ConsumersUnion®

THE ADVOCACY DIVISION OF CONSUMER REPORTS

August 26, 2018

Office of Cable Television, Film,
Music, & Entertainment (OCTFME)
Attn: Lawrence Cooper, General Counsel
1899 9th Street, NE
Washington, DC 20018

Re: Notice of Proposed Rulemaking—Privacy Protections for Cable and Internet Customers, N0071499

Dear Mr. Lawrence Cooper,

Consumers Union (CU), the advocacy division of Consumer Reports,[1] writes to respond to the notice of proposed rulemaking from the Office of Cable Television, Film, Music, and Entertainment (hereinafter the "Agency") on the issue of broadband privacy rules for internet service providers (ISPs) operating in the District of Columbia.

CU strongly encourages the adoption of privacy and security rules governing broadband internet service providers (ISPs). Because of their unique relationship with consumers and the comprehensive—and currently unavoidable—nature of their data collection, ISPs merit dedicated rules to limit their collection and use of customer internet behavioral data for advertising and related purposes. Due to the repeal of the Federal Communications Commission's (FCC) broadband privacy rules, consumers' online communications are afforded less privacy protection than traditional telephonic or paper communications. Therefore, it is vital that states institute strong broadband privacy rules to protect their residents.

The Agency's proposed rules would provide DC residents increased choice, security, and transparency over how ISPs use the data they collect from and about their customers. We appreciate the Agency's leadership on broadband privacy and suggest changes to the proposed rules to ensure that residents are sufficiently protected. Finally, we include more information about ISPs' all-encompassing view of their customers' online activity, the lack of federal preemption issues with the passage of state and local broadband privacy rules, and resources for more information.

Specific Changes to the Proposed Rules

- **Section 3119.3(a) should be amended to require ISPs to provide simple, transparent,**

[1] Consumer Reports is the world's largest independent product-testing organization. It conducts its policy and mobilization work in the areas of telecommunications reform, as well as financial services reform, food and product safety, health care reform, and 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.

and easily accessible electronic methods of allowing consumers to remove their names and addresses from an ISP's list. Consumers need an electronic means of signaling their privacy preferences in addition to the provision of a stamped, self-addressed postcard. In addition to ease of use, an electronic control would allow for the consumer to easily find and potentially change their privacy settings in the future.[2]

- **The "legitimate business purpose" exception in § 3119.7 should be eliminated.** This language is overly broad and could potentially be interpreted to allow for disclosures related to advertising, research, analytics, or measurement that run counter to consumers' reasonable expectations.
- **ISPs should not be able to charge consumers for exercising privacy choices (§ 3119.19).** ISPs should not be allowed to offer pay-for-privacy plans where consumers are effectively charged more for keeping their private information private. Consumers 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 consumers and internet service providers. For many DC residents, Comcast is the only high-speed broadband option.[3] In addition, many residents live in buildings that have restrictive service agreements with one internet provider.[4] The District of Columbia 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 good examples of pay-for-privacy schemes. In 2016, AT&T offered a pay-for-privacy plan with poor results.[5] Not only was it really hard 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

---

[2] As consumers are able to under § 3119.11. *And, see* 15 D.C.M.R. § 3119.3(b).

[3] *Internet Providers in Washington, District of Columbia*, BROADBANDNOW, https://broadbandnow.com/District-Of-Columbia/Washington&sa=D&ust=1535003007033000&usg=AFQjCNF7s3Iso2LiTYGYa_w-LhfJdalj9Q (last visited Aug. 20, 2018).

[4] "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/.

[5] *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.

a reasoned choice about their privacy."[6]

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.[7] By providing pay-for-privacy plans that charge consumers 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.

- **The definition of "personally identifiable information" under § 3119.99 should be broadened** to include (a) government-issued identifiers and (b) 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, device, or household*. Although we appreciate the catchall provision in subsection I of this definition, we recommend the inclusion of these two types of identifiable information in order to sufficiently protect consumers and to give cable providers more guidance on what is meant by this definition.
- **The definition of "personally identifiable information" should include data that could reasonably be reidentified.** The proposed rule excludes aggregate data from the definition of "personally identifiable information" but is vague on individual deidentified records. The definition of "personally identifiable information" should be further clarified to include facially deidentified data that could reasonably be reidentified or reassociated with customer, device, or household.
- **Clarify in §§ 3119.4 and 3119.7 that consent has to clear, freely-given, and separate from any other consent or agreement.** Privacy policies and terms of service agreements are typically too long and filled with legalese for the average consumer to read.[8] A subscriber cannot be meaningfully said to consent to ISP data collection, use, and disclosure merely because they agreed to boilerplate terms of service agreements or privacy policies. Such consent should be separate and presented in clear, easy to

---

[6] *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/.

