SECOND SUBSTITUTE HOUSE BILL 1503

State of Washington   **66th Legislature**   **2019 Regular Session**

By House Appropriations (originally sponsored by Representatives Smith, Hudgins, and Stanford)

READ FIRST TIME 03/01/19.

1   AN   ACT   Relating   to   registration   and   consumer   protection
2 obligations of data brokers; adding a new chapter to Title 19 RCW;
3 creating a new section; prescribing penalties; providing an effective
4 date; and providing an expiration 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)(a) "Brokered personal information" means one or more of the
10 following computerized data elements about a consumer, if categorized
11 or organized for dissemination to third parties:
12   (i) Name;
13   (ii) Address;
14   (iii) Date of birth;
15   (iv) Place of birth;
16   (v) Mother's maiden name;
17   (vi) Unique biometric data generated from measurements or
18 technical analysis of human body characteristics used by the owner or
19 licensee of the data to identify or authenticate the consumer, such
20 as a fingerprint, retina or iris image, or other unique physical
21 representation or digital representation of biometric data;

(vii) Name or address of a member of the consumer's immediate family or household;

(viii) Social security number or other government-issued identification number; or

(ix) Other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty.

(b) "Brokered personal information" does not include publicly available information to the extent that it is related to a consumer's business or profession.

(2) "Business" means a commercial entity, including a sole proprietorship, partnership, corporation, association, limited liability company, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of Washington state, or any other state, the United States, or any other country, or the parent, affiliate, or subsidiary of a financial institution, but it does not include the state, any political subdivision of the state, or a vendor acting solely on behalf of, and at the direction of, the state.

(3) "Chief privacy officer" means the person appointed under RCW 43.105.369(2).

(4) "Consumer" means an individual residing in this state.

(5)(a) "Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.

(b) The following activities conducted by a business, and the collection and sale or licensing of brokered personal information incidental to conducting those activities, does not qualify the business as a data broker:

(i) Providing publicly available information via real-time or near real-time alert services for health or safety purposes; or

(ii) Providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier.

(c) The phrase "sells or licenses" does not include:

(i) A one-time or occasional sale of assets that is not part of the ordinary conduct of the business; or

1   (ii) A sale or license of data that is merely incidental to the
2 business.

3   (6) "Encryption" means use of an algorithmic process to transform
4 data into a form in which the data is rendered unreadable or unusable
5 without the use of a confidential process or key.

6   (7) "License" means a grant of access to, or distribution of,
7 data by one person to another in exchange for consideration. A use of
8 data for the sole benefit of the data provider, where the data
9 provider maintains control over the use of the data, is not a
10 license.

11   (8)(a) "Personally identifiable information" means a consumer's
12 first name or first initial and last name in combination with any one
13 or more of the following digital data elements, when either the name
14 or the other data elements are not encrypted or redacted or protected
15 by another method that renders them unreadable or unusable by
16 unauthorized persons:

17   (i) Social security number;

18   (ii) Motor vehicle operator's license number or nondriver
19 identification card number;

20   (iii) Financial account number or credit or debit card number;

21   (iv) Account passwords or personal identification numbers or
22 other access codes for a financial account.

23   (b) "Personally identifiable information" does not mean publicly
24 available information that is lawfully made available to the general
25 public from federal, state, or local government records.

26   (9) "Record" means any material on which written, drawn, spoken,
27 visual, or electromagnetic information is recorded or preserved,
28 regardless of physical form or characteristic.

29   (10) "Redacted" means rendered unreadable, or truncated so that
30 no more than the last four digits of an identification number are
31 accessible as part of the data.

32   NEW SECTION. **Sec. 2.** (1) Annually, on or before January 31st
33 following a year in which a business meets the definition of data
34 broker as provided in section 1 of this act, a data broker shall:

35   (a) Register with the chief privacy officer;

36   (b) Pay a registration fee of two hundred fifty dollars to the
37 chief privacy officer; and

38   (c) Provide the following information to the chief privacy
39 officer:

(i) The name and primary physical, email, and internet addresses
of the data broker;

(ii) If the data broker permits a consumer to opt out of the data
broker's collection of brokered personal information, opt out of its
databases, or opt out of certain sales of data:

(A) The method for requesting an opt-out;

(B) If the opt-out applies to only certain activities or sales, a
statement specifying to which activities or sales the opt-out
applies;

