OTI Publishes Model State Legislation to Help States Protect Broadband Privacy

BLOG POST

Shutterstock

By **Eric Null**

Oct. 26, 2017

Last Friday marked the one-year anniversary of the Federal Communications Commission's (FCC) vote to adopt **broadband privacy rules**, providing additional privacy protections for broadband customers. However, these protections were **taken away** when Congress repealed the FCC's broadband privacy rules earlier this year.

Today, New America's Open Technology Institute (OTI) publishes **model legislation** to aid states in improving privacy protections for broadband customers. This model was drafted with the help of Chris Laughlin, at Georgetown's Institute for Public Representation, and privacy expert Laura Moy, and it is supported by **many consumer** advocacy and privacy organizations. This legislation is designed to reimplement strong broadband privacy protections and provide Americans real choices over how broadband providers like AT&T and Verizon can use, disclose, and provide access to customer information. OTI encourages states to give consumers the privacy choices they want by using this model as a basis for their own broadband privacy legislation.

The need for state action on broadband privacy

It has long been clear that broadband customers need privacy protections: broadband providers collect and see extensive and nearly comprehensive information about their customers, primarily because they own the conduit over which all internet traffic travels. That information includes web browsing records, geolocation data, financial and health information, and in some cases the content of communications. This universe of information can reveal highly personal and detailed information about a person, including race, nationality, sexual preference, religion, physical location, presence at home, personal banking details, and physical ailments. Without strong protections in place to ensure consumers have real choice and protection over their information, broadband providers would likely operate under the much less stringent "deceptiveness" standard, which allows companies to set their own agendas in densely worded, hard-to-understand privacy policies that customers rarely read.

Almost exactly one year ago, the FCC passed robust, clear broadband privacy rules focusing on consumer choice, data security, and transparency that recognized the important and unique privacy concerns that apply to broadband providers. Among other things, the rules required broadband providers to protect by default (through so-called "opt-in" consent) information the FCC deemed "sensitive." The rules protected web browsing and app usage history in addition to categories traditionally considered sensitive —such as Social Security numbers and information about health and finances. These

increased protections likely would have helped prevent people's private information from being used in unknown, intrusive, and harmful ways.

Unfortunately, Republicans in Congress repealed the broadband privacy rules earlier this year in a rushed and ill-conceived plan, before the rules could even begin protecting consumers. To repeal the rules, Congress used a blunt tool called the Congressional Review Act (CRA). The CRA, which was rarely used prior to 2017, allows Congress to repeal administrative rules in a manner that bypasses normal legislative procedure—including public hearings—and rushes the measure to a final vote with little notice to members of Congress or the public. However, despite fifteen Republicans in the House voting *against their party leadership* to retain the rules, President Trump signed the measure and the rules vanished, leaving in its wake a void of clearly articulated rules to protect broadband customer privacy.

Americans were rightfully upset over the repeal of the broadband privacy rules, which were a response to real consumer needs and desires. Consumers care deeply about their online privacy, but they have **lost control over their data** even as they have indicated they want **more control**. Absent such control, many consumers have decided to **limit** their online activity and speech because of **privacy concerns**. And specific to broadband privacy, **polls showed** that most Americans wanted the FCC's privacy rules to stay in place.

The broadband privacy rules would have put some of that control back into the hands of Americans. In particular, it would have helped protect broadband customers against broadband providers engaging in predatory advertising, a new advertising practice harmful to consumers. Predatory advertising exploits vulnerable communities from a young age, and allows companies to engage in practices like price gouging and digital redlining based on gender, race, ethnicity, income level, or other demographics. Consumers have no reason to expect they are being targeted based on these traits, but they are. For instance, low income individuals may be targeted with ads for **payday loans**. This ad practice thrives because consumers are by-and-large automatically opted in to extensive online tracking systems they may never even know about. With the FCC's rule

that required opt-in consent for use of sensitive customer data, marginalized communities had one more protection in place to prevent these predatory practices from occurring.

Now, without strong rules protecting consumers, states have the opportunity to fill the void left by Congress and provide clear rules-of-the-road when it comes to protecting the privacy of broadband customers. Our **model language**, described below, is a starting point for states that are ready to protect the privacy rights of their citizens. **Twenty-two states** have already introduced broadband privacy legislation, many relying on different language and different sources of authority. Our model legislation, too, is designed to be customized so that states can modify provisions to account for laws that already exist and the level of authority each state has over consumer protection.

OTI's model legislation

Since Congress repealed the broadband privacy rules, OTI has closely consulted with states 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 that adopt language similar to the FCC's rule (like **California and the District of Columbia**), this model language improves on some areas where OTI determined the FCC's rule did not fully protect consumers.

The model language takes a comprehensive approach to protecting broadband privacy. Rather than separate buckets of sensitive and non-sensitive data (the approach used in the FCC rules and by the Federal Trade Commission with respect to other industries), the model requires broadband providers to protect *all* information they collect by default. The model does that 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, 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 is AT&T's **now-defunct broadband internet plan** that cost $30 less per month in exchange for an invasion of privacy. 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 customers to make a reasoned choice about their privacy.

The exceptions included in the model allow for 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 is individualized, making it **much easier** for **that data** to be **associated** with an **individual**. For the advertising of communications-related services exception, the model 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.

As our **allies have argued**, broadband providers and online content companies have deceived the public about previous state attempts to protect broadband privacy by releasing a specious **letter** and **advertisement**. These arguments have no place in this debate and at any rate do not apply to this model. The arguments, made specifically against California's **AB 375**, include the following:

> (1) the bill lacked a clear definition of what businesses the bill covers;
> (2) the bill would lead to recurring pop-ups that would desensitize consumers and "give opportunities to hackers"; and

(3) the bill would prevent broadband providers from using information they have long relied on to prevent cybersecurity attacks and improve their service.

First, the model language (and AB 375) clearly applies only to broadband internet access service providers, not edge providers or any other online content company by virtue of its definition of "BIAS" and "BIAS Provider" in Section 7(b) and (c). Second, the bill does not require any pop-ups, but merely a common-sense requirement that broadband providers allow customers to opt-in via an online portal (most broadband providers *already offer* such online portals to their customers). A broadband provider could choose to use pop-ups as one way to obtain consent, but given their argument in the letter, any such use of pop-ups would be an irresponsible way to obtain that consent. Third, the model unequivocally allows broadband providers to monitor their network for the purpose of protecting security and improving service. At least two provisions of the model apply there: Section 3(a)(i) (allowing for use of information for providing BIAS or for purposes necessary for provision of BIAS) and Section 3(a)(iv) (allowing for use of information "[t]o 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"). Thus, these attempts to mislead the public lack merit and should be ignored.

States have the opportunity to correct Congress's mistake in repealing the broadband privacy rules. This model will hopefully start or help further those conversations within state legislatures. OTI looks forward to being part of those discussions.