BILL REQUEST - CODE REVISER'S OFFICE

BILL REQ. #: H-2560.2/17 2nd draft

ATTY/TYPIST: ML:lel

BRIEF DESCRIPTION: Protecting the privacy and security of internet users.

AN ACT Relating to protecting the privacy and security of internet users; amending RCW 19.255.010; adding a new chapter to Title 19 RCW; providing effective dates; and providing an expiration date.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. **Sec. 1.** The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Broadband internet access service" or "BIAS" 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 federal communications commission finds to be providing a functional equivalent of the service described in this subsection.

(2) "Broadband internet access service provider" or "BIAS provider" means a person engaged in the provision of BIAS.

(3) "Customer" means: (a) A current or former subscriber to a BIAS; or (b) an applicant for a BIAS.

(4) "Customer proprietary information" or "customer PI" means any of the following a carrier acquires in connection with its provision of BIAS:

(a) Individually identifiable customer proprietary network information;

(b) Personally identifiable information; and

(c) Content of communication.

(5) "Customer proprietary network information" or "CPNI" has the same meaning given to that term in section 222(h)(1) of the communications act of 1934, as amended (47 U.S.C. Sec. 222(h)(1)).

(6) "Material change" means any change that a consumer, acting reasonably under the circumstances, would consider important to his or her decisions regarding his or her privacy, including any change to information required by the privacy notice described in section 2 of this act.

(7) "Opt-in approval" means a method for obtaining customer consent to use, disclose, or permit access to the customer's proprietary information. This approval method requires that the carrier obtain from the customer affirmative, express consent allowing the requested usage, disclosure, or access to the customer proprietary information after the customer is provided appropriate notification of the carrier's request consistent with the requirements set forth in this chapter.

(8) "Opt-out approval" means a method for obtaining customer consent to use, disclose, or permit access to the customer's proprietary information. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's proprietary information if the customer has failed to object thereto after the customer is provided appropriate notification of the carrier's request for consent consistent with the requirements set forth in this chapter.

(9) "Person" has the same meaning given that term in section 3 of the federal communications act of 1934, as amended (47 U.S.C. Sec. 153).

(10) "Personally identifiable information" or "PII" means any information that is linked or reasonably linkable to an individual or device.

(11) "Sensitive customer proprietary information" or "sensitive PII" includes:

(a) Financial information;

(b) Health information;

(c) Information pertaining to children;

(d) Social security numbers;

(e) Precise geolocation information;

(f) Content of communications;

(g) Call detail information; and

(h) Web browsing history, application usage history, and the functional equivalents of either.

(12) "Small broadband internet access service provider" or "small BIAS provider" means a provider with one hundred thousand or fewer broadband connections, aggregated over all the provider's affiliates whether within or outside the state.

NEW SECTION. **Sec. 2.** (1) A BIAS provider must notify its customers of its privacy policies. The notice must be clear and conspicuous and in language that is comprehensible and not misleading.

(2) A BIAS provider's notice of its privacy policies under subsection (1) of this section must:

(a) Specify and describe the types of customer proprietary information that the BIAS provider collects by virtue of its provision of BIAS and how it uses that information;

(b) Specify and describe under what circumstances the BIAS provider discloses or permits access to each type of customer proprietary information that it collects;

(c) Specify and describe the categories of entities to which the BIAS provider discloses or permits access to customer proprietary information and the purposes for which the customer proprietary information will be used by each category of entities;

(d) Specify and describe that customers' opt-in approval to use, disclose, or permit access to customer proprietary information will not affect the provision of any BIAS of which he or she is a customer;

(i) That a customer's denial or withdrawal of approval to use, disclose, or permit access to customer proprietary information will not affect the provision of any BIAS of which he or she is a customer; and

(ii) That any grant, denial, or withdrawal of approval for the use, disclosure, or permission of access to the customer proprietary information is valid until the customer affirmatively revokes the

grant, denial, or withdrawal, and inform the customer of his or her right to deny or withdraw access to the proprietary information at any time;

(e) Provide access to a mechanism for customers to grant, deny, or withdraw approval for the BIAS provider to use, disclose, or provide access to customer proprietary information as required by section 3 of this act;

(f) Be completely translated into a language other than English if the BIAS provider transacts business with the customer in that language.

(3) Notice required under subsection (1) of this section must:

(a) Be made available to prospective customers at the point of sale, prior to the purchase of service, whether the point of sale is in person, online, over the telephone, or via another means; and

(b) Be made persistently available through: A clear and conspicuous link on the BIAS provider's homepage; the carrier's mobile application, if it provides one for account management purposes; and any functional equivalent to the carrier's homepage or mobile application. If a carrier does not have a web site, it must provide notice to customers in paper form or another format agreed upon by the customer.

