BILL ANALYSIS

Senate Research Center
88R25295 JES-F

C.S.S.B. 2105
By: Johnson
Business & Commerce
4/25/2023
Committee Report (Substituted)

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

Data brokers are key players in collecting and selling personal data to third parties. These third parties can be companies looking to advertise their businesses or any person interested in information about someone and willing to pay for it. Data brokers take advantage of the lack of adequate data privacy safeguards enshrined in both federal and state law, which puts vulnerable populations, such as survivors of domestic violence, victims of human trafficking, youths, and older adults, at risk for fraud and abuse.

S.B. 2105 creates a comprehensive framework in the Texas Business and Commerce Code to regulate data brokers and empower Texans to control the collection and sale of their personal information to these entities.

First, S.B. 2105 would require data brokers in the state of Texas to register annually with the secretary of state.

Second, in their application to register, data brokers would have to provide a notice on all online platforms used to operate their business, containing who they are, the type of data they collect and other categories designated by the secretary of state.

Third, the secretary of state will set up and maintain a "do not collect" registry that allows individuals to have their data deleted, which would then require data brokers to cease collecting, processing, and transferring that data.

Lastly, the bill also creates civil penalties for data brokers that fail to comply with the law.

(Original Author's/Sponsor's Statement of Intent)

Key Provisions:

Adds Chapter 509 to the Business and Commerce Code, titled "Third Party Data Collection," to do the following:

1. Data covered by the bill—personal identifying information. Specifies that the act applies to personal identifying information from a resident of Texas that is collected, transferred, or processed by a third party data collection entity.
    - Personal identifying information as defined by Section 521.002(1), Business and Commerce Code, including:
        - Name, social security number, date of birth, government-issued identification number;
        - Mother's maiden name;
        - Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
        - Unique electronic identification number, address, or routing code; and
        - Telecommunication access device.
2. Data exempt from the bill. Carves out data that would not be covered by the bill, such as:

- Deidentified data, if the third party entity had taken reasonable measures to ensure the data could not be used to identify the individual and publicly provided notice of their commitment to do so; and contractually obligated the recipient of the data to do the same.
- Employee data;
- Publicly available information; or
- Inferences made exclusively from multiple independent sources of publicly available information that do not reveal sensitive covered data with respect to an individual.

3. Businesses exempt from the bill. Carves out businesses that would not be covered by the bill, such as:

    - Entities who process data on behalf of their clients to benefit their client's employees;
    - Entities under the same common ownership or corporate control sharing data amongst each other so long as a reasonable consumer would expect those entities to do so;
    - Service providers with respect to use of covered data;
    - Government entities and contractors; and
    - Nonprofits, resource centers, or clearinghouses that provide assistance to victims, families, child-serving professionals, and the general public on issues of missing and exploited children.

4. Notice requirement. Requires data brokers to post a clear and conspicuous notice on all platforms they operate on that states the following;

    - Its identity as a third-party collection entity;
    - Language provided by rule of the secretary of state for inclusion in the notice; and
    - Provides a link to the "do not collect" online registry.

5. Annual registration with the secretary of state. Requires data brokers to annually register with the secretary of state by filing a statement that must include:

    - Legal name; contact person; primary physical address, email address, telephone number, and Internet website address;
    - Description of data categories entity processes and transfers;
    - Whether the entity implements a purchaser credentialing process that includes taking reasonable steps to confirm that:

        - The actual identity of the customer and the customer's use of data matches what was provided to the entity; and
        - Customers will not use the data for a nefarious purpose.

    - If an entity has actual knowledge of possessing child personal identifying information, then must also include statements:

        - Detailing applicable data collection practices, databases, sales activities and opt-out policies;
        - Compliance with federal and state law on collecting, using, or disclosing child personal identifying information from and about the Internet;

    - Number of security breaches and how many consumers were affected by them in the preceding year;
    - Litigation or unresolved complaints related to the entity's operation;
    - Website link to allow individuals to easily access the "do not collect" registry.
    - Any other information designated by the secretary of state;

6. "Do not collect" registry. A public "do not collect" registry by the secretary of state that includes:

    - A search feature to identify a specific registered data broker;
    - A link and mechanism for individuals to submit "do not collect" requests to data brokers to delete the person's information within 30 days and to cease collecting, processing, or using the person's data without their "affirmative express consent."

