Before the
D.C. Office of Cable Television, Film, Music, and Entertainment
Washington, DC 20018

In the Matter of	)	
	)	
Office of Cable Television, Film,	)	
Music and Entertainment - Notice of	)	Notice ID: N0071499
Proposed Rulemaking - Privacy Protections	)	
For Cable and Internet Customers	)	

COMMENTS OF NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE

August 24, 2018

Eric Null
New America's Open Technology Institute
740 15th St NW Suite 900
Washington, D.C. 20005

New America's Open Technology Institute (OTI) submits these comments in response to the District of Columbia Office of Cable Television, Film, Music, and Entertainment's (the "Agency") notice of proposed rulemaking, Notice ID N0071499, seeking comment on imposing privacy obligations on cable providers operating in the District.

OTI has been involved in the broadband privacy debate for several years. It released one of the first reports on the subject called *The FCC's Role in Protecting Online Privacy* in January 2016.[1] It submitted several comments to the FCC during its rulemaking proceeding.[2] OTI fought Congress and the Administration as it overturned the broadband privacy rules in early 2017.[3] Once the federal rules were gone, OTI turned its attention to state efforts.[4] It released model legislation last year in response to state requests for help on how to address this issue at the state level.[5] We also supported the DC City Council's broadband privacy efforts last year.[6]

OTI strongly supports the Agency's efforts to impose a rule on cable operators operating in the District. These comments will first discuss why it is important to apply increased privacy protections to broadband (including cable) providers. Then it will discuss the model legislation that OTI published last year, the benefits of that model, and argue that the Agency should use it as a guidepost for the rule it ultimately adopts. Last, there are specific provisions of the proposed rule that should be strengthened.

I. Why Consumers Need Special Privacy Rules for Broadband (Including Cable)

For many reasons, consumers need strong privacy protections over how broadband providers treat their data. As purveyors of the network and gatekeepers to the internet, broadband providers are in a privileged position with nearly-comprehensive access to data about their

---

[1] *The FCC's Role in Protecting Online Privacy*, New America (Jan. 2016), https://static.newamerica.org/attachments/12325-the-fccs-role-in-protecting-online-privacy/CPNI__web.d4fbdb12e83f4adc89f37ebffa3e6075.pdf.

[2] Eric Null, *OTI Defends FCC Proposal to Protect ISP Customers' Data Privacy*, New America (July 11, 2016), https://www.newamerica.org/oti/blog/oti-defends-fcc-proposal-protect-isp-customers-data-privacy; *see also* Eric Null, *FCC Passes New Rules that Actually Increase Consumer Privacy Protections*, New America (Nov. 1, 2016), https://www.newamerica.org/oti/blog/fcc-passes-new-rules-actually-increase-consumer-privacy-protections.

[3] Eric Null, *Don't Repeal Common-Sense Privacy Rules*, New America (Mar. 27, 2017), https://www.newamerica.org/oti/blog/dont-repeal-common-sense-privacy-rules.

[4] *See* Eric Null, *Redrawing the Battle Lines in the ISP Privacy Debate*, Slate (Apr. 17, 2017), http://www.slate.com/articles/technology/future_tense/2017/04/how_to_continue_the_fight_to_protect_consumer_broadband_privacy.html; Eric Null, *The California Legislature Is Trying to Run Out the Clock on Protecting Broadband Privacy*, New America (Sept. 10, 2017), https://www.newamerica.org/oti/blog/california-legislature-trying-run-out-clock-protecting-broadband-privacy.

[5] Press Release, Open Technology Institute Publishes Model State Legislation for Broadband Privacy, New America (Oct. 30, 2017), https://www.newamerica.org/oti/press-releases/open-technology-institute-publishes-model-state-legislation-broadband-privacy. For a full explanation of the model legislation, see Eric Null, *OTI Publishes Model State Legislation to Help States Protect Broadband Privacy*, New America (Oct. 26, 2017), https://www.newamerica.org/oti/blog/oti-publishes-model-state-legislation-help-states-protect-broadband-privacy.

