SB213

RRIDNMM-1

By Senators Orr, Allen

RFD: Fiscal Responsibility and Economic Development

First Read: 06-Mar-24

SYNOPSIS:

Existing law provides for the confidentiality of certain personal information in certain contexts.

This bill would provide that brokers of individual consumers' data must notify consumers of certain information on their website.

This bill would provide that data brokers must register with the Secretary of State.

This bill would provide that data brokers must protect consumers' data through specified security measures.

This bill would require the Secretary of State to adopt rules and procedures to implement and administer the requirements of this bill.

This bill would provide civil penalties for data brokers that violate these notification or registration requirements.

This bill would provide that violations of the duty to protect consumers' data through specified security measures by data brokers constitute violations of the Deceptive Trade Practices Act.

This bill would provide certain persons and information to which the requirements of this bill do not apply.

Section 111.05 of the Constitution of Alabama of

2022, prohibits a general law whose purpose or effect would be to require a new or increased expenditure of local funds from becoming effective with regard to a local governmental entity without enactment by a 2/3 vote unless: it comes within one of a number of specified exceptions; it is approved by the affected entity; or the Legislature appropriates funds, or provides a local source of revenue, to the entity for the purpose.

The purpose or effect of this bill would be to require a new or increased expenditure of local funds within the meaning of the section. However, the bill does not require approval of a local governmental entity or enactment by a 2/3 vote to become effective because it comes within one of the specified exceptions contained in the section.

A BILL

TO BE ENTITLED

AN ACT

Relating to data privacy; to require consumer data brokers to publicly state certain information; to require data brokers to register with the Secretary of State; to require that data brokers protect data using specified security measures; to provide civil and criminal penalties for violations; to provide persons and information to which these requirements do not apply; and in connection therewith would have as its purpose or effect the requirement of a new or increased expenditure of local funds within the meaning of Section 111.05 of the Constitution of Alabama of 2022.

BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

Section 1. For the purposes of this act, the following terms have the following meanings:

(1) BIOMETRIC DATA. Data generated by automatic measurements of an individual's biological patterns or characteristics, including fingerprint, voiceprint, retina or iris scan, information pertaining to an individual's DNA, or another unique biological pattern or characteristic that is used to identify a specific individual.

(2) CHILD. An individual younger than 13 years of age.

(3) COLLECT. In the context of data, means to obtain, receive, access, or otherwise acquire data by any means, including by purchasing or renting the data.

(4) DATA BROKER. A business entity whose principal source of revenue is derived from the collecting, processing, or transferring of personal data that the entity did not collect directly from the individual linked or linkable to the data.

(5) DE-IDENTIFIED DATA. Data that cannot reasonably be linked to an identified or identifiable individual or to a device linked to that individual.

(6) EMPLOYEE. An individual who is a director, officer, staff member, trainee, volunteer, or intern of an employer or an individual working as an independent contractor for an

employer, regardless of whether the individual is paid, unpaid, or employed on a temporary basis. The term does not include an individual contractor who is a service provider.

(7) EMPLOYEE DATA. Information collected, processed, or transferred by an employer if the information satisfies both of the following:

a. Is related to any of the following:

1. A job applicant and was collected during the course of the hiring and application process.

2. An employee who is acting in a professional capacity for the employer, including the employee's business contact information such as the employee's name, position, title, business telephone number, business address, or business e-mail address.

3. An employee's emergency contact information.

4. An employee or the employee's spouse, dependent, covered family member, or beneficiary.

b. Was collected, processed, or transferred solely for any of the following:

1. A purpose relating to the status of an individual described by subparagraph a.1. as a current or former job applicant of the employer.

2. A purpose relating to the professional activities of an employee described by subparagraph a.2. on behalf of the employer.

3. The purpose of having an emergency contact on file for an employee described by subparagraph a.3. and for transferring the information in case of an emergency.

4. The purpose of administering benefits to which an employee described by subparagraph a.4. is entitled or to which another individual described by that paragraph is entitled on the basis of the employee's position with the employer.

(8) GENETIC DATA. Any data, regardless of format, concerning an individual's genetic characteristics. The term includes raw sequence data derived from sequencing all or a portion of an individual's extracted DNA and genotypic and phenotypic information obtained from analyzing an individual's raw sequence data.

(9) KNOWN CHILD. A child under circumstances where a data broker has actual knowledge of, or willfully disregards obtaining actual knowledge of, the child's age.