(4) A BIAS provider must provide existing customers with advance notice of one or more material changes to the carrier's privacy policies. The advance notice must be clear and conspicuous, and in language that is comprehensible and not misleading, and must:

(a) Be provided through email or another means of active communication agreed upon by the customer;

(b) Specify and describe:

(i) The changes made to the BIAS provider's privacy policies, including any changes to what customer proprietary information the carrier collects, and how it uses, discloses, or permits access to such information, the categories of entities to which it discloses or permits access to customer proprietary information, and which, if any, changes are retroactive; and

(ii) Customers' opt-in approval and/or opt-out approval rights with respect to their customer proprietary information, including the material specified in subsection (2)(d) of this section;

(c) Provide access to a mechanism for customers to grant, deny, or withdraw approval for the BIAS provider to use, disclose, or

permit access to customer proprietary information as required by section 3 of this act;

(d) Be completely translated into a language other than English if the telecommunications carrier transacts business with the customer in that language.

(5) Small BIAS providers are exempt from the requirements of this section until July 1, 2019.

NEW SECTION. **Sec. 3.** (1) Except as described in subsection (2) of this section, a BIAS provider may not use, disclose, or permit access to customer proprietary information except with the opt-out or opt-in approval of a customer as described in this section.

(2) A BIAS provider may use, disclose, or permit access to customer proprietary information without customer approval for the following purposes:

(a) In its provision of the internet access service from which such information is derived, or in its provision of services necessary to, or used in, the provision of such service.

(b) To initiate, render, bill, and collect for internet access service.

(c) To protect the rights or property of the BIAS provider, or to protect users of the internet access service and other providers from fraudulent, abusive, or unlawful use of the service.

(d) To provide any inbound marketing, referral, or administrative services to the customer for the duration of a real-time interaction, if such an interaction was initiated by the customer.

(e) To provide either location information or nonsensitive customer proprietary information, or both, to:

(i) 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 user's request for emergency services;

(ii) Inform the user's legal guardian or members of the user's immediate family of the user'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.

(f) As otherwise required or authorized by law.

(3) Except as otherwise provided in this section, a BIAS provider must obtain opt-out approval from a customer to use, disclose, or permit access to any of the customer's nonsensitive customer proprietary information. If it so chooses, a BIAS provider may instead obtain opt-in approval from a customer to use, disclose, or permit access to any of the customer's nonsensitive customer proprietary information.

(4) Except as otherwise provided in this section, a BIAS provider must obtain opt-in approval from a customer to:

(a) Use, disclose, or permit access to any of the customer's sensitive customer proprietary information; or

(b) Make any material retroactive change. For purposes of this section, a material retroactive change means a material change that would result in a use, disclosure, or permission of access to any of the customer's proprietary information previously collected by the BIAS provider for which the customer did not previously grant approval, either through opt-in or opt-out consent, as required by subsections (3) and (4) of this section.

(5) Except as described in subsection (2) of this section, a BIAS provider must at a minimum solicit customer approval pursuant to either subsection (3) or (4) of this section, or both, as applicable, at the point of sale and when making one or more material changes to privacy policies. The solicitation may be part of, or the same communication as, a notice required by section 2 of this act.

(6) A BIAS provider's solicitation of customer approval must be clear and conspicuous and in language that is comprehensible and not misleading. The solicitation must disclose:

(a) The types of customer proprietary information for which the BIAS provider is seeking customer approval to use, disclose, or permit access to;

(b) The purposes for which the customer proprietary information will be used;

(c) The categories of entities to which the BIAS provider intends to disclose or permit access to such customer proprietary information; and

(d) A means to easily access the notice required by section 2(1) of this act and a means to access the mechanism required by subsection (8) of this section.

(7) A BIAS provider's solicitation of customer approval must be completely translated into a language other than English if the BIAS provider transacts business with the customer in that language.

(8) A BIAS provider must make available a simple, easy-to-use mechanism for customers to grant, deny, or withdraw both opt-in approval or opt-out approval at any time. The mechanism must be clear and conspicuous, in language that is comprehensible and not misleading, and made available at no additional cost to the customer. The mechanism must be persistently available on or through the BIAS provider's web site; the BIAS provider's mobile application, if it provides one for account management purposes; and any functional equivalent to the BIAS provider's homepage or mobile application. If a BIAS provider does not have a web site, it must provide a persistently available mechanism by another means such as a toll-free telephone number. The customer's grant, denial, or withdrawal of approval must be given effect promptly and remain in effect until the customer revokes or limits such grant, denial, or withdrawal of approval.

