HOUSE BILL NO. 638

AMENDMENT IN THE NATURE OF A SUBSTITUTE

(Proposed by the House Committee on Communications, Technology and Innovation on _____)

(Patron Prior to Substitute—Delegate Maldonado)

A BILL to amend the Code of Virginia by adding in Title 59.1 a chapter numbered 60, consisting of sections numbered 59.1-614 through 59.1-619, relating to regulation of data brokers; civil penalties.

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding in Title 59.1 a chapter numbered 60, consisting of sections numbered 59.1-614 through 59.1-619, as follows:

CHAPTER 60.

DATA BROKER REGULATION.

§ 59.1-614. Definitions.

As used in this chapter, unless the context requires a different meaning:

"Artificial intelligence system" means any machine learning-based system that, for any explicit or implicit objective, infers from the inputs such system receives how to generate outputs, including content, decisions, predictions, and recommendations, that can influence physical or virtual environments. "Artificial intelligence system" does not include any artificial intelligence system or general purpose artificial intelligence model that is used for development, prototyping, and research activities before such artificial intelligence system or general purpose artificial intelligence model is made available to deployers or consumers.

"Biometric data" means the same as that term is defined in § 59.1-575.

"Business" means a corporation, partnership, sole proprietorship, firm, enterprise, franchise, association, trust or foundation, or any other individual or entity carrying on a business or profession, whether or not for profit. "Business" does not include a state or local agency.

"Consumer" means the same as that term is defined in § 59.1-575.

"Data broker" means a business that knowingly collects and conducts the sale of personally identifiable information of consumers with whom the business does not have a direct relationship to third parties and whose principal source of revenue is the sale of such data. The following activities conducted by a business, and the collection and sale or licensing of personally identifiable information incidental to conducting these activities, do not qualify the business as a "data broker":

1. 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;

2. Providing lawfully obtainable information related to a consumer's business or profession; or

3. Providing lawfully obtainable information through real-time or near-real-time alert services for health or safety purposes.

"Data broker security breach" means an unauthorized acquisition or a reasonable belief of an unauthorized acquisition of more than one element of personally identifiable information maintained by a data broker when the personally identifiable information is not de-identified, redacted, or protected by another method that renders the information unreadable or unusable by an unauthorized person. "Data broker security breach" does not include good faith but unauthorized acquisition of personally identifiable information by an employee or agent of the data broker for a legitimate purpose of the data broker, provided that the personally identifiable information is not used for a purpose unrelated to the data broker's business or subject to further unauthorized disclosure. In determining whether personally identifiable information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data broker may consider:

1. Indications that the personally identifiable 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 personally identifiable information;

2. Indications that the personally identifiable information has been downloaded or copied;

3. Indications that the personally identifiable information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

4. That the personally identifiable information has been made public.

"Data collector" means a person who, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with personally identifiable information, and includes public and private entities.

"De-identified data" means the same as that term is defined in § 59.1-575.

"Direct relationship" means that a consumer has intentionally interacted with a business for the purpose of accessing, purchasing, using, requesting, or obtaining information about the business's products or services. A consumer does not have a "direct relationship" with a business if the purpose of their engagement is to exercise any right described under § 59.1-577, or for the business to verify the consumer's identity. A business does not have a "direct relationship" with a consumer because it collects personally identifiable information directly from the consumer; the consumer must intend to interact with the business. A business is

still a data broker and does not have a direct relationship with a consumer as to the sale of personally identifiable information that such business collected outside of a first party interaction with the consumer.

"Identified or identifiable natural person" means the same as that term is defined in § 59.1-575.

