwanted snooping.

D. The Federal Trade Commission's Protections are Insufficient

Although the Federal Trade Commission (FTC) still likely has jurisdiction over ISPs after the CRA,[44] the FTC protections are far too flimsy: the FTC can only bring enforcement actions under Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices but does not specify privacy obligations or limitations. Further, the FTC lacks the authority to issue regulations and lacks the ability to obtain civil penalties for violations of their weaker statutory mandate.

> "Any fondness for the FTC's approach to privacy is merely support for dramatically weaker privacy protections favored by most corporations…There is no question that consumers favor the FCC's current broadband privacy rules."
>
> *—Consumer Reports's letter to the US Senate, opposing the use of the CRA to nullify the FCC's broadband privacy rules, March 22, 2017*

[39] *Mobile Fact Sheet*, PEW RESEARCH CTR. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/.
[40] Aaron Smith & Monica Anderson, *Online Shopping and E-Commerce*, PEW RESEARCH CTR. (Dec. 19, 2016), http://www.pewinternet.org/2016/12/19/online-shopping-and-e-commerce/.
[41] Liza Gonzalez, *Net Neutrality Repeal Fact Sheets*, INST. FOR LOCAL SELF-RELIANCE (Dec. 21, 2017), https://ilsr.org/net-neutrality-repeal-fact-sheets-by-the-numbers-maps-and-data/.
[42] John Bergamayer, *We Need Title II Protections in the Uncompetitive Broadband Market*, PUBLIC KNOWLEDGE (Apr. 26, 2017), https://www.publicknowledge.org/news-blog/blogs/we-need-title-ii-protections-in-the-uncompetitive-broadband-market.
[43] *Id.*
[44] FTC V. AT&T MOBILITY, LLC, 883 F. 3d 848 (9th Cir. 2018).

E. Low-Implementation Costs of State Broadband Rules

ISPs are already equipped to implement state-specific privacy protections given that they have access to geolocation and street address billing information for their customers. Moreover, most, if not all, ISPs currently allow users to opt out of the secondary usage of their information (though few users know about these controls). A state broadband privacy rule would simply flip the default for residents of a state to the more privacy protective (and reasonably expected) option. Currently, the opt-outs ISPs provide are buried in the company's policies and are very hard for the average user to find.[45] In addition, some ISPs provide multiple opt-outs on different pages, requiring the user to expend more time and energy in order to tell their ISP that they do not want their personal information collected and used for advertising and other purposes.

F. Broadband Privacy Continues to Allow ISPs to Compete in the Edge Provider Market

Edge providers is a term used to describe "any individual or entity that provides any content, application, or service over the Internet, and any individual or entity that provides a device used for accessing any content, application, or service over the Internet."[46] To the extent that an ISP is seeking to compete with other companies in providing other services over the internet, it is free to establish separate, independent affiliates that collect and use consumer information in the same manner as those other companies, subject to the same rules that apply to them. But to the extent that an ISP seeks a *competitive advantage* over edge providers or other internet-based companies (like advertising networks), by virtue of its comprehensive gateway access to personal consumer information, that is but another important reason why consumer privacy protection rules for ISPs need to be strong. Americans may very well prefer not to give their ISP an insider advantage over competing companies in marketing these other services. And consumers should be in control of deciding that. The broadband privacy rules the FCC passed in 2016 would have enabled consumers to be in control of their data, and states are justifiably looking to establish these protections at the state level.

Some compare internet provider activities to those of an edge provider, and argue that ISPs are being unfairly held to a higher standard. However, these two services simply cannot be fairly compared. Although edge providers, like Facebook and Google, also collect and control a lot of data about users and should be better regulated, ISPs have a different relationship with consumers—and a holistic view of consumers' online activities, no matter which edge providers they elect to visit.

---

[45] Libby Watson, *Want to Stop Your Internet Service Provider from Selling Your Browsing Data? It Ain't Easy*, GIZMODO (Apr. 7, 2017), https://gizmodo.com/want-to-stop-your-internet-provider-from-selling-your-b-1793902371.

[46] David Post, *Does the FCC Really Not Get It About the Internet?*, WASH. POST (Oct. 31, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/10/31/does-the-fcc-really-not-get-it-about-the-internet.

In the edge provider market, consumers are able to choose with which companies they interact—and at least have the ability to block third-party tracking to limit those companies' tracking behaviors.[47] Importantly, however, those tools cannot block tracking from the ISP that routes the consumer's traffic. Users could use a virtual private network (VPN) to protect their traffic from ISP surveillance, but this option is expensive and also opens the consumer up to potential snooping by the VPN provider (and ISPs could ban VPN use on their networks in order to get around this barrier). In short, using a VPN does not sufficiently protect consumers since they are merely substituting one set of eyes for another.