[6] Eric Null, *As California Drops Broadband Privacy (for Now), D.C. Picks It Up*, New America (Sept. 19, 2017), https://www.newamerica.org/oti/blog/california-drops-broadband-privacy-now-dc-picks-it; Letter to Chairman Kenyan McDuffie from ACLU et al., Sept. 18, 2017, https://consumersunion.org/wp-content/uploads/2017/09/DC-broadband-support-letter-9.18.17.pdf.

customers. For their part, consumers must access the internet through a broadband provider, which collects a substantial subscription fee for that service. Thus, to receive internet access service, customers have no choice but to disclose a vast array of data to their provider. The data broadband providers collect and see is highly personal and detailed, including web browsing records, geolocation data, financial and health information, and in some cases the content of communications. This universe of data can reveal, for instance, a customer's race or nationality, sexual preference, religion, physical location, presence at home, personal banking details, and physical ailments.

Armed with such comprehensive and revealing data, providers can and likely do create intricate profiles of their individual subscribers. Further, they are able to use, sell, or provide access to that data for a variety of purposes, including targeting digital advertisements for products like payday loans or expensive and unnecessary medications. To make matters worse, the broadband market lacks robust competition.[7] Thus, broadband customers in most cases cannot switch providers, as they often can with providers of online services like email, browsers, or video streaming sites, to avoid a broadband provider's privacy practices. As such, consumers should have the right to choose, through opt-in consent, whether and how their providers can use their personal information for purposes other than providing the service.

OTI is encouraged to see the Office of Cable Television, Film, Music, and Entertainment take an active role in this debate. There is substantial uncertainty around privacy rules and the proper role of federal agencies. While OTI has long argued that the FCC should oversee broadband provider privacy practices, the FCC's recent decision to reclassify broadband back to a Title I information service means that the Federal Trade Commission (FTC) oversees broadband practices. However, the FTC is not the appropriate agency to oversee the broadband market.[8] For instance, it is a small agency with only deceptive and unfairness authority (where it primarily policies privacy promises companies set themselves), and it has no network or communications expertise and little rulemaking authority.

The Agency's effort could result in clear rules of the road for cable providers in the District, similar to Seattle's efforts over a year ago.[9]

---

[7] Comments of New America's Open Technology Institute to Federal Trade Commission, Competition and Consumer Protection in the 21st Century: Competition and Consumer Protection Issues in Communication, Information, and Media Technology Networks (Aug. 20, 2018), https://newamericadotorg.s3.amazonaws.com/documents/OTI_Final_FTC_BIAS_Comments_Question_2.pdf; Comments of New America's Open Technology Institute to the Federal Communications Commission, Communications Marketplace Report, Dkt. 18-231 et al. (Aug. 17, 2018), https://ecfsapi.fcc.gov/file/10817788202976/FCC%20Fixed%20Broadband%20Competition%20Comments%20of%20OTI%20ILSR%20NLC%20NCC%20NATOA.pdf.

[8] Comments of Free Press Comments to Federal Trade Commission, Competition and Consumer Protection in the 21st Century: Competition and Consumer Protection Issues in Communication, Information, and Media Technology Networks (Aug. 20, 2018).

[9] Kristen Glundberg-Prossor, *Seattle Issues Rule to Strengthen Broadband Privacy for Consumers*, Seattle.gov (May 3, 2017), http://techtalk.seattle.gov/2017/05/03/city-of-seattle-information-technology-department-directors-rule-2017-01.

II. OTI's model bill provides strong privacy protections and the Agency should use it as a guidepost for the rule it ultimately adopts

Since Congress repealed the broadband privacy rules, OTI has closely consulted with states and localities working to implement broadband privacy legislation of their own. While OTI has previously supported the FCC's broadband privacy rule and continues to support states and localities that adopt language similar to the FCC's rule, the model language improves on some areas where OTI determined the FCC's rule did not fully protect consumers.