"Lawfully obtainable information" means information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

"Personally identifiable information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, whether directly or indirectly, with a particular consumer. "Personally identifiable information" includes the following:

1. Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or similar identifier;

2. Characteristics of protected classifications under state or federal law;

3. Commercial information, including records of personal property, product or service purchases, whether obtained or considered, or other purchasing or consuming histories or tendencies;

4. Biometric data;

5. Internet or other electronic network activity information, including browsing history, search history, and information regarding a consumer's interaction with an internet website application or advertisement;

6. Precise geolocation data;

7. Audio, electronic, visual, thermal, olfactory, or similar information;

8. Information related to profession or employment;

9. Education information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g);

10. Inferences drawn from any of the information identified in this definition to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes; and

11. Sensitive data.

"Personally identifiable information" does not include lawfully obtainable information or personally identifiable information that has been de-identified.

"Precise geolocation data" means that same as that term is defined in § 59.1-575.

"Sale of personally identifiable information" means the exchange of personally identifiable information for monetary or other valuable consideration by a data broker to a third party. "Sale of personally identifiable information" does not include a one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business or a sale of personally identifiable information that is merely incidental to the business.

"Sensitive data" means the same as that term is defined in § 59.1-575.

§ 59.1-615. Acquisition of personally identifiable information; prohibition.

A. No person shall acquire personally identifiable information through fraudulent means.

B. No person shall acquire or use personally identifiable information for the purpose of:

1. Stalking of harassing another person;

2. Committing a fraud, including identity theft, financial fraud, or email fraud; or

3. Engaging in unlawful discrimination, including employment discrimination or housing discrimination.

§ 59.1-616. Data brokers; comprehensive information security program.

A. 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 according to:

1. The size, scope, and type of business of the data broker;

2. The amount of resources available to the data broker;

3. The amount of stored data; and

4. The need for security and confidentiality of personally identifiable information.

A data broker shall adopt safeguards in the comprehensive 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 or federal laws or regulations applicable to the data broker, including the Consumer Data Protection Act (§ 59.1-575 et seq.).

B. A comprehensive information security program required pursuant to subsection A shall include the following features:

1. Designation of one or more employees to maintain the program;

2. 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;

3. 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 of detecting and preventing security system failures;

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

5. Disciplinary measures for violations of the comprehensive information security program rules;

6. Measures that prevent terminated employees from accessing records containing personally identifiable information;

7. Supervision of third-party service providers by taking reasonable steps to select and retain such providers that are capable of maintaining appropriate security measures to protect personally identifiable information consistent with applicable law and by requiring such providers by contract to implement and maintain appropriate security measures for personally identifiable information;

8. 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;

9. 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;

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

11. Documentation of responsive actions taken in connection with any incident involving a breach of security and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personally identifiable information.

C. A comprehensive information security program required pursuant to subsection A shall, to the extent technically feasible, include the following technical elements:

1. A secure user authentication protocol that has (i) the control of user identifications and other identifiers; (ii) a reasonably secure method of assigning and selecting passwords or use of unique identifier technologies, such as biometrics or token devices; (iii) 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; (iv) the ability to restrict access to only active users and active user accounts; and (v) the ability to block access

to user identification after multiple unsuccessful attempts to gain access;

2. Secure access control measures that restrict access to records and files containing personally identifiable information to those who need such information to perform their job duties and assign to each person with computer access unique identifications plus passwords that are not vendor-supplied default passwords and that are reasonably designed to maintain the integrity of the security of the access controls;

3. A mechanism that ensures that all transmitted records and files containing personally identifiable information that will travel across public networks and all data containing personally identifiable information to be transmitted wirelessly shall be transformed to de-identified data prior to such travel or transmission;

4. Reasonable monitoring of systems for unauthorized use of or access to personally identifiable information;

5. A mechanism that ensures that all personally identifiable information stored on laptops or other portable devices is de-identified prior to such storage;

6. 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;

7. Reasonably up-to-date versions of system security agent software that shall 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 that most current security updates on a regular basis; and

8. Education and training of employees in the proper use of the computer security system and the importance of personally identifiable information security.

Nothing in this subsection shall prohibit a comprehensive information security program from providing a higher degree of security than the protocols described in this subsection.