(10) PERSONAL DATA. Any information, including sensitive data, that is linked or reasonably linkable to a identified or identifiable individual. The term includes pseudonymous data when the information is used by a controller or processor in conjunction with additional information that reasonably links the information to an identified or identifiable individual. The term does not include de-identified data, employee data, or publicly available information.

(11) PRECISE GEOLOCATION DATA. Information accessed on a device or technology that shows the past or present physical location of an individual or the individual's device with sufficient precision to identify street-level location information of the individual or device in a range of

not more than 1,850 feet. The term does not include location information regarding an individual or device identifiable or derived solely from the visual content of a legally obtained image, including the location of a device that captured the image.

(12) PROCESS. In the context of data, an operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(13) PUBLICLY AVAILABLE INFORMATION. Information to which any of the following apply:

a. Is lawfully made available through governmental records.

b. A business has a reasonable basis to believe is lawfully available to the general public through widely distributed media.

c. Is lawfully made available by a consumer, or by an individual to whom a consumer has disclosed the information, unless the consumer has restricted access to the information to a specific audience.

(14) SENSITIVE DATA.

a. A government-issued identifier not required by law to be publicly available, including any of the following:

1. A Social Security number.

2. A passport number.

3. A driver license number.

b. Information that describes or reveals an individual's mental or physical health diagnosis, condition, or treatment.

c. An individual's financial information, except the last four digits of a debit or credit card number, including any of the following:

1. A financial account number.

2. A credit or debit card number.

3. Information that describes or reveals the income level or bank account balances of the individual.

d. Biometric data.

e. Genetic data.

f. Precise geolocation data.

g. An individual's private communication, and that if made using a device, is not made using a device provided by the individual's employer that provides conspicuous notice to the individual that the employer may access communication made using the device. These communications include, unless the data broker is the sender or an intended recipient of the communication, all of the following:

1. The individual's voicemails, e-mails, texts, direct messages, or mail.

2. Information that identifies the parties involved in the communications.

3. Information that relates to the transmission of the communications, including telephone numbers called, telephone numbers from which calls were placed, the time calls were made, call duration, and location information of the parties to the call.

h. A log-in credential, security code, or access code for an account or device.

i. Information identifying the sexual behavior of the individual in a manner inconsistent with the individual's reasonable expectation regarding the collection, processing, or transfer of the information.

j. Calendar information, address book information, phone or text logs, photos, audio recordings, or videos that are both:

1. Maintained for private use by an individual and stored on the individual's device or in another location.

2. Not communicated using a device provided by the individual's employer unless the employee was provided conspicuous notice that the employer may access communication made using the device.

k. A photograph, film, video recording, or other similar medium that shows the individual or a part of the individual nude or wearing undergarments.

l. Information revealing the video content requested or selected by an individual that is neither of the following:

1. Collected by a provider of broadcast television service, cable service, satellite service, streaming media service, or other video programming, as that term is defined by 47 U.S.C. § 613.

2. Used solely for transfers for independent video measurement.

m. Information regarding a known child.

n. Information revealing an individual's racial or ethnic origin, color, religious beliefs, or union membership.

o. Information identifying an individual's online activities over time accessing multiple Internet websites or online services.

p. Information collected, processed, or transferred for the purpose of identifying information described by this subdivision.

(15) SERVICE PROVIDER. A person that receives, collects, processes, or transfers personal data on behalf of, and at the direction of, a business or governmental entity, including a business or governmental entity that is another service provider, in order for the person to perform a service or function with or on behalf of the business or governmental entity.

(16) TRANSFER. In the context of data, to disclose, release, share, disseminate, make available, sell, or license the data by any means or medium.

Section 2. (a) Except as provided by subsection (b), this act applies to personal data from an individual that is collected, transferred, or processed by a data broker.

(b) This chapter does not apply to any of the following data:

(1) De-identified data, if the data broker does all of the following:

a. Takes reasonable technical measures to ensure that the data is not able to be used to identify an individual with whom the data is associated.

b. Publicly commits to both of the following in a clear and conspicuous manner:

1. To process and transfer the data solely in a de-identified form without any reasonable means for reidentification.

2. To not attempt to identify the information to an individual with whom the data is associated.

c. Contractually obligates a person that receives the information from the provider to both of the following:

1. Comply with this subsection with respect to the information.

2. Include those contractual obligations in any subsequent transfer of the data to another person.

(2) Employee data.

(3) Publicly available information.

(4) Inferences made exclusively from multiple independent sources of publicly available information that does not reveal sensitive data with respect to an individual.

(5) Data subject to Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, et seq.