The model language, attached to this comment, takes a comprehensive approach to protecting broadband privacy. Rather than separate buckets of sensitive and non-sensitive data (the approach used in the Agency's proposal and in the FCC rules), the model requires broadband providers to protect all information they collect by default. The model ensures that protection by requiring broadband providers obtain opt-in consent before using, selling, disclosing, or providing access to customer information (which includes merely de-identified data) for any purpose, with some exceptions. The model also requires broadband providers to provide clear and prominent notice of its privacy practices and to use reasonable security measures to protect its customers' data.

The model bans so-called "pay for privacy" schemes, which the Agency's proposal allows. Pay-for-privacy schemes are where a broadband provider will upcharge a customer who wants to protect his or her privacy—or will provide a steep discount to customers who agree to essentially no limitations on how the broadband provider can use his or her data. It is a predatory practice designed to coerce or, at best, induce customers into giving away their privacy rights. The clearest example of the harms that can result from these practices is AT&T's now-defunct broadband internet plan that cost $30 less per month in exchange for routine privacy invasions.[10] The inducement engendered by such a steep discount effectively took away the ability of AT&T customers to make a reasoned choice about their privacy.

The exceptions included in the model allow broadband providers to use information for reasonable purposes. Some commonly-allowed exceptions include use of information for emergency situations and billing. Two other notable exceptions are for aggregate data and advertising of communications-related services. Aggregate data generally presents fewer privacy risks to customers, as data is presented collectively, without identifiers attached to any particular data point. This is in stark contrast to merely "de-identified" data, which has some identifiers removed but remains individualized, making it much easier for that data to be associated with an individual.[11] For the advertising of communications-related services exception, the model

---

[10] Jon Brodkin, *AT&T to End Targeted Ads Program, Give All Users Lowest Available Price*, Ars Technica (Sept. 30, 2016), https://arstechnica.com/information-technology/2016/09/att-to-end-targeted-ads-program-give-all-users-lowest-available-price.

[11] *E.g.*, Boris Lubarsky, *Re-Identification of "Anonymized" Data*, Georgetown Law Technology Review (Apr. 2017), https://www.georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017; Sharad Goel & Arvind Narayanan, *Why You Shouldn't Be Comforted by Internet Providers' Promises to Protect Your Privacy*, Slate (Apr. 4, ,2017), http://www.slate.com/blogs/future_tense/2017/04/04/don_t_be_comforted_by_internet_providers_promises_to_prot

requires "opt-out" consent rather than opt-in. This exception is included because broadband providers may have a First Amendment right to advertise their own services to their customers, at least according to *US West v. FCC*, a case decided by the United States Court of Appeals for the 10th Circuit. However, aside from some limited exceptions, the model requires broadband providers to obtain opt-in consent from customers to use, disclose, sell, or permit access to its customer data.

OTI's model legislation is appropriately tailored to the broadband (and cable) market and represents the best balancing of customer privacy needs versus broadband industry needs. The model bill does not prevent any type of advertising, it merely switches the default so consumers have the ability to understand how their data is used by their broadband provider, rather than assuming consent without any action on the customer's part. The Agency should use this legislation as a guidepost for the rule it ultimately adopts.

III. The proposal should be amended to be stronger in certain areas

Regardless of whether the ultimate rule reflects model bill language, there are several key areas where the proposal should be amended.

Refining the definition of "Cable Operator." Much of the rule does not apply to the cable broadband aspect of cable providers. For instance, section 3119.4 requires "cable operator[s]" not to use the cable system to collect, record, monitor, or observe personally identifiable information concerning any customer without prior consent. "Cable operator" is defined in part as any person or persons who provide cable services over a cable system. A cable service is defined as "[t]he one-way transmission to subscribers of video programming or other programming service."[12] Thus, a cable operator includes only those operators that provide *one-way transmission* of *video programming*. If the intent is to protect the privacy of cable broadband customers, the simplest way to fix this issue would be to amend the definition of "cable operator" to include the provision of wire or radio communications services over their cable facilities.[13]

Opt-in for all non-service-related uses. The proposal requires opt-in consent for collection of data in section 3119.4, and allows an exception for collection when that data is necessary to provide the underlying cable or other service. However, the rule should also prevent all non-service-related uses of that data without opt-in consent. For instance, a cable provider

---

ect_your_privacy.html; Arvind Narayanan & Edward W. Felten, *No Silver Bullet: De-Identification Still Doesn't Work* (July 9, 2014), http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf; Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

[12] DC Code §34-1251.03(4)(A).