IV. Broadband Privacy Rules Should Not Allow ISPs to Penalize Consumers

Privacy is a right, not a luxury good. Any effective broadband privacy law should prohibit ISPs from charging Americans more or discriminating against them for effectuating their privacy preferences. Americans should have more control over what personal information ISPs have access to and they should not be penalized preferring to keep their private information private. Americans already pay steep monthly rates to their ISPs and mobile phone providers; they do not expect those service providers to monetize the very sensitive information contained in their internet traffic. In addition, pay-for-privacy plans disproportionately affect low income individuals. Therefore, ISPs should not be allowed to incentivize consumers to give away their privacy in order for the company to increase profits. Pay-for-privacy schemes could also further exacerbate the untenable and unbalanced relationship between Americans and internet service providers. Many Americans lack a choice in broadband service providers.[48] In addition, many residents live in buildings that have restrictive service agreements with one internet provider.[49] State and local governments should reinstate broadband privacy protections for their residents precisely to help alleviate this unbalanced relationship between consumers and internet providers.

In addition, the internet industry has not provided compelling examples of pay-for-privacy schemes. In 2016, AT&T offered a pay-for-privacy plan with poor results.[50] Not only was it

---

[47] For instance, a consumer who uses a browser extension such as uBlock, Disconnect.me, or Privacy Badger—or a browser such as Brave that blocks tracking—can stop Google and Facebook from tracking them on other sites such as the New York Times or WebMD.

[48] *See infra* Non-Competitive Market Prevents Consumer Agency.

[49] "The record in this inquiry is clear—competition for video and broadband services in multiple tenant environments ("MTEs," also referred to as multiple dwelling units, "MDUs") is far less robust than the market for these services in single family homes…Without access to these providers, residents of MTEs will be denied the benefits inherent to a competitive telecommunications market—innovative services (such as fiber), higher speeds, and lower prices." *Reply Comments to the Fed. Commc'n Comm'n, Re: Improving Competitive Broadband Access to Multiple Tenant Environments*, INCOMPAS (Aug. 22, 2017), http://www.incompas.org/files/INCOMPAS%20Reply%20Comment%20GN%2017-142.pdf; *see*, *also*, Susan Crawford, *The New Payola: Deals Landlords Cut with Internet Providers*, WIRED (June 27, 2016), https://www.wired.com/2016/06/the-new-payola-deals-landlords-cut-with-internet-providers/.

[50] *See* Karl Bode, *AT&T's $30 'Don't Be Snooped On' Fee is Even Worse than Everybody Thought*, TECHDIRT (Mar. 2, 2015), https://www.techdirt.com/articles/20150219/11473630072/ats-30-dont-be-snooped-fee-is-even-worse-than-everybody-thought.shtml. Comcast has discussed offering a similar program in regulatory filings. *See Comments*

confusing and difficult for consumers to opt out of the collection and use of their data in the first place, the disparity between the privacy protective plan and the discounted plan was $30 dollars a month, a significant portion of the monthly charge. And the discounted amount was not even tied to the relative value of the personal data being shared: "The inducement engendered by such a steep discount, which did not even appear tied to the monetary value of the data, effectively took away the ability of AT&T customer to make a reasoned choice about their privacy."[51]

Furthermore, pay-for-privacy plans will also serve to make monthly service plan costs less transparent and frustrate consumer efforts to comparison shop. Consumers already lack transparency about their monthly service fees and are subject to surprising additional fees and charges on their (already-steep) cable bills. Accordingly, in June 2018 Consumer Reports announced our "What the Fee?!" campaign by delivering more than 100,000 petition signatures to Comcast's headquarters, calling on the company, and the entire cable industry, to eliminate hidden fees and clearly advertise the full price of their service so consumers can effectively comparison shop.[52] By providing pay-for-privacy plans that charge Americans more if they choose to protect their privacy, ISPs will further obscure the full price of broadband service and prevent consumers from easily comparison shopping. In addition, since each ISP has different business affiliates and data sharing agreements, consumers are currently unable to compare pay-for-privacy plans against one another in order to evaluate how privacy-invasive the discounted plan is.

Finally, due to the vast amount of information that ISPs have access to, they are able to discriminate against consumers on the basis of other signals of low-income status. For instance, in 2016, Phoenix, Arizona-based cable provider, Cable One, identified which customers had poor credit and used that information to downgrade their customer service.[53] As the examples above

---

to the Fed. Commc'n Comm'n Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, COMCAST (Aug. 1, 2016), https://assets.documentcloud.org/documents/3004210/Comcast-FCC-Filing.pdf.

