88R9015 JES-F

By:  Holland H.B. No. 4917

A BILL TO BE ENTITLED

AN ACT

relating to the regulation of third-party data collection entities; providing a civil penalty and authorizing a fee.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1.  Subtitle A, Title 11, Business & Commerce Code, is amended by adding Chapter 509 to read as follows:

CHAPTER 509. THIRD-PARTY DATA COLLECTION

Sec. 509.001.  DEFINITIONS. In this chapter:

(1)  "Biometric identifier" has the meaning assigned by Section 503.001.

(2)  "Child" means an individual younger than 18 years of age.

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

(4)  "Covered data" means personal identifying information to which this chapter applies as provided by Section 509.002.

(5)  "Deidentified data" means information that does not identify and is not linked or cannot reasonably be linked to an individual or to a device linked to that individual, regardless of whether the information is aggregated.

(6)  "Employee" includes 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" means information collected, processed, or transferred by an employer if the information:

(A)  is related to:

(i)  a job applicant and was collected during the course of the hiring and application process;

(ii)  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;

(iii)  an employee's emergency contact information; or

(iv)  an employee or the employee's spouse, dependent, covered family member, or beneficiary; and

(B)  was collected, processed, or transferred solely for:

(i)  a purpose relating to the status of a person described by Paragraph (A)(i) as a current or former job applicant of the employer;

(ii)  a purpose relating to the professional activities of an employee described by Paragraph (A)(ii) on behalf of the employer;

(iii)  the purpose of having an emergency contact on file for an employee described by Paragraph (A)(iii) and for transferring the information in case of an emergency; and

(iv)  the purpose of administering benefits to which an employee described by Paragraph (A)(iv) is entitled or to which another person described by that paragraph is entitled on the basis of the employee's position with the employer.

(8)  "Genetic data" means any data, regardless of format, concerning an individual's genetic characteristics. The term includes:

(A)  raw sequence data derived from sequencing all or a portion of an individual's extracted DNA; and

(B)  genotypic and phenotypic information obtained from analyzing an individual's raw sequence data.

(9)  "Personal identifying information" has the meaning assigned by Section 521.002.

(10)  "Precise geolocation data" means 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.

(11)  "Process," in the context of data, means to conduct or direct any operation or set of operations performed on the data, including using, storing, or otherwise handling the data.

(12)  "Publicly available information" means information:

(A)  that a business entity or service provider reasonably believes is lawfully available to the general public:

(i)  from a governmental record, unless use of the information by the business entity violates the governmental entity's restriction or terms of use for that information;

(ii)  from widely distributed media, including information from:

(a)  a telephone book or online directory;

(b)  a television, Internet, or radio program;

(c)  the news media; or

(d)  a generally available Internet website or online service on which the relevant information has not been restricted to a specific audience;

(iii)  from a disclosure as required by law; or

(iv)  by visual observation in a public place, other than data collected by a device in the individual's possession; and

(B)  that is not:

(i)  an obscene visual depiction under 18 U.S.C. Section 1460;

(ii)  an inference:

(a)  made exclusively from multiple independent sources of publicly available information; and

(b)  that does not disclose an individual's sensitive information;

(iii)  a biometric identifier;

(iv)  combined with personal identifying information;

(v)  genetic information not disclosed by the individual in a manner provided by Paragraph (A); or

(vi)  a nonconsensual intimate image, if known to be nonconsensual.

(13)  "Sensitive covered data" means:

(A)  a government-issued identifier not required by law to be available publicly, including:

(i)  a social security number;

(ii)  a passport number; or

(iii)  a driver's 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:

(i)  a financial account number;

(ii)  a credit or debit card number; or

(iii)  information that describes or reveals the income level or bank account balances of the individual;

(D)  a biometric identifier;

(E)  genetic data;

(F)  precise geolocation data;

(G)  an individual's private communication that:

(i)  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; and

(ii)  includes, unless the third-party data collection entity is the sender or an intended recipient of the communication:

(a)  the individual's voicemails, e-mails, texts, direct messages, or mail;

(b)  information that identifies the parties involved in the communications; and

(c)  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:

(i)  maintained for private use by an individual and stored on the individual's device or in another location; and

(ii)  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 not:

(i)  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. Section 613(h)(2); or

(ii)  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; or

(P)  information collected, processed, or transferred for the purpose of identifying information described by this subdivision.