[13] The definition of "other service" could use some clarification. Notably, "other service" is defined as a wire or radio communications service provided using the facilities of a cable operator "used in the provision of cable service." While OTI would argue that language inequivocally means "other service" includes cable broadband, the ambiguity could be exploited by cable operators who think that inclusion of that language is meant to narrow the requirement to just cable TV. The words "that are used in the provision of cable service" could be removed from the definition of "other service" to avoid that problem.

may need to collect the websites a customer visits because it needs to serve the correct website to the right customer. That collection is allowed under section 3119.4. Once that data is collected, however, the rule does not appear to prevent any subsequent use of that information (only its disclosure under section 3119.7). Thus, the cable provider would be free to use that information to allow targeted advertising, or research or analytics, contrary to consumer expectations. The Agency should add a provision preventing the use of any data it collects for non-service-related purposes and preventing use of any data for purposes other than those for which it was collected. The Agency already has a similar rule for telecommunications services and other utilities.[14]

Opt-in for use of merely de-identified data. The proposed rule does not adequately differentiate and treat differently aggregate and merely de-identified data. Aggregate data presents fewer privacy risks than identifiable data. Congress defined aggregate data in the Communications Act as data that both (1) had individual identifiers and characteristics removed and (2) was "collective" and related to a group or category of services or customers.[15] Because both of these elements had to be met, consumers were given fewer protections over it.[16] However, merely de-identified data does not meet both elements, it only has identifiers removed. As a result, de-identified data can often be easily re-identified (as discussed above).[17] This is true even if companies that use and share de-identified data follow the three requirements the FCC laid out in its rule from 2016.[18] Given how easily de-identified data can be re-identified, broadband providers should be required to receive opt-in consent from their customers before taking that risk.

Removing the "legitimate business activity" exception. The term "legitimate business activity" in section 3119.7 in the listed exemptions to the opt-in requirement for disclosure of customer data is far too broad. It could mean essentially anything, such as advertising, research, or analytics, which would be contrary to consumer expectations. The primary problem here is that "legitimate" would likely be interpreted for anything that is "legal" rather than having any meaningful limitation on the practices allowed. The easiest way to address this problem is simply to remove the provision. It is sufficient to allow an exemption for opt-in for disclosure of information when the "disclosure is necessary to render a cable service or other service."

---

[14] DCMR §15-308.3 ("Unless a Customer consents in writing, Utility, Energy Supplier or Telecommunications Service Provider may not disclose or use information that is (1) about the Customer, and (2) was supplied to the Electric or Natural Gas Utility or Energy Supplier by the Customer for any purpose other than the purpose for which the information was originally acquired.").

[15] 47 USC §222(h)(2).

[16] 47 USC §222(c)(3)

[17] Arvind Narayanan, Johanna Huey, & Edward W. Felten, *A Precautionary Approach to Big Data Privacy* 5 (Mar. 15, 2015), http://randomwalker.info/publications/precautionary.pdf.

[18] Data was considered "de-identified" under the FCC's rule if the carrier (1) determines that the information is not reasonably linkable to an individual or device; (2) publicly commits to maintain and use the data in a non-individually identifiable fashion and to not attempt to re-identify the data; and (3) contractually prohibits any entity to which it discloses or permits access to the de-identified data from attempting to re-identify the data. Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Report and Order, 31 FCC Rcd 13911, ¶106 (2016), https://docs.fcc.gov/public/attachments/FCC-16-148A1_Rcd.pdf.

Strengthening breach notification. The breach notification requirements in sections 3119.15 and 3119.16 are too deferential to providers. The information that broadband providers hold about their customers is extremely accurate and personal, meaning any breach of that data should be taken very seriously and notification should be a strong default rule. Specifically, the proposal requires disclosure of a breach unless the operator "can *reasonably* determine that no harm to customers is *reasonably* likely to occur as a result of the breach." There are two "reasonableness" determinations in that language, meaning the provider has two bites at the "reasonableness" apple in determining whether to disclose data breaches. Instead of allowing so much reasonableness, the rule should require breach notification unless the operator "can determine that no harm to customers is reasonably likely."