(9) Customer consent to or approval of the activities described in this section obtained prior to the effective date of this section is considered to be in compliance with the requirements of this section. BIAS providers that have obtained such consent or approval are not required to obtain new consent or approval for the same activities.

(10) Small BIAS providers are exempt from the requirements of this section until July 1, 2019.

NEW SECTION. **Sec. 4.** (1) A BIAS provider must take reasonable measures to protect customer PI from unauthorized use, disclosure, or access.

(2) The security measures taken by a BIAS provider to implement subsection (1) of this section must appropriately take into account each of the following factors:

(a) The nature and scope of the BIAS provider's activities;

(b) The sensitivity of the data it collects;

(c) The size of the BIAS provider; and

(d) Technical feasibility.

(3) A BIAS provider may employ any lawful security measures that allow it to implement the requirement set forth in this section.

NEW SECTION. **Sec. 5.** (1) A BIAS provider must not condition, or effectively condition, provision of BIAS on a customer's agreement to waive privacy rights guaranteed by law or rule, including this chapter. A BIAS provider must not terminate service or otherwise refuse to provide BIAS as a direct or indirect consequence of a customer's refusal to waive any such privacy rights.

(2) A BIAS provider that offers a financial incentive, such as lower monthly rates, in exchange for a customer's approval to use, disclose, or permit access to the customer's proprietary information must do all of the following:

(a) Provide notice explaining the terms of any financial incentive program that is clear and conspicuous, and in language that is comprehensible and not misleading. The notice must be provided both at the time the program is offered and at the time a customer elects to participate in the program. The notice must:

(i) Explain that the program requires opt-in approval to use, disclose, or permit access to customer PI;

(ii) Include information about what customer PI the provider will collect, how it will be used, and with what categories of entities it will be shared and for what purposes;

(iii) Be easily accessible and separate from any other privacy notifications, including but not limited to any privacy notifications required by this chapter;

(iv) Be completely translated into a language other than English if the BIAS provider transacts business with the customer in that language; and

(v) Provide at least as prominent information to customers about the equivalent service plan that does not necessitate the use, disclosure, or access to customer PI beyond that required or permitted by law or rule, including under this chapter.

(b) Obtain customer opt-in approval in accordance with section 3(4) of this act for participation in any financial incentive program.

(c) If customer opt-in approval is given, the BIAS provider must make available a simple, easy-to-use mechanism for customers to withdraw approval for participation in such a financial incentive program at any time. The mechanism must be clear and conspicuous, in language that is comprehensible and not misleading, and must be persistently available on or through the BIAS provider's web site; the BIAS provider's mobile application if it provides one for account

management purposes; and any functional equivalent to the BIAS provider's homepage or mobile application. If a BIAS provider does not have a web site, it must provide a persistently available mechanism by another means such as a toll-free telephone number.

NEW SECTION. **Sec. 6.** The legislature finds that the practices covered by this chapter are matters affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. A violation of this chapter is not reasonable in relation to the development and preservation of business and constitutes an unfair or deceptive act or practice in the conduct of trade or commerce and unfair method of competition for purposes of applying the consumer protection act, chapter 19.86 RCW.

NEW SECTION. **Sec. 7.** The consumer privacy and security account is created in the state treasury. All receipts from recoveries by the office of the attorney general for lawsuits related to the consumer protection act under the provisions of this chapter, or otherwise designated to this account must be deposited into the account. Moneys in the account may be spent only after appropriation. Expenditures from the account may be used only for costs incurred by the office of the attorney general in the administration and enforcement of this chapter.

NEW SECTION. **Sec. 8.** (1) In consultation with the utilities and transportation commission, the office of data and privacy protection, and the department of commerce, the office of the attorney general shall review and analyze additional opportunities to increase consumer privacy transparency, control, and protection through the regulation of additional industry categories engaged in the provision of internet or mobile content or services. The office of the attorney general shall report its findings to the appropriate committees of the legislature by December 1, 2020.

(2) This section expires July 1, 2021.

Sec. 9. RCW 19.255.010 and 2015 c 64 s 2 are each amended to read as follows:

(1) Any person or business that conducts business in this state and that owns or licenses data that includes personal information, or operates as a BIAS provider as defined under section 1 of this act,

shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.

(2) Any person or business that maintains data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(3) The notification required by this section may be delayed if the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(4) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.