(14)  "Service provider" means a person that receives, collects, processes, or transfers personal identifying information 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.

(15)  "Third-party data collection entity" means a business entity that collects, processes, or transfers covered data that the entity did not collect directly from the individual linked or linkable to the data.

(16)  "Transfer," in the context of data, means to disclose, release, share, disseminate, make available, or license the data by any means or medium.

Sec. 509.002.  APPLICABILITY TO CERTAIN DATA. (a) Except as provided by Subsection (b), this chapter applies to personal identifying information from an individual who resides in this state that is collected, transferred, or processed by a third-party data collection entity.

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

(1)  deidentified data, if the third-party data collection entity:

(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; or

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

Sec. 509.003.  APPLICABILITY OF CHAPTER TO CERTAIN BUSINESS ENTITIES. (a) Except as provided by Subsection (b), this chapter applies to a third-party data collection entity, which is a business entity that, in a 12-month period, derives:

(1)  more than 50 percent of the entity's revenue from processing or transferring covered data that the entity did not collect directly from the individuals to whom the data pertains; or

(2)  revenue from processing or transferring the covered data of more than 50,000 individuals that the entity did not collect directly from the individuals to whom the data pertains.

(b)  This chapter does not apply to:

(1)  a business entity that:

(A)  is engaging in the business of processing employee data for a third party for the sole purpose of providing benefits to the third party's employees; or

(B)  is collecting covered data from another entity to which the entity is related by common ownership or corporate control if a reasonable consumer would expect the entities to share the relevant data;

(2)  a business entity that is a service provider with respect to the entity's use of covered data;

(3)  a governmental entity or an entity that is collecting, processing, or transferring covered data as a service provider for a governmental entity; or

(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.

Sec. 509.004.  NOTICE ON WEBSITE OR MOBILE APPLICATION. A third-party data collection entity that maintains an Internet website or mobile application shall post a conspicuous notice on the website or application that:

(1)  states that the entity maintaining the website or application is a third-party data collection entity;

(2)  must be clear, not misleading, and be 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; and

(4)  provides a link to the "do not collect" online registry established under Section 509.006.

Sec. 509.005.  REGISTRATION. (a) To conduct business in this state, a third-party data collection entity to which this chapter applies that collects, processes, or transfers the covered date of individuals residing in this state shall register with the secretary of state by filing a registration statement and paying a registration fee of $300.

(b)  The registration statement must include:

(1)  the legal name of the third-party data collection entity;

(2)  a contact person and the primary physical address, e-mail address, telephone number, and Internet website address for the entity;

(3)  a description of the categories of data the entity processes and transfers;

(4)  a statement of whether or not the entity implements a purchaser credentialing process that includes taking reasonable steps to confirm that:

(A)  the actual identity of the entity's customer and the customer's use of the data matches the identity and intended use provided to the entity by the customer; and

(B)  the entity's customers will not use the data for a nefarious purpose;

(5)  if the entity has actual knowledge that the entity possesses personal identifying information of a child:

(A)  a statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the personal identifying information of a child; and

(B)  a statement on how the entity complies with applicable federal and state law regarding the collection, use, or disclosure of personal identifying information from and about a child on the Internet;

(6)  the number of security breaches the entity 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;

(7)  any litigation or unresolved complaints related to the operation of the entity; and

(8)  any Internet website link the entity provides to allow individuals to easily access the "do not collect" online registry established under Section 509.006.

(c)  A registration of a third-party data collection entity may include any additional information or explanation the third-party data collection entity chooses to provide to the secretary of state concerning the entity's data collection practices.

(d)  A registration certificate expires on the first anniversary of its date of issuance. A third-party data collection entity may renew a registration certificate by filing a renewal application, in the form prescribed by the secretary of state, and paying a renewal fee in the amount of $300.

Sec. 509.006.  REGISTRY OF THIRD-PARTY COLLECTING ENTITIES; DO NOT COLLECT REQUESTS. (a) The secretary of state shall establish and maintain, on its Internet website, a searchable, central registry of third-party data collection entities registered under Section 509.005.