Section 3. (a) Except as provided by subsection (b), this act applies only to a data broker that derives either of the following within a 12-month period:

(1) More than 50 percent of the data broker's revenue from processing or transferring personal data that the data broker did not collect directly from the individuals to whom the data pertains.

(2) Revenue from processing or transferring the personal data of more than 50,000 individuals that the data

broker did not collect directly from the individuals to whom the data pertains.

(b) This chapter does not apply to any of the following:

(1) A service provider, including a service provider that engages in the business of processing employee data for a third-party employer for the sole purpose of providing benefits to the third-party employer's employees.

(2) A person that collects personal data from another person to which the person is related by common ownership or corporate control, provided a reasonable consumer would expect the persons to share data.

(3) A federal, state, tribal, territorial, or local governmental entity, including a body, authority, board, bureau, commission, district, agency, or political subdivision of a governmental entity.

(4) An entity that serves as a congressionally designated nonprofit, national resource center, or clearinghouse to provide assistance to victims, families, child-serving professionals, and the general public on missing and exploited children issues.

(5) A consumer reporting agency or other entity that furnishes information for inclusion in a consumer credit report or obtains a consumer credit report, but only to the extent the entity engages in activity regulated or authorized by the Fair Credit Reporting Act, 15 U.S.C. § 1681, et seq., including the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a

consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living.

(6) A financial institution subject to Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, et seq.

Section 4. A data broker that maintains an Internet website or mobile application shall post a conspicuous notice on the website or application that complies with all of the following:

(1) States that the entity maintaining the website or application is a data broker.

(2) Is clear, not misleading, and readily accessible by the general public, including individuals with a disability.

(3) Contains language provided by rule of the Secretary of State for inclusion in the notice.

Section 5. (a) To conduct business in this state, a data broker that is subject to this act shall register by January 1, 2025, with the Secretary of State by filing a registration certificate and paying a registration fee of three hundred dollars ($300).

(b) The registration certificate must include all of the following:

(1) The legal name of the data broker.

(2) A contact individual and the primary physical address, e-mail address, telephone number, and Internet website address for the data broker.

(3) A description of the categories of data the data

broker processes and transfers.

(4) A statement of whether or not the data broker implements a purchaser credentialing process.

(5) If the data broker has actual knowledge that the data broker possesses personal data of a known child, both of the following:

a. A statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the personal data of a known child.

b. A statement as to how the data broker complies with applicable federal and state law regarding the collection, use, or disclosure of personal data from and about a child on the Internet.

(6) The number of security breaches the data broker has experienced during the year immediately preceding the year in which the registration is filed and, if known, the total number of consumers affected by each breach.

(c) The registration certificate may include any additional information or explanation the data broker chooses to provide to the Secretary of State concerning the data broker's data collection practices.

(d) A registration certificate expires on the first anniversary of its date of issuance and every year thereafter. A data broker may renew a registration certificate by filing a renewal application, in the form prescribed by the Secretary of State, and paying a renewal fee of three hundred dollars ($300).

Section 6. (a) The Secretary of State shall establish and maintain, on its Internet website, a searchable, central registry of data brokers registered pursuant to Section 5.

(b) The registry must include both of the following:

(1) A search feature that allows an individual searching the registry to identify a specific data broker.

(2) For each data broker, the information filed under Section 5(b).

Section 7. (a) A data broker conducting business in this state has a duty to protect personal data held by the data broker in accordance with this section.

(b) A data broker shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and employs administrative, technical, and physical safeguards that are appropriate for:

(1) The data broker's size, scope, and type of business;

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

(3) The amount of data stored by the data broker; and

(4) The need for security and confidentiality of the personal data stored by the data broker.

(c) The comprehensive information security program required by this section must:

(1) Incorporate safeguards that are consistent with the safeguards for protection of personal data and information of a similar character under state or federal laws and rules applicable to the data broker;

(2) Include the designation of one or more employees of the data broker to maintain the program;

(3) Require the identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other record containing personal data, and the establishment of a process for evaluating and improving, as necessary, the effectiveness of the current safeguards for limiting those risks, including:

a. Requiring ongoing employee and contractor education and training, including education and training for temporary employees and contractors of the data broker, on the proper use of security procedures and protocols and the importance of personal data security;

b. Mandating employee compliance with policies and procedures established under the program; and

c. Providing a means for detecting and preventing security system failures;

(4) Include security policies for the data broker's employees relating to the storage, access, and transportation of records containing personal data outside of the broker's physical business premises;