§ 59.1-617. Data brokers; registration.

Beginning on December 1, 2027, and annually thereafter, a data broker operating in the Commonwealth shall register with the Secretary of the Commonwealth by paying a registration fee of $1,000 and providing the following information:

1. The name and primary physical, email, and internet addresses of the data broker;

2. If the data broker permits a consumer to opt out of the data broker's collection of personally identifiable information, opt out of its databases, or opt out of certain sales of data, (i) the method for

requesting an opt-out; (ii) which activities or sales the opt-out applies to, if the opt-out applies only to certain activities or sales; and (iii) whether the data broker permits a consumer to authorize a third party to perform the opt-out on the consumer's behalf;

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

4. A statement stating whether the data broker implements a purchaser credentialing process;

5. The number of data broker security breaches that the data broker experienced during the prior year, and, if known, the total number of consumers affected by such breaches;

6. Where the data broker has actual knowledge that it possesses the personally identifiable information of minors, a separate statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the personally identifiable information of minors;

7. Whether the data broker collects:

a. Precise geolocation data;

b. Reproductive health care data;

c. Biometric data;

d. Data related to immigration status;

e. Data related to sexual orientation;

f. Data related to union membership;

g. Data related to name, date of birth, zip code, email address, or phone number;

h. Account login data in combination with any required security code, access code, or password that would permit access to a consumer's account by a third party;

i. Data related to driver's license number, state identification card number, tax identification number, social security number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of an individual; or

j. Data related to mobile advertising identification number, connected television identification number, or vehicle identification number;

8. Whether the data broker has shared or sold consumer data in the past year with or to:

a. A foreign business or government;

b. The federal government;

c. A state government;

d. Any law enforcement agency, unless such data was shared pursuant to a subpoena or court order; or

e. A developer of an artificial intelligence system;

9. Between one and three of the most common categories of personally identifiable information that the data broker collects; and

10. Any additional information or explanation the data broker chooses to provide concerning its data collection practices.

The Secretary of the Commonwealth shall post on its website the registration information provided by data brokers as described in this section.

§ 59.1-618. Exemptions; conflicts.

A. This chapter shall not apply to data subject to the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.) or Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.).

B. This chapter is intended to supplement, not supplant, the laws of the Commonwealth relating to data privacy, including the Consumer Data Protection Act (§ 59.1-575 et seq.), which laws shall continue to apply to persons described in this chapter, unless the context clearly indicates otherwise. To the extent that any provisions of this chapter conflict with such other laws of the Commonwealth, the provisions of this chapter shall prevail. Where this chapter is silent, such other laws shall apply.

§ 59.1-619. Enforcement; civil penalties.

A. The Attorney General shall have exclusive authority to enforce the provisions of this chapter.

B. Prior to initiating any action under this chapter, the Attorney General shall provide a data broker or other person 30 days' written notice identifying the specific provisions of this chapter the Attorney General alleges have been or are being violated. If within the 30-day period such data broker or person cures the noticed violation and provides the Attorney General an express written statement that the alleged violations have been cured and that no further violations shall occur, no action shall be initiated against such data broker or person.

C. If a data broker or other person continues to violate this chapter following the cure period in subsection B or breaches an express written statement provided to the Attorney General under that subsection, the Attorney General may initiate an action in the name of the Commonwealth and may seek an injunction to restrain any violations of this chapter and civil penalties of up to $7,500 for each violation under this chapter. All civil penalties, expenses, and attorney fees collected pursuant to this chapter shall be paid into the state treasury and credited to the Regulatory, Consumer Advocacy, Litigation, and Enforcement Revolving Trust Fund.

D. The Attorney General may recover reasonable expenses incurred in investigating and preparing the

case, including attorney fees, in any action initiated under this chapter.

E. Nothing in this chapter shall be construed as providing the basis for, or be subject to, a private right of action for violations of this chapter or under any other law.

2. That the provisions of this act shall become effective on July 1, 2027.