(b)  The registry must include:

(1)  a search feature that allows a person searching the registry to identify a specific third-party data collection entity;

(2)  for each third-party data collection entity, the information filed under Section 509.005(b); and

(3)  a link and mechanism by which individuals may submit do not collect requests to third-party collection entities, other than consumer reporting agencies, as provided by Subsection (c).

(c)  The secretary of state shall ensure that under the mechanism described by Subsection (b) an individual has the capability to easily submit a single request requiring all registered third-party data collection entities to:

(1)  delete, not later than the 30th day after receiving the request, all covered data related to the requesting individual that is in their possession and was not collected from the individual directly; and

(2)  cease collecting, processing, or transferring covered data related to the requesting individual, unless the entity receives the individual's affirmative express consent to continue to collect, process, or transfer data, as applicable, in accordance with Subsection (e).

(d)  Notwithstanding Subsection (c), a third-party data collection entity may decline to comply with a request under that subsection if the entity:

(1)  knows that the individual has been convicted of a crime related to the abduction or sexual exploitation of a child, and that the data the entity is collecting is necessary to effectuate the purposes of a federal or state sex offender registry or of an entity described by Section 509.003(b)(4); or

(2)  is a consumer reporting agency governed by the Fair Credit Reporting Act (15 U.S.C. Section 1681 et seq.).

(e)  For purposes of Subsection (c)(2), an individual is considered to have given the individual's affirmative express consent if the individual, by an affirmative act, clearly communicates the individual's specific and unambiguous authorization for the act or practice in response to a specific request by a third-party data collection entity that:

(1)  is provided to the individual in a clear, conspicuous, and separate disclosure presented through:

(A)  the primary medium by which the entity offers its products or services; or

(B)  another medium regularly used in conjunction with the entity's products or services;

(2)  includes a description of the processing purpose for which the individual's consent is sought, that:

(A)  clearly states the specific categories of personal identifying information the business will collect, process, or transfer for that purpose;

(B)  includes a prominent heading; and

(C)  is written in easily understood language intended to enable a reasonable individual to identify and understand the processing purpose for which consent is sought;

(3)  explains the individual's right to give and revoke consent under this section;

(4)  is made in a manner reasonably accessible to and usable by an individual with a disability;

(5)  is made available in each language in which the business provides a product or service for which consent is sought;

(6)  presents the option to refuse consent at least as prominently as the option to accept; and

(7)  ensures that refusing to consent takes not more than the same amount of steps to complete as the option to accept consent.

(f)  If the processing purpose disclosed to an individual in a request made under Subsection (e) changes, a third-party data collection entity must request and receive a new consent that meets the requirements of that subsection before the entity is able to collect, transfer, or process any further information pursuant to that consent.

(g)  An individual's inaction or continued use of a service or product provided by a third-party data collection entity does not constitute an individual's affirmative express consent for purposes of Subsection (e).

(h)  A third-party data collection entity may not obtain or attempt to obtain an individual's affirmative express consent under Subsection (b) through:

(1)  the use of a false, fraudulent, or materially misleading statement or representation; or

(2)  the design, modification, or manipulation of a user interface to impair a reasonable individual's autonomy to consent or to withhold certain personal identifying information.

Sec. 509.007.  CIVIL PENALTY. (a) A third-party data collection entity that violates Section 509.004, 509.005, or 509.006 is liable to this state for a civil penalty as prescribed by this section.

(b)  A civil penalty imposed against a third-party data collection entity under this section:

(1)  subject to Subdivision (2), may not be 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)  may not exceed $10,000 assessed against the same entity in a 12-month period.

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

Sec. 509.008.  DECEPTIVE TRADE PRACTICE. A violation of this chapter constitutes a deceptive trade practice in addition to the practices described by Subchapter E, Chapter 17, and is actionable under that subchapter.

Sec. 509.009.  RULES. The secretary of state shall adopt rules as necessary to implement this chapter.

SECTION 2.  Not later than December 1, 2023, the secretary of state shall adopt rules necessary to facilitate registration by a third-party data collection entity under Section 509.005, Business & Commerce Code, as added by this Act.

SECTION 3.  Chapter 509, Business & Commerce Code, as added by this Act, applies only to the collection, processing, or transfer of personal identifying information by a third-party data collection entity on or after the effective date of this Act.

SECTION 4.  This Act takes effect September 1, 2023.