Require an online portal for consent and data access requirements. Anytime the proposal would require something to occur in the physical world, it should also make provision for it to happen through a customer portal. Section 3119.3 requires the operator to send a stamped, self-addressed postcard that would allow removal of the customer from any lists the operator has. Section 3119.10 requires operators to provide access to customer information "at the local offices of the cable operator or at reasonable times and at a convenient place designated by the cable operator." There is simply no reason that either of these should happen strictly in the physical world. In fact, section 3119.19(c) requires the operator to provide a "simple, easy-to-use mechanism for customers to withdraw approval for participation in [a] financial incentive program at any time." The same portal could be used to comply with other provisions of the rule. Using an online portal would be far more convenient for both consumers and operators

Amend the second disclosure notice. While OTI generally favors clear, thoughtful notice of privacy practices, the separate notices required under sections 3119.8 and 3119.9 are redundant. OTI would prefer to see section 3119.9 amended to require a second notice only if there were changes between the pre-disclosure notice of section 3119.8 and the post-disclosure notice of 3119.9. This will cut down on the number of notices customers receive while still providing the same amount of information to the customer.

Make the required reports public. The proposal requires cable operators to provide several different types of reports and records in sections 3119.17, .20, and .21. These reports should be made routinely public, rather than forcing the public to file freedom of information requests every time they are filed. Either the cable companies could voluntarily make them available, or the Agency could create a website that would compile them all in one place.

Refining several definitions. Some other definitions should be amended as well. "Affiliate" is too narrowly defined. The addition of the clause "and provides any cable service or other service" cabins the definition to only affiliates that are cable or broadband providers. However, cable companies like Comcast own other companies that are not cable or broadband providers—namely NBC-Universal—yet the rule should not allow for those affiliates to use the cable systems to collect data about cable subscribers.

The definition of "subscriber" is also too narrow. While the definition appears to come from DC Code §34-1251.03(30), it creates a significant loophole: the rule would not prevent the

cable operator from collecting, using, disclosing, or selling data on people who inquired about service but never officially subscribed, or on people who were once subscribers but have since moved on. A privacy-protective rule should not include such a significant loophole.

The "personally identifiable information" definition is also incomplete. If the Agency ultimately decides not to adopt the definition in the OTI model bill, then the definition should at least mirror the FCC's definition in its 2016 rule. First, it should include any information that is linked or reasonably linkable to an individual or device. Second, it should include the following types of information: financial and health information, information pertaining to children, social security numbers, precise geo-location information, content of communications, call detail information, and web browsing history, application usage history, and the functional equivalents of either.

IV. The Agency should consult with the city of Seattle

The Agency should consult with the city of Seattle, if it has not already. In May 2017, in the immediate aftermath of the FCC broadband privacy rules repeal, Seattle enacted its own cable privacy rule[19] pursuant to its cable franchising authority.[20] The rule enacted in Seattle was similar to the rule proposed by the Agency. The Agency should consult with the city of Seattle to learn about that city's experience, and determine if there are any ways the rule can be improved beyond what has already been argued in these and other comments.

V. Conclusion

OTI supports the Agency's efforts in adopting a cable privacy rule. The Agency should improve the proposal by incorporating provisions of the OTI model bill that are not currently reflected in the rule. However, in the event the Agency does not, there are several improvements that should be made to ensure the rule has teeth and can be enforced effectively against cable providers in the District. OTI looks forward to continued engagement with the Agency as it continues to craft its final rule.

[19] ITD Director's Rule 2017-01, Seattle.gov (May 3, 2017), http://www.seattle.gov/Documents/Departments/SeattleIT/SeattleRule_ITD-2017-01.pdf.
[20] Jon Fingas, *Seattle Enacts Broadband Privacy Rules Where the FCC Won't*, Engadget (May 6, 2017), https://www.engadget.com/2017/05/06/seattle-broadband-privacy-rules.

