By:  Capriglione H.B. No. 4390

A BILL TO BE ENTITLED

AN ACT

relating to the privacy of personal identifying information; imposing a civil penalty.

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

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

SUBTITLE C. PRIVACY OF PERSONAL IDENTIFYING INFORMATION

CHAPTER 541. PERSONAL IDENTIFYING INFORMATION PROCESSED BY CERTAIN BUSINESSES

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 541.001.  SHORT TITLE. This chapter may be cited as the Texas Privacy Protection Act.

Sec. 541.002.  DEFINITIONS. In this chapter:

(1)  "Business" means a for-profit entity, including a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of the entity's shareholders or other owners.

(2)  "Collect" means:

(A)  buying, renting, gathering, obtaining, receiving, inferring, creating, or accessing any personal identifying information pertaining to an individual by any means; or

(B)  obtaining personal identifying information relating to an individual, actively or passively, or by observing the individual's behavior.

(3)  "Device" means any physical object capable of connecting to the Internet, directly or indirectly, or to another device and transmitting information.

(4)  "Personal identifying information" means a category of information relating to an identified or identifiable individual. The term does not include a specific category of personal identifying information that the attorney general exempts from this definition by rule. The term includes:

(A)  a social security number;

(B)  a driver's license number, passport number, military identification number, or any other similar number issued on a government document and used to verify an individual's identity;

(C)  a financial account number, credit or debit card number, or any security code, access code, or password that is necessary to permit access to an individual's financial account;

(D)  unique biometric information, including a fingerprint, voice print, retina or iris image, or any other unique physical representation;

(E)  physical or mental health information, including health care information;

(F)  the private communications or other user-created content of an individual that is not publicly available;

(G)  religious affiliation or practice information;

(H)  racial or ethnic origin information;

(I)  precise geolocation data; and

(J)  unique genetic information.

(5)  "Privacy risk" means potential adverse consequences to an individual or society at large arising from the processing of personal identifying information, including:

(A)  direct or indirect financial loss or economic harm;

(B)  physical harm;

(C)  psychological harm, including anxiety, embarrassment, fear, or other demonstrable mental trauma;

(D)  significant inconvenience or expenditure of time;

(E)  adverse outcomes or decisions with respect to an individual's eligibility for a right, benefit, or privilege in employment, including hiring, firing, promotion, demotion, or compensation;

(F)  credit or insurance harm, including denial of an application or obtaining less favorable terms related to housing, education, professional certification, or health care services;

(G)  stigmatization or reputational harm;

(H)  disruption and intrusion from unwanted commercial communications or contacts;

(I)  price discrimination; and

(J)  any other adverse consequence that affects an individual's private life, private family matters, actions or communications within an individual's home or similar physical, online, or digital location, if an individual has a reasonable expectation that personal identifying information will not be processed.

(6)  "Processing" means any operation or set of operations that are performed on personal identifying information or on sets of personal identifying information, including the collection, creation, generation, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, transfer, or dissemination of the information or otherwise making the information available.

(7)  "Third party" means a person engaged by a business to process, on behalf of the business, personal identifying information collected by the business.

Sec. 541.003.  APPLICABILITY. (a) This chapter applies only to a business that:

(1)  does business in this state;

(2)  has more than 50 employees;

(3)  collects the personal identifying information of more than 5,000 individuals, households, or devices or has that information collected on the business's behalf; and

(4)  satisfies one or more of the following thresholds:

(A)  has annual gross revenue in an amount that exceeds $25 million; or

(B)  derives 50 percent or more of the business's annual revenue by processing personal identifying information.

(b)  Except as provided by Subsection (c), this chapter applies only to personal identifying information that is:

(1)  collected over the Internet or any other digital network or through a computing device that is associated with or routinely used by an end user; and

(2)  linked or reasonably linkable to a specific end user.

(c)  This chapter does not apply to personal identifying information that is:

(1)  collected solely for facilitating the transmission, routing, or connections by which digital personal identifying information and other data is transferred between or among businesses; or

(2)  transmitted to and from the individual to whom the personal identifying information relates if the collector of the information does not access, review, or modify the content of the information, or otherwise perform or conduct any analytical, algorithmic, or machine learning processes on the information.