        - Data brokers would have discretion to not comply with a request from individuals with convictions relating to child abduction or sexual exploitation nor requests from consumer reporting agencies.
        - This bill also defines the procedure for obtaining affirmative express consent.

7. Penalties for failure to comply. Failure for data brokers to comply with the law would:

    - Result in civil penalties that must be:

        - More than $100 for each day the entity is in violation and amount of unpaid registration fees; but
        - Less than $10,000 assessed against the same entity in a 12-month period; and

    - Constitute a deceptive trade practice under Chapter 17 of the Business and Commerce Code and render the entity liable to action by the attorney general's consumer protection division.

Committee Substitute:

- Replaces "third-party data collection entity" with "data broker" to align with comparable state data broker laws;
- Amends multiple definitions to better comply with state and federal data privacy regulations;
- Ensures that activities of federal, state, tribal, territorial, and government entities are exempt;
- Clarifies the necessary information required for data brokers to disclose when registering with the secretary of state;
- Removes language requiring the establishment of a "do not collect" registry, which would have allowed consumers residing in Texas to opt out of the collection and sale of their personal data with a one-time online submission;
- Enhances the protection of personal data by requiring data brokers to implement and maintain a Comprehensive Information Security Program;
- Changes the applicability of a Deceptive Trade Practice violation to failure of a data broker to implement and maintain a Comprehensive Information Security Program;
- Ensures that activities of financial institutions and credit reporting agencies subject to applicable federal law are exempt;
- Removes language requiring data brokers to ask their customers to disclose what they intend to do with the data they provide;
- Aligns data broker reporting requirements with the federal Child Online Privacy and Protection Act; and
- Ensures that secretary of state rulemaking takes into account the time necessary for data brokers to come into compliance.

Support:

- Texas Appleseed
- Texas Public Policy Foundation
- Texas Council on Family Violence

C.S.S.B. 2105 amends current law relating to the registration of and certain other requirements relating to data brokers, provides a civil penalty, and authorizes a fee.

RULEMAKING AUTHORITY

Rulemaking authority is expressly granted to the secretary of state in SECTION 1 (Section 509.010, Business and Commerce Code) of this bill.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends Subtitle A, Title 11, Business and Commerce Code, by adding Chapter 509, as follows:

CHAPTER 509. DATA BROKERS

Sec. 509.001. DEFINITIONS. Defines "biometric data," "child," "collect," "data broker," "deidentified data," "employee," "employee data," "genetic data," "individual," "known child," "personal data," "precise geolocation data," "process," "publicly available information," "sensitive data," "service provider," and "transfer."

Sec. 509.002. APPLICABILITY TO CERTAIN DATA. (a) Provides that this chapter, except as provided by Subsection (b), applies to personal data from an individual that is collected, transferred, or processed by a data broker.

(b) Provides that this chapter does not apply to the following data:

(1) deidentified data, if the data broker:

(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 in a clear and conspicuous manner:

(i) to process and transfer the data solely in a deidentified form without any reasonable means for reidentification; and

(ii) to not attempt to identify the information to an individual with whom the data is associated; and

(C) contractually obligates a person that receives the information from the provider:

(i) to comply with this subsection with respect to the information; and

(ii) to require that those contractual obligations be included 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 do not reveal sensitive data with respect to an individual; or

(5) data subject to Title V, Gramm-Leach-Bliley Act (15 U.S.C. Section 6801 et seq.).

Sec. 509.003. APPLICABILITY OF CHAPTER TO CERTAIN ENTITIES. (a) Provides that this chapter, except as provided by Subsection (b), applies only to a data broker that, in a 12-month period, derives:

(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; or

(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) Provides that this chapter does not apply to:

(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 or entity that collects personal data from another person or entity to which the person or entity is related by common ownership or corporate control, provided a reasonable consumer would expect the persons or entities 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 person or entity that furnishes information for inclusion in a consumer credit report or obtains a consumer credit report, but only to the extent the person or entity engages in activity regulated or authorized by the Fair Credit Reporting Act (15 U.S.C. Section 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; or

(6) a financial institution subject to Title V, Gramm-Leach-Bliley Act (15 U.S.C. Section 6801 et seq.).

Sec. 509.004. NOTICE ON WEBSITE OR MOBILE APPLICATION. Requires a data broker that maintains an Internet website or mobile application to post a conspicuous notice on the website or application that:

(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; and

(3) contains language provided by rule of the secretary of state (SOS) for inclusion in the notice.