MODEL STATE LEGISLATION

Privacy of broadband internet access service customer personal information

1. PRIVACY OF CUSTOMER PERSONAL INFORMATION. A BIAS Provider shall not use, disclose, sell, or permit access to Customer Personal Information, except as set forth below.
2. CUSTOMER CONSENT.
    a. A BIAS Provider may use, disclose, sell, or permit access to Customer Personal Information if the BIAS Provider obtains prior Opt-In Consent from the Customer, who may revoke that consent at any time.
    b. A BIAS Provider shall employ a mechanism for Customers to grant, deny, or withdraw consent that is easy to use, clear, conspicuous, comprehensible, not misleading, persistently available through all methods the BIAS Provider gives Customers for account management, in the language primarily used to conduct business with the Customer, and made available to the Customer for no additional cost.
    c. A Customer's grant, denial, or withdrawal of consent shall be given effect promptly and remain in effect until the Customer revokes or limits the grant, denial, or withdrawal of consent.
    d. A BIAS Provider shall not
        i. refuse to serve a Customer who does not provide consent under this section; or
        ii. charge a Customer a higher price or offer a Customer a discount or another benefit based on the Customer's decision to provide or not provide consent.
3. EXCEPTIONS.
    a. A BIAS Provider may use, disclose, sell, or permit access to Customer Personal Information without Customer approval in the following circumstances:
        i. For the purpose of providing BIAS from which such information is derived or for purposes necessary for the provision of such service;
        ii. To comply with legal process or other laws, court orders, or administrative orders;
        iii. To initiate, render, bill for, and collect payment for BIAS;
        iv. To protect the rights or property of the BIAS Provider or to protect BIAS Customers and other BIAS Providers from fraudulent, abusive, or unlawful use of or subscription to such BIAS;
        v. To provide location information concerning the Customer

1. to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the Customer's request for emergency services;
2. to inform the Customer's legal guardian, members of the Customer's family, or to a person reasonably believed by the BIAS Provider to be a close personal friend of the Customer, of the Customer's location in an emergency situation that involves the risk of death or serious injury; or
3. to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.

b. Unless otherwise prohibited by state law, a BIAS Provider may use, disclose, sell, or permit access to Customer Personal Information to advertise or market the BIAS Provider's communications-related services to the Customer, provided that the Customer may opt out of that use, disclosure, sale, or access at any time and the BIAS Provider provides notice to the Customer of the right to opt out in accordance with the requirements set forth in Section 6.

4. AGGREGATE CUSTOMER PERSONAL INFORMATION DATASETS. Nothing in this law restricts BIAS Providers from
   a. generating an Aggregate Customer Personal Information Dataset using Customer Personal Information; or
   b. using, disclosing, selling, or permitting access to an Aggregate Customer Personal Information Dataset it generated.
5. SECURITY OF CUSTOMER PERSONAL INFORMATION. A BIAS Provider shall implement and maintain reasonable measures to protect Customer Personal Information from unauthorized use, disclosure, sale, access, destruction, or modification.
   a. Whether security measures are reasonable shall be informed by the following factors:
      i. The nature and scope of the BIAS Provider's activities;
      ii. The sensitivity of the data it collects;
      iii. The size of the BIAS Provider; and
      iv. The technical feasibility of the measures.
   b. A BIAS Provider may employ any lawful security measures to comply with the requirement set forth in this section.
   c. A BIAS Provider shall not retain Customer Personal Information for longer than reasonably necessary to accomplish the purposes for which the information was collected, unless otherwise required by section (3) or unless the data is part of an Aggregate Customer Personal Information Dataset.
6. NOTICE. A BIAS Provider shall provide a clear, prominent, comprehensible, and not misleading notice of the requirements of subsections (1)-(5) to each of its Customers in the language primarily used to conduct business with the Customer at the point of sale

and when seeking Opt-In Consent, and it shall make the notice subsequently and persistently available through all methods the BIAS Provider gives Customers for account management.

