Broadband ISP Privacy Act of 2018

An Act to foster competition in local Internet service and to provide consumers with meaningful choice about the collection and use of their private information.

SECTION 1. FINDINGS.

(1) Internet service providers (ISPs) are an essential link for Americans to access the Internet.

(2) ISPs exert significant market power because they operate large physical infrastructures that are expensive and difficult to replicate.

(3) The cost of replicating this investment is insurmountable to many new potential entrants, and mobile and satellite Internet is not a viable replacement for broadband.

(4) The high cost of competing prevents entrants from competing with incumbent ISPs.

(5) The lack of competition in the broadband market means consumers have little to no choice about how companies treat their personal information, and prevents consumers from exercising control over how their data is used.

(6) Encouraging competition between ISPs will allow consumers to choose which company to use based on criteria chosen by the consumer, such as privacy practices.

(7) Requiring ISPs to display privacy policies and obtain affirmative consent from consumers will raise consumer awareness of how their information is being used.

(8) Prohibiting ISPs from penalizing or enticing consent or lack of consent means users have true control over how their information is collected, used, and distributed.

SEC. 2. DEFINITIONS.

In this Act—

(1) "Broadband Internet access service" means 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 state Attorney General finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this part.

(2) "ISP" means a provider of broadband Internet access service that has entered into a franchise agreement, right-of-way agreement, or any other agreement with the state or a municipality within the state, or uses facilities subject to those agreements, even if the ISP is not party to the agreements.

(3) “Customer” means anyone currently or formerly subscribed to or applying to subscribe to services provided by an ISP.

(4) “Customer proprietary information” means any of the following an ISP acquires from a customer in connection with the ISP’s provision of Internet or related services:

(a) Contents of communication;

(b) Call detail information;

(c) Precise geolocation information;

(d) Web browsing history, application usage history, and the functional equivalents of either;

(e) MAC addresses and other device identifiers; and

(f) Other personally identifiable information, which consists of any information that is linked or reasonably linkable to an individual or device.

(5) “Local loop” means the physical wiring or cabling in the broadband Internet network that connects the customer’s premises to facilities owned, maintained, or otherwise operated by the ISP for the provision of broadband Internet service. The term also includes any facilities or information necessary to make full use of the local loop for broadband Internet access services.

SEC. 3. UNBUNDLING.

By no later than 180 days after the passage of this Act, each ISP must—

(1) Provide nondiscriminatory access to its local loop to any requesting ISP so long as the requesting ISP demonstrates that it intends to use those elements for the provision of broadband Internet access service.

(2) Provide such access on an unbundled basis, and allow access to each network element in a manner that allows the requesting ISP to combine and operate the elements in order to provide broadband Internet access service.

(3) Provide access to its network elements on rates, terms, and conditions that are just, reasonable, and nondiscriminatory.

SEC. 4. OPT-IN CONSENT.

(1) Consent—An ISP may only collect, use, disclose, sell, or permit access to customer proprietary information with the opt-in consent described below or pursuant to the exceptions listed below.

(a) Except as otherwise provided in this section, an ISP shall obtain opt-in consent from a customer in order to:

(i) collect, use, disclose, sell, or permit third-party access to any of the customer's proprietary information; or

(ii) make any material retroactive change that would result in a use, disclosure, or permission of access to any of the customer's proprietary information previously collected by the provider for which the customer did not previously grant approval.

(b) An ISP shall, at a minimum, solicit customer opt-in consent at the point of sale of a service and at any such time that the ISP makes any material change to its privacy or data-use policy or policies. Such solicitation of the customer must be clear, conspicuous, and in language that is comprehensible and not misleading.

(2) Soliciting Consent—An ISP must assume that a customer does not consent to the use of the customer's proprietary information, and the ISP must solicit the customer in order to obtain that consent.

(a) Whenever an ISP solicits a customer for opt-in consent, the ISP must disclose to the customer:

(i) The types of information the ISP is seeking to use, disclose, or permit access to; and

(ii) The purposes for which that information will be used, including likely recipients of the customer proprietary information.

(b) The solicitation of customer approval must be available in any language other than English indicated by a customer as the customer's primary language.

(c) The solicitation of customer approval must make clear that the customer has the right to withhold consent without suffering any adverse consequences from the ISP.

(d) An ISP shall provide the mechanism by which the customer may provide or withhold consent to the customer free of charge in an accessible format.

(e) An ISP must promptly give effect to the customer's grant, denial, or withdrawal of consent promptly and continue to honor the customer's choice until the customer revokes, limits, or modifies the grant, denial, or withdrawal of consent.

(3) Exceptions—An ISP may collect, use, disclose, sell, or permit access to customer proprietary information without customer approval for the following purposes:

(a) in its provision of internet service or services necessary to the internet service of the customer;

(b) to bill and collect payment for internet service;

(c) to protect the rights or property of the ISP;

(d) to protect users of the internet service and other ISPs from fraudulent, abusive, or unlawful use of the service;

(e) to provide any inbound marketing or administrative services to the customer if such service was requested by the customer;

(f) to provide location information or other customer proprietary information to:

(i) respond to the customer's request for emergency services;

(ii) nform the customer's legal guardian or immediate family of the customer's location in an emergency situation that involves the risk of death or serious physical harm; or

(iii) providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency;

(g) to law enforcement in the event of a crime or other emergency; or

(h) as otherwise required or authorized by law.

SEC. 5. PROHIBITED BUSINESS PRACTICES.

(1) An ISP may not withhold or deny service to any customer based on the customer withholding consent required under section 4.

(2) An ISP may not charge a customer a higher price for a service based on the customer withholding consent required under section 4.

(3) An ISP shall not offer to exchange a discount price or other service in return for a customer providing or not providing consent required under section 4.

SEC. 6. ENFORCEMENT.

(1) In the case of a violation of this Act, the state Attorney General may issue an injunction to enjoin the practice found to be in violation of the Act. If a court finds that an ISP has violated any provision in this Act, the court shall issue an injunction enjoining any such further violations of the Act without requiring a finding that any individual was in fact harmed by the violation.

(a) While an injunction described in subsection 1 is in force against an ISP, that ISP shall, every six months, provide to the state Attorney General a report detailing its practices for ensuring compliance with the Act. This order shall be in effect until such time that the Attorney General represents to the court that the order is no longer necessary.

(b) If an ISP is found to be in violation of this Act after such time as an injunction has been issued against it under subsection 1, further violations of the Act shall be punishable by fines not to exceed 4% of the ISPs annual revenue attributable to its provision of broadband Internet access service.

(2) The state Attorney General may, in addition to remedies permitted in subsection 1, commence an action in state court against the ISP to recover $500,000 for the first violation and $1,000,000 for each subsequent violation.

(3) A customer whose customer personal information is disclosed or sold or to which access is granted in violation of section 4 of this Act, or whose service was affected in availability or pricing in violation of section 5 of this Act, shall have a private right of action against the ISP that disclosed, sold or permitted access to the customer personal information and shall be entitled to recover up to $500,000.