[7] *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).

[8] And, indeed, it would be inefficient to do so. A study by Aleecia McDonald and Lorrie Cranor estimated that reading every site's privacy policy would take users over 244 hours per year, at a collective societal cost in wasted opportunity of over $600 billion. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, J. OF LAW & POLICY FOR THE INFO. SOCIETY (2008), https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf.

understand language. By ensuring that the consent is given via a separate disclosure, consumers will be better informed about ISPs' data practices and able to decide whether or not to share their personal information.

- **Clarify that data collected without consent pursuant to narrow exceptions in § 3119.4 cannot be used for secondary purposes without consent.** Companies may still collect very sensitive data without consent simply in order to by providing internet access or prevent fraud. This data should not be used for other purposes without the customer's permission. Consumers' choice around the collection of their data should also apply to the secondary use of their data, including for advertising, marketing, and research purposes. Importantly, the rules' protections should apply 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.

The Rationale for State and Local Broadband Privacy Rules

Because there are no protections at the federal level, it is vital that states pass broadband privacy rules to protect their residents. 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.[9] DC residents need strong privacy protections over how ISPs treat their data. Therefore, we encourage the Agency to institute strong rules protecting residents' data due to the unique insight ISPs have into customer activity and the lack of protections at the federal level.

The Unique Role of ISPs

An ISP has an intimate, all-encompassing window into its customers' behavior because they provide internet service that gives 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 unfettered access by the ISP. And consumers often have no choice over which ISP to use.[10] All of an individual's traffic flows over that internet connection,

[9] *Security Breach Notification Laws*, NAT'L CONF. 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.

[10] Most consumers only have a choice of one or two high-speed broadband providers. Forty percent of all Americans are limited to one ISP. 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/. The majority of the US broadband market is controlled by two providers: Comcast and Charter. John Bergmayer, *We Need Title II Protections in the Uncompetitive Broadband Market*, PUB. KNOWLEDGE (Apr. 26, 2017), https://www.publicknowledge.org/news-blog/blogs/we-need-title-ii-protections-in-the-uncompetitive-broadband-market. 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. *Id*. This lack of competition means that consumers cannot necessarily avoid one ISP's data policies simply by switching service providers. This trend of corporate consolidation seems unlikely to abate anytime soon, especially after the Supreme Court's recent decision in *Ohio v. American Express*. 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 restore the traditional relationship between ISPs and their customers—and

traffic which can convey very personal information such as personal banking details, presence at home, sexual preference, physical ailments, physical location, race or nationality, and religion.[11] Even when traffic is encrypted, ISPs still know the sites and services their customers use.

Unfortunately, many consumers are unaware that their ISP collects and sells many kinds of sensitive and private information. User information that ISPs routinely collect and share with business partners includes: "geo-location" 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.

The potential misuses of personal information go well beyond aggressive product marketing: ISPs' pervasive surveillance practices gives virtually anyone willing to pay—identity thieves and other scam artists, employers, insurance and financial service providers, business and professional rivals, and even former romantic partners—the ability to assemble a detailed and highly personal dossier of your life. Essentially anything a consumer does or expresses on the internet that they would like to keep private could be examined and used to their disadvantage, including communications with doctors or lawyers, political activities, job inquiries, dating site history.

ISPs have taken advantage of the lack of controls on their activities and violated consumers' expectations of privacy in a number of ways. For instance, with such comprehensive data, ISPs can create intricately detailed profiles of their customers to sell for a variety of purposes, including targeted digital advertisements for products like payday loans or expensive and unnecessary medications. And ISPs sold consumer data to marketers,[12] hijacked searches in order to direct traffic to business partners,[13] snooped through individuals web traffic in order to deliver ads,[14] pre-installed software on consumers' phones in order to track their activity on the device,[15]

---

protect our online activities and communications from unwanted snooping.

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

[12] 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/.

[13] "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/.

[14] Three ISPs have been known to do this: AT&T, Charter, and CMA. AT&T snooped on web traffic for some of their paid Wi-Fi 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

and placed undeletable and undetectable tracking cookies in order to track consumers activities on their mobile phones.[16] The majority of these abuses were made transparent through the work of outside researchers. Consumers should not have to depend on such research to know what ISPs collect about them and what is done with their information.

Consumers should have control over whether their ISP monetizes the data it collects in providing internet service. And consumers clearly desire the protections the FCC rules would have provided.[17] For these reasons, we encourage the state and local agencies to reinstate the broadband privacy and security protections consumers lost due to the federal repeal.