a. The notice required by this section shall also specify and describe, or link to a resource that specifies and describes,
    i. the types of Customer Personal Information collected, how that information is used by the BIAS Provider, and how long the BIAS Provider retains the data;
    ii. the circumstances under which the BIAS Provider discloses, sells, or permits access to the information that it collects;
    iii. the categories of entities to which the BIAS Provider discloses, sells, or permits access to Customer Personal Information, and the purposes for which each category of entity will use the information; and
    iv. the Customer's right to consent with regard to the use of, disclosure of, sale of, or access to their Customer Personal Information, and how that right may be exercised.
b. A BIAS Provider shall provide advance notice of Material Changes to how it uses, discloses, sells, or permits access to Customer Personal Information or the notice required under this section and a reminder that a Customer may grant, deny, or withdraw consent at any time in manner that accords with the requirements of this section.
c. A BIAS Provider shall disclose the Customer Personal Information of the Customer, upon affirmative written request by the Customer, to any person designated by the Customer.

7. DEFINITIONS.
    a. Aggregate Customer Personal Information Dataset:
        i. Collective data that relates to a group or category of Customers, from which individual Customer identities and characteristics have been removed, and that is not linked or reasonably linkable to any individual person, household, or device.
    b. Broadband Internet Access Service or BIAS:
        i. A mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Federal Communications Commission finds to be providing a functional equivalent of the service described in this subsection.
    c. Broadband Internet Access Service Provider or BIAS Provider:
        i. A person or entity engaged in the provision of BIAS, but only insofar as the person or entity is providing BIAS.
    d. Customer:
        i. A current or former subscriber to BIAS; and

ii. An applicant for BIAS.

e. Customer Personal Information:
    i. Information collected by a BIAS provider from or about a Customer that is made available to the BIAS Provider by a Customer solely by virtue of the BIAS Provider–Customer relationship, including the following:
        1. name and billing information;
        2. government-issued identifiers, such as Social Security and driver's license numbers;
        3. other contact information, such as physical address, email address, or phone number;
        4. demographic information, such as date of birth, age, race, ethnicity, nationality, religion, political beliefs, gender, or sexual orientation;
        5. financial information, health information, or information pertaining to children;
        6. geolocation information sufficient to identify street name and name of a city or town;
        7. information that relates to the quantity, technical configuration, type, destination, location, and amount of use of the BIAS, including web browsing history, application usage history, timing of use, quantity of use, and origin and destination Internet Protocol (IP) addresses of all traffic;
        8. content of communications, which includes any part of the substance, purport, or meaning of a communication or any other part of a communication that is highly suggestive of the substance, purpose, or meaning of a communication, and includes application payload;
        9. device identifiers, such as Media Access Control (MAC) address, International Mobile Equipment Identity (IMEI) number, and IP address; and
        10. 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.
    ii. Information related to Customers that has merely had Customer identities and characteristics removed.

f. "Material Change" means any change that a Customer, acting reasonably under the circumstances, would consider important to the customer's decisions regarding the customer's privacy.

g. "Opt-In Consent" means affirmative, express Customer approval for the requested use, disclosure, sale, or access to the Customer Personal Information after the Customer is provided appropriate notification of its practices under section 6.

8. ENFORCEMENT. [States should decide what type of enforcement to include, such as private right of action, attorney general enforcement, etc.]
9. WAIVER. Any waiver by a Customer of the provisions of this law shall be deemed contrary to public policy and shall be void and unenforceable.
10. APPLICABILITY. The requirements of this law shall apply to BIAS Providers operating within [STATE] when providing BIAS to their Customers that are residents of and physically located in [STATE].
11. SEVERABILITY. The provisions of this law are severable. If any provision of this law or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application. It is the intent of the Legislature that this law would have been adopted regardless of whether an invalid provision had not been included or an invalid application had not been made.
12. AUTHORITY. [STATE] adopts [this law] pursuant to all inherent state authority under the Tenth Amendment of the United States Constitution and all relevant authority granted and preserved to the states by Title 47 of the United States Code. [If state has other authority such as general consumer protection law, add relevant statutes here.]