Sec. 541.004.  EXEMPTIONS. This chapter does not apply to:

(1)  publicly available information;

(2)  protected health information governed by Chapter 181, Health and Safety Code, or collected by a covered entity or a business associate of a covered entity, as those terms are defined by 45 C.F.R. Section 160.103, that is governed by the privacy, security, and breach notification rules in 45 C.F.R. Parts 160 and 164 adopted by the United States Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191) and Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5);

(3)  personal identifying information collected by a consumer reporting agency, as defined by Section 20.01, if the information is to be:

(A)  reported in or used to generate a consumer report, as defined by Section 1681a(d) of the Fair Credit Reporting Act (15 U.S.C. Section 1681 et seq.); and

(B)  used solely for a purpose authorized under that Act;

(4)  personal identifying information processed in accordance with the Gramm-Leach-Bliley Act (Pub. L. No. 106-102) and its implementing regulations; or

(5)  education information that is not publicly available personally identifiable information under the Family Educational Rights and Privacy Act of 1974 (20 U.S.C. Section 1232g) (34 C.F.R. Part 99).

Sec. 541.005.  RULES. The attorney general shall adopt rules necessary to implement, administer, and enforce this chapter.

SUBCHAPTER B. BUSINESS DUTIES

Sec. 541.051.  COLLECTION OF PERSONAL IDENTIFYING INFORMATION. A business may not collect personal identifying information unless:

(1)  the collection of the information is relevant and necessary to accomplish the purpose for which the information was collected; and

(2)  that purpose is specifically disclosed by the business in the notice required under Section 541.054.

Sec. 541.052.  PROCESSING OF PERSONAL IDENTIFYING INFORMATION. (a) A business may only process personal identifying information if:

(1)  the information is relevant to accomplish the purposes for which the information is to be processed;

(2)  those purposes are specifically disclosed by the business in the notice required under Section 541.054; and

(3)  the information is processed only to the extent necessary to achieve one or more of those purposes.

(b)  A business may not process personal identifying information unless:

(1)  the individual whose personal identifying information is collected by the business explicitly consents to the processing of the information; or

(2)  the business is required by law to process the information.

(c)  Notwithstanding Subsection (a), a business may not process personal identifying information if:

(1)  the business knows processing the information will likely:

(A)  violate state or federal law; or

(B)  interfere with or deny a right or privilege of an individual granted under the United States Constitution; or

(2)  the information is to be processed using automated processing, including algorithmic, machine learning, or artificial intelligence processing or predictive analysis, unless the processing is performed after the business:

(A)  conducts an objective and documented assessment of the automated processing and the results of the processing and determines the processing is reasonably free from bias and error;

(B)  analyzes the privacy risk of using automated processing and takes reasonable steps to mitigate that risk; and

(C)  concludes that, after all reasonable steps are taken to mitigate any privacy risk, the automated processing of the personal identifying information does not cause or is not likely to cause a substantial privacy risk.

Sec. 541.053.  DATA SECURITY PROGRAM. (a) A business shall develop, implement, and maintain a comprehensive data security program that contains administrative, technical, and physical safeguards for personal identifying information.

(b)  The safeguards required under Subsection (a) must be:

(1)  documented by the business; and

(2)  appropriate considering the:

(A)  size and complexity of the business;

(B)  nature and scope of the business's activities; and

(C)  sensitivity of the personal identifying information processed by the business.

Sec. 541.054.  NOTICE REQUIRED. (a) A business in a conspicuous manner shall provide a notice that includes a reasonably full and complete description of the business's practices governing the processing of personal identifying information before collecting personal identifying information. The notice must include:

(1)  the categories of personal identifying information processed by the business;

(2)  details on the type of processing used by the business;

(3)  the purposes for which the business processes personal identifying information; and

(4)  the involvement of any third party in processing personal identifying information on behalf of the business.

(b)  The notice required by Subsection (a) must be:

(1)  clear, drafted in plain language, and easy to understand; and

(2)  located in a prominent location at the business and on the business's Internet website if the business has an Internet website.

(c)  If a business processes geolocation data, biometric information, genetic information, racial or ethnic origin information, religious affiliation or practice information, physical or mental health information, or other personal identifying information that when processed is likely to create a significant privacy risk, the business must, before collecting the information, explicitly specify in the notice required under Subsection (a):

(1)  the categories or items of personal identifying information processed by the business, as applicable; and

(2)  the purposes for processing that information.

(d)  The information required under Subsection (c) must be included in the notice in a manner that is conspicuous, readily available, accessible, accurate, and easy to understand.

(e)  The notice required under this section may be included in the privacy policy required by Section 541.055.