No Federal Preemption of State Action on Broadband Privacy

The federal government can only preempt[18] a state law or regulation when there is a federal law or regulation on this issue. 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. Nor is there a rule at the federal level regulating broadband privacy. In the wake of this repeal, 24 states and the District of Columbia have introduced legislation concerning residents' online privacy.[19] In addition, at least 19 states and the District of Columbia have introduced or are considering legislation reinstating some or all of the protections contained within the FCC rules.[20] Two states have passed

---

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/.

[15] 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 SECURITY TEST (2011), http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/.

[16] 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 FOUNDATION (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/.

[17] Recent research from Forrester shows that consumers in the US and Europe are increasingly concerned about how their data is being used online. 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. This concern has resulted in individuals trusting fewer brands. *Id*. Additionally, 61 percent of US adults expressed concern about the sharing of their data or online behaviors between companies. *Id*. And an increasing number of consumers (33 percent) block ads when online and use browser do-not-track settings (25 percent). *Id*. Despite these tools, the majority of consumers (61 percent) would like to do more to protect their privacy. Lee Raine, *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/.

[18] By way of background, legal preemption occurs when, by legislative or regulatory action, a "higher" level of government (in this case, federal) eliminates or reduces the authority of a "lower" level (e.g., state) over a given issue.

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

[20] *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/.

legislation that requires ISPs to protect some private information about consumers and one state, Minnesota, also requires ISPs to get permission from customers before disclosing browsing information.[21]

Modern courts have generally applied a presumption against preemption, especially in regulatory areas ordinarily left to the states. Courts have declined to find state law preempted unless a federal statute provides a "clear statement" that state law is to be preempted.[22] In this case there is no federal rules regulating consumer broadband privacy, let alone clear statements providing express preemptive language, so there is no threat of federal preemption on state consumer privacy laws.

In addition, states have a lot of authority over the ISPs that operate within their borders.[23] And ISPs are already equipped to implement state-specific privacy protections given that they know the precise location of all their customers. The cost to implement this change would also be very small, and thus will not burden interstate commerce, because it should only require modest coding changes. Due to the fact that most, if not all, ISPs provide opt-outs allowing users to effectuate their data privacy preferences, all a privacy rule would require is that the company sets the default for residents of a state to be the more privacy protective one (i.e., essentially changing their opt-outs to opt-ins).[24] And for critical protections not already covered by their opt-outs the it is not unreasonable for these companies to bear a small cost for added software changes to ensure the protection of DC residents.

Contact Details and More Information

Broadband privacy protections are necessary because individuals depend on the internet, ISPs have a unique and all-encompassing view of consumer data through their online gatekeeper role, and consumers greatly value their privacy,[25] yet lack the ability to effectuate their preferences due to a non-competitive ISP marketplace.[26] Since the federal government is not acting on the issue of broadband privacy (and there is no issue of preemption of state action), we encourage state and local action on broadband privacy to protect their residents. **For these reasons we support the adoption of strong broadband privacy rules by the Agency and we hope our**

---

[21] "Nevada and Minnesota require internet service providers (ISPs) to keep private certain information concerning their customers, unless the customer gives permission to disclose the information. Both states prohibit disclosure of personally identifying information…" *Privacy Legislation*, *supra* note 19.

[22] *See*, *e.g.*, RICE V, SANTA FE ELEVATOR CORP., 331 U.S. 218, 230 (1947); TENNESSEE, V. FEDERAL COMMUNICATIONS COMM'N, 832 F.3d 597 (6th Cir. 2016); NIXON V. MISSOURI MUNICIPAL LEAGUE, 541 U.S. 125 (2004).

[23] Since ISPs are companies that operate in and seek business with a state, states have broad purview over these companies.

[24] 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.

[25] A recent survey from Consumer Reports found that 92 percent of Americans think companies should have to get permission before sharing or selling users' online data. *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/.

[26] *Supra* text accompanying note 10.

comments have helped clarified some of the issues covered by the proposed rules.

For more information about broadband privacy and the importance of a free and open internet, please consult Open Technology Institute's model[27] broadband privacy model bill and our work[28] on privacy and technology issues.

For more information on Consumers Union's broadband privacy rule and legislation recommendations, please contact:

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

Katie McInnis
Staff Attorney
katherine.mcinnis@consumer.org
202.462.6262

[27] *Model State Legislation for Broadband Privacy*, *supra* note 6.
[28] *Our Work: Privacy*, CONSUMERS UNION, https://consumersunion.org/topic/phones-media/privacy-2/ (last visited July 31, 2018).