[51] *Open Technology Institute Publishes Model State Legislation for Broadband Privacy*, OPEN TECH. INST. (Oct. 30, 2017), https://www.newamerica.org/oti/press-releases/open-technology-institute-publishes-model-state-legislation-broadband-privacy/.

[52] *Consumer Reports Launches "What the Fee?!" Campaign at Comcast Headquarters*, CONSUMER REPORTS (June 28, 2018), https://www.consumerreports.org/media-room/press-releases/2018/06/consumer-reports-launches-what-the-fee-campaign/; *What the Fee?!*, CONSUMER REPORTS, https://action.consumerreports.org/whatthefee/ (last visited Aug. 23, 2018).

[53] And although the company might be subject to legal action on the basis of this discrimination, it would be difficult for a customer to prove this discrimination. (However, this practice would have likely been prohibited by the FCC broadband privacy rules.) In addition, this practice disproportionately affects communities of color: "The use of credit score to screen potential customers is already a barrier to home internet adoption that disproportionately impacts communities of color," says Free Press Research Director S. Derek Turner. "But what Cable ONE is apparently doing takes this to a much more dangerous territory. Because there are systemic biases that impact the credit scores of communities of color, Cable ONE is in essence adopting a policy that will result in inferior service for customers based solely on the biased credit score metric, and as a consequence, people of color will disproportionately receive this inferior service," he added."" Karl Bode, *Cable Company Admits It Gives Poor Credit Score Customers—Even Worse Customer Service*, TECHDIRT (June 3, 3016), https://www.techdirt.com/articles/20160602/09105734602/cable-company-admits-it-gives-poor-credit-score-

indicate, broadband providers should be prohibited from denying or providing worse service to customers or applicants who do not opt-in to the use of their data, including charging them higher prices or offering inferior products or services.

V. Specific Elements of State Broadband Privacy Proposals

State legislators have started drafting proposals for reinstating the broadband privacy protections contained in the now-repealed FCC broadband privacy rules in order to adequately protect and secure their residents' online privacy. Regardless of specific language, however, any state broadband privacy law should, at a minimum, include:

- **Transparency.** In order for consumers to make decisions about their data, they need to be informed of the ISP's data practices. Providers should be required to disclose the types of personal information it collects about its users, how that information is used, and how long the company retains the data. In addition, the ISP should disclose the circumstances under which they disclose, sell, or permit access to personal customer information. The consumer should also know what categories of entities the company discloses, shares, or permits access to this information and the purposes for which each category of entity will use that information. Consumers must also have a clear statement from the company regarding the consumer's right to consent with regard to the use of, disclosure of, sale of, or access to their personal information and how that right may be exercised.
- **Comprehensive definition of personal data.** The scope of personal information that should be protected as private and subject to opt-in consent for use, disclosure, sale, or access should include such identifiers as name and billing information and government-issued identifiers, but also any information that the ISP has access to by virtue of their role as a gatekeeper to the internet such as unique device identifiers, internet addresses, browsing information, and app usage. Although it is permissible to exclude aggregated data from "personal information," de-identified browsing data should not be excluded from this definition since it is hard to render such data unidentifiable.[54] The definition of personal information should be broad enough to include any information concerning a customer that is collected or made available and is maintained in a way that the information is linked or reasonably linkable to a customer or device.
- **Separate, opt-in consent for most secondary usage or transfer of data.** Consumers are less aware and less able to control what secondary usage is made of their data that the company has collected about the consumer. Consumers should have a dedicated prompt requiring opt-in approval for secondary use or transfer of their data, including

customers-even-worse-customer-service.shtml.

[54] Kevah Waddell, *Your Browsing History Alone Can Give Away Your Identity*, THE ATLANTIC (Feb. 6, 2017), https://www.theatlantic.com/technology/archive/2017/02/browsing-history-identity/515763/.

for advertising, marketing, and research purposes. Protections should apply whether the data even if the data never leaves the ISP—consumers still do not expect their service provider to surveil their online traffic to target ads or for vague research purposes.