Sec. 541.055.  PRIVACY POLICY. A business shall make publicly available on an ongoing basis a privacy policy that:

(1)  generally articulates the processing practices of the business for personal identifying information, including any analysis or predictions made by the business based on the processing of personal identifying information by the business;

(2)  includes an accurate and easy method for an individual to access the individual's personal identifying information that the business has processed about the individual; and

(3)  states that the business is required to:

(A)  stop processing personal identifying information on the date an individual closes the individual's account with the business; and

(B)  not later than the 30th day after the date the individual closes the account, delete the individual's personal identifying information unless retention of the information is required by other law or is necessary to comply with other law.

Sec. 541.056.  ACCESS TO INFORMATION. A business shall allow an individual to promptly and reasonably obtain:

(1)  confirmation of whether personal identifying information concerning the individual is processed by the business;

(2)  a description of the categories of personal identifying information processed by the business;

(3)  an explanation in plain language of the specific types of personal identifying information collected by the business; and

(4)  access to the individual's personal identifying information.

Sec. 541.057.  DELETION OF PERSONAL IDENTIFYING INFORMATION. If an individual who maintains an account with a business closes the account, the business shall:

(1)  stop processing the individual's personal identifying information on the date the individual closes the account;

(2)  not later than the 30th day after the date the account is closed, delete the individual's personal identifying information unless retention of the information is required by other law or is necessary to comply with other law; and

(3)  if the business engages a third party to process personal identifying information, notify the third party that the individual is closing the account.

Sec. 541.058.  ACCOUNTABILITY PROGRAM. To ensure compliance with this chapter, a business shall implement an ongoing accountability program and maintain an internal publication of the written policies and procedures necessary to implement the program. The program must include:

(1)  a process to identify, assess, and mitigate any reasonably foreseeable privacy risk;

(2)  procedures to provide remedies for privacy risk;

(3)  an annual assessment of the program and supporting policies and procedures;

(4)  methods and procedures for responding to data breaches and for addressing inquiries and complaints concerning personal identifying information; and

(5)  procedures for internal enforcement of the business's policies and discipline for noncompliance.

Sec. 541.059.  INFORMATION SHARED WITH THIRD PARTY. (a) A business that engages a third party to process personal identifying information collected by the business shall:

(1)  use due diligence in selecting the third party and shall ensure that the third party complies with the requirements of this chapter that apply to the third party; and

(2)  annually obtain from the third party verification that the third party is complying with the requirements.

(b)  Notwithstanding Subsection (a), a business may not share with any third party who the business engages to process the information an individual's biometric, health, or genetic information unless the individual consents to the sharing of the information.

(c)  A third party that processes personal identifying information received from a business may only process the information to the extent the business is authorized to process the information under Section 541.052 and shall:

(1)  implement a data security program described by Section 541.053;

(2)  implement an accountability program described by Section 541.058; and

(3)  if the business notifies the third party under Section 541.057 that an individual is closing the individual's account with the business:

(A)  stop processing the individual's personal identifying information on the date the individual closes the account; and

(B)  not later than the 30th day after the date the account is closed, delete the individual's personal identifying information unless retention of the information is required by other law or is necessary to comply with other law.

SUBCHAPTER C. ENFORCEMENT

Sec. 541.101.  CIVIL PENALTY. (a) A business that violates this chapter or a third party that violates Section 541.059(c) is liable to this state for a civil penalty in an amount of not more than $10,000 for each violation, not to exceed a total amount of $1 million.

(b)  The attorney general may bring an action in the name of the state against the business or third party to recover the civil penalty imposed under this section.

(c)  The attorney general is entitled to recover reasonable expenses, including reasonable attorney's fees, court costs, and investigatory costs, incurred in bringing an action under this section.

Sec. 541.102.  BUSINESS IMMUNITY FROM LIABILITY. A business that is in compliance with this chapter and engages a third party to process on behalf of the business personal identifying information collected by the business may not be held liable for a violation of Section 541.059(c) by the third party if the business does not have actual knowledge or a reasonable belief that the third party intends to violate that section.

SECTION 2.  Subchapter Z, Chapter 2252, Government Code, is amended by adding Section 2252.909 to read as follows:

Sec. 2252.909.  SALE OF PERSONAL IDENTIFYING INFORMATION PROHIBITED. Notwithstanding any other law, a governmental entity may not sell or offer to sell personal identifying information, as defined by Section 541.002, Business & Commerce Code, that is:

(1)  unique genetic information;

(2)  precise geolocation data; or

(3)  unique biometric information, including a fingerprint, voice print, retina or iris image, or any other unique physical representation.

SECTION 3.  This Act takes effect September 1, 2019.