
HOUSE BILL 2200

State of Washington

65th Legislature

2017 Regular Session

By Representatives Hansen, Taylor, Smith, Buys, Harmsworth, Graves, Maycumber, J. Walsh, Kraft, Haler, Condotta, Nealey, Bergquist, Steele, Van Werven, Stonier, Macri, Farrell, Cody, Slatter, Tarleton, Senn, Kagi, Pollet, Frame, Chapman, Dye, Hudgins, Stanford, Reeves, Dent, Hayes, Ryu, Peterson, Sells, Kloba, Santos, Johnson, Fitzgibbon, Holy, Ormsby, Caldier, Sawyer, Wylie, Hargrove, Kilduff, Blake, Orcutt, Gregerson, Young, Appleton, Shea, Koster, Morris, Tharinger, Irwin, Muri, Schmick, Volz, Goodman, Clibborn, McCaslin, Pellicciotti, Doglio, Jinkins, Dolan, Kirby, Sullivan, Lytton, Kretz, Riccelli, Rodne, McBride, McCabe, and Pettigrew

Read first time 04/05/17. Referred to Committee on Technology & Economic Development.

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

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

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

9 (1) "Broadband internet access service" or "BIAS" means a mass-
10 market retail service by wire or radio that provides the capability
11 to transmit data to and receive data from all or substantially all
12 internet endpoints, including any capabilities that are incidental to
13 and enable the operation of the communications service, but excluding
14 dial-up internet access service. This term also encompasses any
15 service that the federal communications commission finds to be
16 providing a functional equivalent of the service described in this
17 subsection.

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

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

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

4 (a) Individually identifiable customer proprietary network
5 information;

6 (b) Personally identifiable information; and

7 (c) Content of communication.

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

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

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

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

32 (9) "Person" has the same meaning given that term in section 3 of
33 the federal communications act of 1934, as amended (47 U.S.C. Sec.
34 153).

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

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

40 (a) Financial information;

1 (b) Health information;
2 (c) Information pertaining to children;
3 (d) Social security numbers;
4 (e) Precise geolocation information;
5 (f) Content of communications;
6 (g) Call detail information; and
7 (h) Web browsing history, application usage history, and the
8 functional equivalents of either.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

28 (b) Specify and describe:

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

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

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

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

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

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

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

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

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

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

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

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

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

28 (i) A public safety answering point, emergency medical service
29 provider or emergency dispatch provider, public safety, fire service,
30 or law enforcement official, or hospital emergency or trauma care
31 facility, in order to respond to the user's request for emergency
32 services;

33 (ii) Inform the user's legal guardian or members of the user's
34 immediate family of the user's location in an emergency situation
35 that involves the risk of death or serious physical harm; or

36 (iii) Providers of information or database management services
37 solely for purposes of assisting in the delivery of emergency
38 services in response to an emergency.

39 (f) As otherwise required or authorized by law.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 33 (a) The nature and scope of the BIAS provider's activities;
- 34 (b) The sensitivity of the data it collects;
- 35 (c) The size of the BIAS provider; and
- 36 (d) Technical feasibility.

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

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

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

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

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

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

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

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

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

31 (b) Obtain customer opt-in approval in accordance with section
32 3(4) of this act for participation in any financial incentive
33 program.

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

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

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

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

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

31 (2) This section expires July 1, 2021.

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

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

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

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

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

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

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

38 (a) Social security number;

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

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

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

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

14 (~~(7)~~) (8) For purposes of this section, "secured" means
15 encrypted in a manner that meets or exceeds the national institute of
16 standards and technology (NIST) standard or is otherwise modified so
17 that the personal information is rendered unreadable, unusable, or
18 undecipherable by an unauthorized person.

19 (~~(8)~~) (9) For purposes of this section and except under
20 subsections (~~(9) and~~) (10) and (11) of this section, "notice" may
21 be provided by one of the following methods:

22 (a) Written notice;

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

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

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

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

36 (iii) Notification to major statewide media.

37 (~~(9)~~) (10) A person or business that maintains its own
38 notification procedures as part of an information security policy for
39 the treatment of personal information and is otherwise consistent
40 with the timing requirements of this section is in compliance with

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

4 ~~((+10+))~~ (11) A covered entity under the federal health insurance
5 portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et
6 seq., is deemed to have complied with the requirements of this
7 section with respect to protected health information if it has
8 complied with section 13402 of the federal health information
9 technology for economic and clinical health act, Public Law 111-5 as
10 it existed on July 24, 2015. Covered entities shall notify the
11 attorney general pursuant to subsection ~~((+15+))~~ (16) of this section
12 in compliance with the timeliness of notification requirements of
13 section 13402 of the federal health information technology for
14 economic and clinical health act, Public Law 111-5 as it existed on
15 July 24, 2015, notwithstanding the notification requirement in
16 subsection ~~((+16+))~~ (17) of this section.

17 ~~((+11+))~~ (12) A financial institution under the authority of the
18 office of the comptroller of the currency, the federal deposit
19 insurance corporation, the national credit union administration, or
20 the federal reserve system is deemed to have complied with the
21 requirements of this section with respect to "sensitive customer
22 information" as defined in the interagency guidelines establishing
23 information security standards, 12 C.F.R. Part 30, Appendix B, 12
24 C.F.R. Part 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12
25 C.F.R. Part 364, Appendix B, and 12 C.F.R. Part 748, Appendices A and
26 B, as they existed on July 24, 2015, if the financial institution
27 provides notice to affected consumers pursuant to the interagency
28 guidelines and the notice complies with the customer notice
29 provisions of the interagency guidelines establishing information
30 security standards and the interagency guidance on response programs
31 for unauthorized access to customer information and customer notice
32 under 12 C.F.R. Part 364 as it existed on July 24, 2015. The entity
33 shall notify the attorney general pursuant to subsection ~~((+15+))~~
34 (16) of this section in addition to providing notice to its primary
35 federal regulator.

36 ~~((+12+))~~ (13) Any waiver of the provisions of this section is
37 contrary to public policy, and is void and unenforceable.

38 ~~((+13+))~~(14)(a) Any consumer injured by a violation of this
39 section may institute a civil action to recover damages.

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

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

6 (~~(14)~~) (15) Any person or business that is required to issue
7 notification pursuant to this section shall meet all of the following
8 requirements:

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

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

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

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

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

18 (~~(15)~~) (16) Any person or business that is required to issue a
19 notification pursuant to this section to more than five hundred
20 Washington residents as a result of a single breach shall, by the
21 time notice is provided to affected consumers, electronically submit
22 a single sample copy of that security breach notification, excluding
23 any personally identifiable information, to the attorney general. The
24 person or business shall also provide to the attorney general the
25 number of Washington consumers affected by the breach, or an estimate
26 if the exact number is not known.

27 (~~(16)~~) (17) Notification to affected consumers and to the
28 attorney general under this section must be made in the most
29 expedient time possible and without unreasonable delay, no more than
30 forty-five calendar days after the breach was discovered, unless at
31 the request of law enforcement as provided in subsection (3) of this
32 section, or due to any measures necessary to determine the scope of
33 the breach and restore the reasonable integrity of the data system.

34 (~~(17)~~) (18) The attorney general may bring an action in the
35 name of the state, or as parens patriae on behalf of persons residing
36 in the state, to enforce this section. For actions brought by the
37 attorney general to enforce this section, the legislature finds that
38 the practices covered by this section are matters vitally affecting
39 the public interest for the purpose of applying the consumer
40 protection act, chapter 19.86 RCW. For actions brought by the

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

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

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

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

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

--- END ---