Sec. 509.005. REGISTRATION. (a) Requires a data broker to which this chapter applies, to conduct business in this state, to register with SOS by filing a registration statement and paying a registration fee of $300.

(b) Requires that the registration statement include:

(1) the legal name of the data broker;

(2) a contact person 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:

(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; and

(B) a statement on 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; and

(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) Authorizes a registration of a data broker to include any additional information or explanation the data broker chooses to provide to SOS concerning the data broker's data collection practices.

(d) Provides that a registration certificate expires on the first anniversary of its date of issuance. Authorizes a data broker to renew a registration certificate by filing a renewal application, in the form prescribed by SOS, and paying a renewal fee in the amount of $300.

Sec. 509.006. REGISTRY OF DATA BROKERS. (a) Requires SOS to establish and maintain, on its Internet website, a searchable, central registry of data brokers registered under Section 509.005.

(b) Requires that the registry include:

(1) a search feature that allows a person searching the registry to identify a specific data broker; and

(2) for each data broker, the information filed under Section 509.005(b).

Sec. 509.007. PROTECTION OF PERSONAL DATA: COMPREHENSIVE INFORMATION SECURITY PROGRAM. (a) Provides that a data broker conducting business in this state has a duty to protect personal data held by that data broker as provided by this section.

(b) Requires a data broker to 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 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 personal data stored by the data broker.

(c) Requires that the comprehensive information security program required by this section:

(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 regulations 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 by:

(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 by 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) require the regular review of the scope of the program's security measures that is required to occur:

(A) at least annually; and

(B) whenever 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 protection of personal data in response to that event; and

(12) to the extent technically 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) the use of secure user authentication protocols that include each of the following features:

(i) controlling user log-in credentials and other identifiers;

(ii) using a reasonably secure method of assigning and selecting passwords or using unique identifier technologies, which are authorized to include biometrics or token devices;

(iii) 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;

(iv) restricting access to only active users and active user accounts; and

(v) blocking access to user credentials or identification after multiple unsuccessful attempts to gain access;

(B) the use of secure access control measures that include:

(i) restricting access to records and files containing personal data to only employees or contractors who need access to that personal data to perform the job duties of the employees or contractors; and

(ii) assigning to each employee or contractor with access to a computer containing personal data unique identification and a password, which is prohibited from being 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:

(i) transmitted records and files containing personal data that will travel across public networks; and

(ii) 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 files containing personal data on a system that is connected to the Internet, the use of reasonably current firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personal data; and

(G) the use of:

(i) a reasonably current version of system security agent software that is required to include malware protection and reasonably current patches and virus definitions; or

(ii) 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.

Sec. 509.008. CIVIL PENALTY. (a) Provides that a data broker that violates Section 509.004 or 509.005 is liable to this state for a civil penalty as prescribed by this section.

(b) Provides that a civil penalty imposed against a data broker under this section:

(1) subject to Subdivision (2), is prohibited from being in an amount less than the total of:

(A) $100 for each day the entity is in violation of Section 509.004 or 509.005; and

(B) the amount of unpaid registration fees for each year the entity failed to register in violation of Section 509.005; and

(2) is prohibited from exceeding $10,000 assessed against the same data broker in a 12-month period.

(c) Authorizes the attorney general to bring an action to recover a civil penalty imposed under this section. Authorizes the attorney general to recover reasonable attorney's fees and court costs incurred in bringing the action.

Sec. 509.009. DECEPTIVE TRADE PRACTICE. Provides that a violation of Section 509.007 by a data broker constitutes a deceptive trade practice in addition to the practices described by Subchapter E (Deceptive Trade Practices and Consumer Protection), Chapter 17, and is actionable under that subchapter.

Sec. 509.010. RULES. Requires SOS to adopt rules as necessary to implement this chapter.

SECTION 2. Requires SOS, not later than December 1, 2023, to adopt rules necessary to facilitate registration by a data broker under Section 509.005, Business and Commerce Code, as added by this Act, including by incorporating into the rules adequate time for a data broker to comply with Chapter 509, Business and Commerce Code, as added by this Act, following the adoption of the rules.

SECTION 3. Makes application of Chapter 509, Business and Commerce Code, as added by this Act, prospective to December 1, 2023.

SECTION 4. Effective date: September 1, 2023.