(5) Provide disciplinary measures for violations of a policy or procedure established under the program;

(6) Include measures for preventing a terminated employee from accessing records containing personal data;

(7) Provide policies for the supervision of third-party service providers that include:

a. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal data consistent with applicable law; and

b. Requiring third-party service providers, by contract, to implement and maintain appropriate security measures for personal data;

(8) Provide reasonable restrictions on physical access to records containing personal data, including requiring the records containing the data to be stored in a locked facility, storage area, or container;

(9) Include regular monitoring to ensure that the program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal data and, as necessary, upgrading information safeguards to limit the risk of unauthorized access to or unauthorized use of personal data;

(10)a. Require the regular review of the scope of the program's security measures;

b. A review of the scope of the program's security measures must occur at least annually and anytime there is a material change in the data broker's business practices that may reasonably affect the security or integrity of records containing personal data;

(11) Require the documentation of responsive actions taken in connection with any incident involving a breach of security, including a mandatory post-incident review of each event and the actions taken, if any, to make changes in

business practices relating to the protection of personal data in response to that event; and

(12) To the extent feasible, include the following procedures and protocols with respect to computer system security requirements or procedures and protocols providing a higher degree of security, for the protection of personal data:

a. Using secure user authentication protocols that include:

1. Controlling user log-in credentials and other identifiers;

2. Using a reasonably secure method of assigning and selecting passwords or using unique identifier technologies, which may include biometrics or token devices;

3. Controlling data security passwords to ensure that the passwords are kept in a location and format that do not compromise the security of the data the passwords protect;

4. Restricting access to only active users and active user accounts; and

5. Blocking access to user credentials or identification after multiple unsuccessful attempts to gain access;

b. Using secure access control measures that include:

1. Restricting access to records containing personal data to only employees or contractors who need access to the personal data to perform their job duties; and

2. Assigning to each employee or contractor with access to a computer containing personal data a unique identification

and password, which may not be a vendor-supplied default password, or using another protocol reasonably designed to maintain the integrity of the security of the access controls to personal data;

c. Encryption of:

1. Transmitted records containing personal data that will travel across public networks; and

2. Data containing personal data that is transmitted wirelessly;

d. Reasonable monitoring of systems for unauthorized use of or access to personal data;

e. Encryption of all personal data stored on laptop computers or other portable devices;

f. For records containing personal data on a system that is connected to the Internet, using reasonably current firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personal data; and

g. Using:

1. A reasonably current version of system security agent software that must include malware protection and reasonably current patches and virus definitions; or

2. A version of system security agent software that is supportable with current patches and virus definitions and is set to receive the most current security updates on a regular basis.

(d) A violation of this section by a data broker constitutes a violation of the Deceptive Trade Practices Act, Chapter 19 of Title 8, Code of Alabama 1975, and shall be subject to the same penalties as provided therein.

Section 8. (a) A data broker that violates Section 4 or 5 shall be assessed the following civil penalties by the Secretary of State:

(1) One hundred dollars ($100) for each day the entity is in violation.

(2) The amount of unpaid registration fees for each year the entity fails to register as required by Section 5.

(b) A civil penalty assessed pursuant to this section may not exceed ten thousand dollars ($10,000) against a single data broker during a 12-month period.

(c) The Attorney General may bring an action to recover any civil penalty assessed under this section and may recover reasonable attorney fees and court costs incurred in bringing the action.

(d)(1) All penalties collected pursuant to this act shall be deposited into the Consumer Privacy Protection Fund which is created in the State Treasury. The fund shall be administered by the Secretary of State for the purpose of implementing and administering this act.

(2) No money shall be withdrawn or expended from this fund for any purpose unless the monies have been appropriated by the Legislature and allocated pursuant to this act. Any monies appropriated shall be budgeted and allocated pursuant to the Budget Management Act in accordance with Article 4, commencing with Section 41-4-80 of Chapter 4 of Title 41, Code of Alabama 1975, and only in the amounts provided by the

Legislature in the general appropriations act or other appropriations act.

Section 9. The Secretary of State shall adopt rules as necessary to implement this act.

Section 10. This act does not apply to the collection, processing, or transfer of personal data by a data broker before January 1, 2025.

Section 11. Although this bill would have as its purpose or effect the requirement of a new or increased expenditure of local funds, the bill is excluded from further requirements and application under Section 111.05 of the Constitution of Alabama of 2022, because the bill defines a new crime or amends the definition of an existing crime.

Section 12. This act shall become effective on October 1, 2024.