H-0526.5

HOUSE BILL 1503

State of Washington 66th Legislature 2019 Regular Session

By Representatives Smith, Hudgins, and Stanford

Read first time 01/23/19. Referred to Committee on Innovation, Technology & Economic Development.

AN ACT Relating to registration and consumer protection obligations of data brokers; adding a new chapter to Title 19 RCW; prescribing penalties; providing an effective date; 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)(a) "Brokered personal information" means one or more of the following computerized data elements about a consumer, if categorized or organized for dissemination to third parties:

(i) Name;

(ii) Address;

(iii) Date of birth;

(iv) Place of birth;

(v) Mother's maiden name;

(vi) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical 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) "Consumer" means an individual residing in this state.

(4)(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) Providing publicly available information via real-time or near real-time alert services for health or safety purposes, 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.

(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

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

(5)(a) "Data broker security breach" means an unauthorized acquisition or a reasonable belief of an unauthorized acquisition of more than one element of brokered personal information maintained by a data broker when the brokered personal information is not

encrypted, redacted, or protected by another method that renders the information unreadable or unusable by an unauthorized person.

(b) "Data broker security breach" does not include good faith but unauthorized acquisition of brokered personal information by an employee or agent of the data broker for a legitimate purpose of the data broker, provided that the brokered personal information is not used for a purpose unrelated to the data broker's business or subject to further unauthorized disclosure.

(c) In determining whether brokered personal information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data broker may consider the following factors, among others:

(i) Indications that the brokered personal information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing brokered personal information;

(ii) Indications that the brokered personal information has been downloaded or copied;

(iii) Indications that the brokered personal information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

(iv) Indications that the brokered personal information has been made public.

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

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

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

(i) Social security number;

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

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

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

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

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

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

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

(a) Register with the chief privacy officer;

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

(c) Provide the following information to the chief privacy 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 data broker security breaches 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) 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.

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

NEW SECTION. **Sec. 3.** (1) A data broker shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

(a) The size, scope, and type of business of the data broker;

(b) The personally identifiable information the data broker is obligated to safeguard under the comprehensive information security program;

(c) The amount of resources available to the data broker;

(d) The amount of stored data; and

(e) The need for security and confidentiality of personally identifiable information.

(2) A data broker shall adopt safeguards in the comprehensive information security program that are consistent with the safeguards for protection of personally identifiable information and information of a similar character set forth in other state rules or federal regulations applicable to the data broker.

(3) A comprehensive information security program under this section shall at a minimum have the following features:

(a) Designation of one or more employees to maintain the program;

(b) Identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other records containing personally identifiable information, and a process for evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including:

(i) Ongoing employee training, including training for temporary and contract employees;

(ii) Employee compliance with policies and procedures; and

(iii) Means for detecting and preventing security system failures;

(c) Security policies for employees relating to the storage, access, and transportation of records containing personally identifiable information outside business premises;

(d) Disciplinary measures for violations of the comprehensive information security program rules;

(e) Measures that prevent terminated employees from accessing records containing personally identifiable information;

(f) Supervision of service providers, by:

(i) Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personally identifiable information consistent with applicable law; and

(ii) Requiring third-party service providers by contract to implement and maintain appropriate security measures for personally identifiable information;

(g) Reasonable restrictions upon physical access to records containing personally identifiable information and storage of the records and data in locked facilities, storage areas, or containers;

(h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personally identifiable information and upgrading information safeguards as necessary to limit risks;

(i) Regular review of the scope of the security measures, at least annually and whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personally identifiable information;

(j) Documentation of responsive actions taken in connection with any incident involving a breach of security; and

(k) Mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personally identifiable information.

(4) A comprehensive information security program under this section must at a minimum, and to the extent technically feasible, have the following computer system security elements:

(a) Secure use authentication protocols, as follows:

(i) An authentication protocol that has the following features:

(A) Control of user IDs and other identifiers;

(B) A reasonably secure method of assigning and selecting passwords or use of unique identifier technologies, such as biometrics or token devices;

(C) Control of data security passwords to ensure that such passwords are kept in a location and format that do not compromise the security of the data they protect;

(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

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

NEW SECTION. **Sec. 4.** (1) A person shall not acquire brokered personal information through fraudulent means.

(2) A person shall not acquire or use brokered personal information for the purpose of:

(a) Stalking or harassing another person;

(b) Committing a fraud, including identity theft, financial fraud, or email fraud; or

(c) Engaging in unlawful discrimination, including employment discrimination and housing discrimination.

NEW SECTION. **Sec. 5.** (1) A violation of this chapter 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 the purpose of applying the consumer protection act, chapter 19.86 RCW.

(2) This chapter may be enforced solely by the attorney general under the consumer protection act, chapter 19.86 RCW.

NEW SECTION. **Sec. 6.** (1) On or before July 1, 2020, the attorney general and the chief privacy officer shall submit a preliminary report concerning the implementation of this act to the economic development committees of the legislature.

(2) On or before January 1, 2021, the attorney general and the chief privacy officer shall update their preliminary report and provide additional information concerning the implementation of this act to the economic development committees of the legislature.

(3) On or before January 1, 2020, the attorney general shall:

(a) Review and consider the necessity of additional legislative and regulatory approaches to protecting the data security and privacy of Washington consumers, including:

(i) Whether to expand the duties and the resources necessary to support the chief privacy officer; and

(ii) Whether to expand or reduce the scope of regulation to businesses with direct relationships to consumers; and

(b) Report its findings and recommendations to the economic development committees of the legislature.

This section expires January 1, 2022.

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

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

--- END ---