(C) Whether the data broker permits a consumer to authorize a
third party to opt out on the consumer's behalf;

(D) A statement specifying the data collection, databases, or
sales activities from which a consumer may not opt out;

(iii) Whether the data broker implements a purchaser
credentialing process;

(iv) The number of breaches of the security of the system that
the data broker has experienced during the prior year, and if known,
the total number of consumers affected by the breaches;

(v) Where the data broker has actual knowledge that it possess
the brokered personal information of minors, a separate statement
detailing the data collection practices, databases, sales activities,
and opt-out policies that are applicable to the brokered personal
information of minors; and

(vi) Any additional information that the data broker chooses to
provide concerning its data collection practices.

(2) The chief privacy officer is authorized to coordinate with a
third party for the purpose of collecting the registration fee under
subsection (1)(b) of this section.

(3) A data broker that fails to fulfill the requirements of
subsection (1) of this section is subject to:

(a) A civil penalty of fifty dollars for each day, not to exceed
a total of ten thousand dollars for each year, it fails to register
pursuant to this section;

(b) A fine equal to the fees due under this section during the
period it failed to register pursuant to this section; and

(c) Other penalties imposed by law.

(4) The attorney general may maintain an action to collect the
penalties imposed in this section and to seek appropriate injunctive
relief.

1   (5) For purposes of this section, "breach of the security of the
2   system" has the same meaning as in RCW 19.255.010.

3   NEW SECTION. **Sec. 3.**   (1) A data broker shall develop,
4   implement, and maintain a comprehensive information security program
5   that is written in one or more readily accessible parts and contains
6   administrative, technical, and physical safeguards that are
7   appropriate to:
8   (a) The size, scope, and type of business of the data broker;
9   (b) The personally identifiable information the data broker is
10 obligated to safeguard under the comprehensive information security
11 program;
12   (c) The amount of resources available to the data broker;
13   (d) The amount of stored data; and
14   (e) The need for security and confidentiality of personally
15 identifiable information.
16   (2) A data broker shall adopt safeguards in the comprehensive
17 information security program that are consistent with the safeguards
18 for protection of personally identifiable information and information
19 of a similar character set forth in other state rules or federal
20 regulations applicable to the data broker.
21   (3) A comprehensive information security program under this
22 section shall at a minimum have the following features:
23   (a) Designation of one or more employees to maintain the program;
24   (b) Identification and assessment of reasonably foreseeable
25 internal and external risks to the security, confidentiality, and
26 integrity of any electronic, paper, or other records containing
27 personally identifiable information, and a process for evaluating and
28 improving, where necessary, the effectiveness of the current
29 safeguards for limiting such risks, including:
30   (i) Ongoing employee training, including training for temporary
31 and contract employees;
32   (ii) Employee compliance with policies and procedures; and
33   (iii) Means for detecting and preventing security system
34 failures;
35   (c) Security policies for employees relating to the storage,
36 access, and transportation of records containing personally
37 identifiable information outside business premises;
38   (d) Disciplinary measures for violations of the comprehensive
39 information security program rules;

1   (e) Measures that prevent terminated employees from accessing
2 records containing personally identifiable information;
3   (f) Supervision of service providers, by:
4   (i) Taking reasonable steps to select and retain third-party
5 service providers that are capable of maintaining appropriate
6 security measures to protect personally identifiable information
7 consistent with applicable law; and
8   (ii) Requiring third-party service providers by contract to
9 implement and maintain appropriate security measures for personally
10 identifiable information;
11   (g) Reasonable restrictions upon physical access to records
12 containing personally identifiable information and storage of the
13 records and data in locked facilities, storage areas, or containers;
14   (h) Regular monitoring to ensure that the comprehensive
15 information security program is operating in a manner reasonably
16 calculated to prevent unauthorized access to or unauthorized use of
17 personally identifiable information and upgrading information
18 safeguards as necessary to limit risks;
19   (i) Regular review of the scope of the security measures, at
20 least annually and whenever there is a material change in business
21 practices that may reasonably implicate the security or integrity of
22 records containing personally identifiable information;
23   (j) Documentation of responsive actions taken in connection with
24 any incident involving a breach of security; and
25   (k) Mandatory post-incident review of events and actions taken,
26 if any, to make changes in business practices relating to protection
27 of personally identifiable information.
28   (4) A comprehensive information security program under this
29 section must at a minimum, and to the extent technically feasible,
30 have the following computer system security elements:
31   (a) Secure use authentication protocols, as follows:
32   (i) An authentication protocol that has the following features:
33   (A) Control of user IDs and other identifiers;
34   (B) A reasonably secure method of assigning and selecting
35 passwords or use of unique identifier technologies, such as
36 biometrics or token devices;
37   (C) Control of data security passwords to ensure that such
38 passwords are kept in a location and format that do not compromise
39 the security of the data they protect;