(5) For purposes of this section, "personal information" <u>for a business or person that is not operating as a BIAS provider as defined under section 1 of this act</u> means an individual's first name or first initial and last name in combination with any one or more of the following data elements:

(a) Social security number;

(b) Driver's license number or Washington identification card number; or

(c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(6) For purposes of this section, "personal information" for a person or business operating as a BIAS provider as defined under section 1 of this act has the same meaning as "customer proprietary information" as defined in section 1 of this act, and includes "sensitive customer proprietary information" as defined in section 1 of this act.

(7) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

((~~(7)~~)) (8) For purposes of this section, "secured" means encrypted in a manner that meets or exceeds the national institute of standards and technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.

((~~(8)~~)) (9) For purposes of this section and except under subsections ((~~(9) and~~)) (10) and (11) of this section, "notice" may be provided by one of the following methods:

(a) Written notice;

(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001; or

(c) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(i) Email notice when the person or business has an email address for the subject persons;

(ii) Conspicuous posting of the notice on the web site page of the person or business, if the person or business maintains one; and

(iii) Notification to major statewide media.

((~~(9)~~)) (10) A person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section is in compliance with

the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

((~~(10)~~)) (11) A covered entity under the federal health insurance portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et seq., is deemed to have complied with the requirements of this section with respect to protected health information if it has complied with section 13402 of the federal health information technology for economic and clinical health act, Public Law 111-5 as it existed on July 24, 2015. Covered entities shall notify the attorney general pursuant to subsection ((~~(15)~~)) (16) of this section in compliance with the timeliness of notification requirements of section 13402 of the federal health information technology for economic and clinical health act, Public Law 111-5 as it existed on July 24, 2015, notwithstanding the notification requirement in subsection ((~~(16)~~)) (17) of this section.

((~~(11)~~)) (12) A financial institution under the authority of the office of the comptroller of the currency, the federal deposit insurance corporation, the national credit union administration, or the federal reserve system is deemed to have complied with the requirements of this section with respect to "sensitive customer information" as defined in the interagency guidelines establishing information security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part 364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, as they existed on July 24, 2015, if the financial institution provides notice to affected consumers pursuant to the interagency guidelines and the notice complies with the customer notice provisions of the interagency guidelines establishing information security standards and the interagency guidance on response programs for unauthorized access to customer information and customer notice under 12 C.F.R. Part 364 as it existed on July 24, 2015. The entity shall notify the attorney general pursuant to subsection ((~~(15)~~)) (16) of this section in addition to providing notice to its primary federal regulator.

((~~(12)~~)) (13) Any waiver of the provisions of this section is contrary to public policy, and is void and unenforceable.

((~~(13)~~))(14)(a) Any consumer injured by a violation of this section may institute a civil action to recover damages.

(b) Any person or business that violates, proposes to violate, or has violated this section may be enjoined.

(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

((~~(14)~~)) (15) Any person or business that is required to issue notification pursuant to this section shall meet all of the following requirements:

(a) The notification must be written in plain language; and

(b) The notification must include, at a minimum, the following information:

(i) The name and contact information of the reporting person or business subject to this section;

(ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach; and

(iii) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.

((~~(15)~~)) (16) Any person or business that is required to issue a notification pursuant to this section to more than five hundred Washington residents as a result of a single breach shall, by the time notice is provided to affected consumers, electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the attorney general. The person or business shall also provide to the attorney general the number of Washington consumers affected by the breach, or an estimate if the exact number is not known.

((~~(16)~~)) (17) Notification to affected consumers and to the attorney general under this section must be made in the most expedient time possible and without unreasonable delay, no more than forty-five calendar days after the breach was discovered, unless at the request of law enforcement as provided in subsection (3) of this section, or due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

((~~(17)~~)) (18) The attorney general may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce this section. For actions brought by the attorney general to enforce this section, the legislature finds that the practices covered by this section are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. For actions brought by the

attorney general to enforce this section, a violation of this section is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for purposes of applying the consumer protection act, chapter 19.86 RCW. An action to enforce this section may not be brought under RCW 19.86.090.

NEW SECTION. **Sec. 10.** Sections 4 and 9 of this act take effect January 1, 2018.

NEW SECTION. **Sec. 11.** Sections 2 and 3 of this act take effect July 1, 2018.

NEW SECTION. **Sec. 12.** If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected.

NEW SECTION. **Sec. 13.** Sections 1 through 8 of this act constitute a new chapter in Title 19 RCW.

--- END ---