- **No pay-for-privacy plans or discrimination.** Privacy should not be a luxury good, and any service plan that charges users more for making privacy-conscious choices will disproportionately affect lower income households. In addition, ISPs should be prevented from discriminating against consumers in other ways due to their privacy preferences. Pay-for-privacy schemes are especially pernicious in the broadband industry because (1) the marketplace is uncompetitive, (2) ISPs have an all-encompassing and unique view of all of a user's activities online, and (3) consumers depend on and need broadband internet access to perform daily tasks.[55]
- **Reasonable exceptions for operational use.** The general prohibition on secondary usage without consent should include thoughtful exceptions allowing collection and use of consumer data for reasonable operational purposes. Thus, a provider should be able to use or disclose consumer personal information without consumer approval for the purpose of delivering its services, to comply with legal processes or other legal orders, and to initiate, render, bill for, and collect payment for the service. A legislative proposal should also allow the use of customer information for security and fraud prevention, and to improve network performance, but such collection and use should be limited and proportionate—an ISP should not collect and store all possible data in perpetuity simply because it might theoretically have some value in the future. However, a bill should not allow for broad exceptions for measurement, product improvement, or research. If an ISP wants a customer's data for those purposes, it should ask and receive permission first.
- **Data security.** ISPs should be required to implement and maintain reasonable measures to protect consumer personal information from unauthorized use, disclosure, sale, access, destruction, or modification. Reasonable security measures mean that the measures are informed by the nature and scope of the ISP's activities, the sensitivity of the data it collects, the size of the ISP, and the technical feasibility of the measures.
- **Data minimization.** The ISP shall not retain consumer personal information for longer than reasonably necessary to accomplish the purposes for which the information was collected. Data minimization also decreases the amount of consumer information that is vulnerable to a future breach, and thus is part of reasonable data security practices.
- **Data breach notification.** In the case of a breach of consumer personal information, ISPs should notify affected customers, the state body charged with supervision of telecommunications service providers, and law enforcement unless the provider is able to reasonably determine that a data breach is unlikely to pose a risk of harm to the

[55] *See infra* Broadband Privacy Rules Should Not Allow ISPs to Penalize Consumers for Their Privacy Preferences.

affected customers. The notice should detail what kind of information was breached. The ISP should notify state and local authorities within seven business days of when the provider reasonably determines that a breach has occurred if the breach impacts 5,000 or more customers. ISPs must provide notice to affected customers without unreasonable delay, but within no more than 30 days.

- **Robust enforcement.** Under the applicable state laws and regulations, the provisions in the broadband privacy legislation should be subject to robust enforcement in order to ensure that residents are sufficiently protected and their choices regarding the collection and use of their data are respected. The penalties to the ISP for failing to meet the requirements of the broadband privacy legislation must be clear and meaningful. In addition to enforcement by a state attorney general—and potentially local enforcers as well—a private right of action should be implemented so ISPs are sufficiently incentivized to protect consumer privacy.

Many state proposals are strong and closely align to the FCC's rule, the above principles, and the recently-published model state legislation[56] authored by New America's Open Technology Institute and supported by a coalition of consumer and public interest organizations, including Consumer Reports. Two states, Minnesota[57] and Nevada,[58] require ISPs to keep private certain information concerning their customers unless the customer opts-in to the disclosure. In addition, Seattle, WA[59] and Tacoma, WA[60] have also passed broadband privacy rules for ISPs. Finally, in 2019 Maine not only passed a law that not only reinstates that protections contained within the FCC's broadband privacy rules, but also prohibits pay-for-privacy programs.[61]

Additional local and state governments can build on this momentum to ensure that Americans' right to privacy is protected online as well as it is on the phone and in the mail.

VI. Contact Details and More Information

For more information about broadband privacy and the importance of a free and open internet, please consult our work[62] on privacy and technology issues.

---

[56] *Open Technology Institute Publishes Model State Legislation for Broadband Privacy*, OPEN TECH. INST. (Oct. 30, 2017), https://www.newamerica.org/oti/press-releases/open-technology-institute-publishes-model-state-legislation-broadband-privacy/.

[57] Minn. Stat. §§ 325M.01 - 325M.09, available at http://www.revisor.leg.state.mn.us/stats/325M.

[58] Nevada Revised Stat. § 205.498, available at https://www.leg.state.nv.us/NRS/NRS-205.html#NRS205Sec498.

[59] *ITD Directors Rule 2017-01*, CITY OF SEATTLE (May 3, 2017), *available at* http://www.seattle.gov/Documents/Departments/SeattleIT/SeattleRule_ITD-2017-01.pdf.

[60] *Resolution No. 39702*, CITY OF TACOMA, (Apr. 2017), https://muninetworks.org/sites/www.muninetworks.org/files/2017-04-Resolution-onilne-privacy.pdf.

[61] *An Act to Protect the Privacy of Online Customer Information*, *supra* note 16.

[62] *Our Work: Privacy*, CONSUMER REPORTS, https://advocacy.consumerreports.org/issue/tech-privacy/ (last visited Feb. 26, 2019).

For more information on Consumer Reports's broadband privacy legislation recommendations, please contact:

Katie McInnis
Policy Counsel
katie.mcinnis@consumer.org
202.462.6262

Justin Brookman
Director, Consumer Privacy and Technology Policy
justin.brookman@consumer.org
202.462.6262