                    2SHB 1503

(D) Restricting access to only active users and active user accounts; and

(E) Blocking access to user identification after multiple unsuccessful attempts to gain access; or

(ii) An authentication protocol that provides a higher level of security than the features specified in (a)(i) of this subsection;

(b) Secure access control measures that:

(i) Restrict access to records and files containing personally identifiable information to those who need such information to perform their job duties; and

(ii) Assign to each person with computer access unique identifications plus passwords, which are not vendor-supplied default passwords, that are reasonably designed to maintain the integrity of the security of the access controls or a protocol that provides a higher degree of security;

(c) Encryption of all transmitted records and files containing personally identifiable information that will travel across public networks and encryption of all data containing personally identifiable information to be transmitted wirelessly or a protocol that provides a higher degree of security;

(d) Reasonable monitoring of systems for unauthorized use of or access to personally identifiable information;

(e) Encryption of all personally identifiable information stored on laptops or other portable devices or a protocol that provides a higher degree of security;

(f) For files containing personally identifiable information on a system that is connected to the internet, reasonably up-to-date firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personally identifiable information or a protocol that provides a higher degree of security;

(g) Reasonably up-to-date versions of system security agent software that must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions and is set to receive the most current security updates on a regular basis or a protocol that provides a higher degree of security; and

1 (h) Education and training of employees on the proper use of the
2 computer security system and the importance of personally
3 identifiable information security.

4 NEW SECTION. **Sec. 4.** (1) A person shall not acquire brokered
5 personal information through fraudulent means.
6 (2) A person shall not acquire or use brokered personal
7 information for the purpose of:
8 (a) Stalking or harassing another person;
9 (b) Committing a fraud, including identity theft, financial
10 fraud, or email fraud; or
11 (c) Engaging in unlawful discrimination, including employment
12 discrimination and housing discrimination.

13 NEW SECTION. **Sec. 5.** (1) A violation of this chapter is not
14 reasonable in relation to the development and preservation of
15 business and is an unfair or deceptive act in trade or commerce and
16 an unfair method of competition for the purpose of applying the
17 consumer protection act, chapter 19.86 RCW.
18 (2) This chapter may be enforced solely by the attorney general
19 under the consumer protection act, chapter 19.86 RCW.

20 NEW SECTION. **Sec. 6.** (1) On or before July 1, 2020, the
21 attorney general and the chief privacy officer shall submit a
22 preliminary report concerning the implementation of this act to the
23 economic development committees of the legislature.
24 (2) On or before January 1, 2021, the attorney general and the
25 chief privacy officer shall update their preliminary report and
26 provide additional information concerning the implementation of this
27 act to the economic development committees of the legislature.
28 (3) On or before January 1, 2020, the attorney general shall:
29 (a) Review and consider the necessity of additional legislative
30 and regulatory approaches to protecting the data security and privacy
31 of Washington consumers, including:
32 (i) Whether to expand the duties and the resources necessary to
33 support the chief privacy officer; and
34 (ii) Whether to expand or reduce the scope of regulation to
35 businesses with direct relationships to consumers; and
36 (b) Report its findings and recommendations to the economic
37 development committees of the legislature.

1   This section expires January 1, 2022.

2   NEW SECTION. **Sec. 7.** Sections 1 through 6 and 8 of this act
3 constitute a new chapter in Title 19 RCW.

4   NEW SECTION. **Sec. 8.** Sections 1 through 5 of this act take
5 effect January 1, 2020.

6   NEW SECTION. **Sec. 9.** If specific funding for the purposes of
7 this act, referencing this act by bill or chapter number, is not
8 provided by June 30, 2019, in the omnibus appropriations act, this
9 act is null and void.

--- END ---