SENATE BILL 339
By Campbell

HOUSE BILL 932

By McKenzie

AN ACT to amend Tennessee Code Annotated, Title 47; Title 50 and Title 61, relative to biometric data.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF TENNESSEE:

SECTION 1. Tennessee Code Annotated, Title 47, Chapter 18, is amended by adding the following as a new part:

47-18-3201.

This part is known and may be cited as the "Consumer Biometric Data Protection Act."

47-18-3202.

As used in this part:

(1) "Biometric identifier":

(A) Means data generated by automatic measurement of an individual's biological characteristics, such as an eye retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry; and

(B) Does not include:

(i) A writing sample, written signature, digital or physical photograph, human biological sample used for valid scientific testing or screening, demographic data, tattoo description, or physical description, such as height, weight, hair color, eye color, donated organ, or tissue;

(ii) A donated organ, tissue, blood, or serum stored on behalf of a recipient or potential recipient of an anatomical gift and

obtained or stored by an organ procurement agency that has been designated by the secretary of the United States department of health and human services as an organ procurement organization; and

(iii) Information collected, used, or stored for healthcare treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d et seq.), including an x-ray, magnetic resonance imaging or a positron emission tomography-computed tomography scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition;

(2) "Biometric information":

(A) Means information or data, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier; and

(B) Does not include information derived from an item or procedure described in subdivision (1)(B);

(3) "Confidential and sensitive information":

(A) Means personal information that can be used to uniquely identify an individual or an individual's account or property; and

(B) Includes a genetic marker or genetic testing information; a unique identifier number used to locate an account or property, including an account number, PIN number, or passcode; a driver license number; or a social security number;

(4) "Political subdivision" means a municipality, public corporation, body politic, authority, district, metropolitan government, county, agency, department, or board of the aforementioned entities, or another form of local government;

(5) "Private entity":

(A) Means an individual, partnership, corporation, limited liability company, association, or other group, however organized; and

(B) Does not include this state or a political subdivision of this state, a court of this state, or a clerk, judge, or other judicial officer of this state; and

(6) "Written authorization" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.

47-18-3203.

(a) A private entity shall not collect, capture, purchase, receive through trade, or otherwise obtain an individual's biometric identifier or biometric information, unless the private entity first:

(1) Informs the individual, or the individual's legally authorized representative, in writing:

(A) That the individual's biometric identifier or biometric information is being collected or stored; and

(B) The specific purpose and length of time for which a biometric identifier or biometric information is being collected, stored, and used; and

(2) Receives written authorization from the individual, or the individual's legally authorized representative, to collect, capture, purchase, receive through

trade, or otherwise obtain the individual's biometric identifier or biometric information.

(b) A private entity in possession of a biometric identifier or biometric information shall not:

(1) Sell, lease, trade, or otherwise profit from an individual's biometric identifier or biometric information; or

(2) Disclose or redisclose, or otherwise disseminate an individual's biometric identifier or biometric information unless:

(A) The individual to which the biometric identifier or biometric information belongs, or the individual's legally authorized representative, consents to the disclosure, redisclosure, or other form of dissemination;

(B) The disclosure, redisclosure, or other dissemination is necessary to complete a financial transaction requested or authorized by the individual to which the biometric identifier or biometric information belongs, or the individual's legally authorized representative;

(C) The disclosure, redisclosure, or other dissemination is required by state or federal law or municipal ordinance; or

(D) The disclosure, redisclosure, or other dissemination is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(c) A private entity in possession of a biometric identifier or biometric information shall store, transmit, and protect from disclosure all biometric identifiers and biometric information:

(1) Using the reasonable standard of care within the private entity's industry; and

(2) In a manner that is at least as protective as the manner in which the private entity stores, transmits, and protects other confidential and sensitive information; provided, that the manner in which the private entity stores, transmits, and protects other confidential and sensitive information conforms to standards that are at least as stringent as the standard described in subdivision (c)(1).

(d)

(1) A private entity in possession of a biometric identifier or biometric information shall:

(A) Develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining the biometric identifiers or information has been satisfied, or within three (3) years of the individual's last interaction with the private entity, whichever occurs first; and

(B) Comply with its established retention schedule and destruction guidelines. This subdivision (d)(2) does not require the private entity to comply with its established retention schedule and destruction guidelines if the private entity has received, or anticipates that it will receive, a valid warrant or subpoena issued by a court of competent jurisdiction that required the private entity to maintain the biometric identifiers or biometric information.

(2) A private entity operating before or on January 1, 2024, shall develop and make available to the public the written policy required in subdivision (d)(1) by January 1, 2024. A private entity incorporated or otherwise created after

January 1, 2024, shall develop and make available to the public the written policy required in subdivision (d)(1) within ninety (90) days of incorporation or creation.

47-18-3204.

(a) A violation of this part constitutes a violation of the Tennessee Consumer Protection Act of 1977, compiled in part 1 of this chapter. A violation of this part constitutes an unfair or deceptive act or practice affecting trade or commerce and is subject to the penalties and remedies as provided in the Tennessee Consumer Protection Act of 1977, in addition to the penalties and remedies in this part.

(b) An individual affected by a violation of this part may bring a private cause of action in a court of competent jurisdiction in this state against a private entity that the individual believes violated this part.

(c)

(1) If a court finds that a private entity violated this part, then the court may award the following to the prevailing party for each violation:

(A)

(i) For a negligent violation of this part, liquidated damages of one thousand dollars ($1,000), or actual damages, whichever is greater; or

(ii) For a reckless or willful violation of this part, liquidated damages of five thousand dollars ($5,000), or actual damages, whichever is greater;

(B) Court costs and reasonable attorneys' fees, including expert witness fees; and

(C) Other relief, including an injunction, as the court may deem appropriate.

(2) For purposes of determining how many violations a private entity has committed:

(A) Each instance of a private entity collecting, capturing, purchasing, receiving through trade, or otherwise obtaining an individual's biometric identifier or biometric information pursuant to § 47-18-3203(a) constitutes a separate violation;

(B) Each instance of a private entity selling, leasing, trading, or otherwise profiting from an individual's biometric identifier or biometric information constitutes a separate violation;

(C) Each instance of a private entity disclosing or redisclosing, or otherwise disseminating an individual's biometric identifier or biometric information without consent pursuant to § 47-18-3203(b)(2) constitutes a separate violation;

(D) Each instance of a private party failing to store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry, or in a manner that is at least as protective as the manner in which the private entity stores, transmits, and protects other confidential and sensitive information, pursuant to § 47-18-3203(c) constitutes a separate violation; and

(E) Each day of a private entity failing to develop and comply with a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information pursuant to § 47-18-3203(d)(1) constitutes a separate violation.

47-18-3205.

This part does not:

(1) Affect or otherwise prevent the admission or discovery of a biometric identifier or biometric information in an action in a court, tribunal, board, or agency;

(2) Apply in conflict with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. § 1320d et seq.), or rules promulgated pursuant to HIPAA. If application of this part would conflict with HIPAA, this part does not apply;

(3) Apply to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 (15 U.S.C. §§ 6801-6809 and 6821-6827), or rules promulgated pursuant to the act; or

(4) Apply to a contractor, subcontractor, or agent of a political subdivision, including this state, when the contractor, subcontractor, or agent is working for the political subdivision.

SECTION 2. This act takes effect January 1, 2024, the public welfare requiring it, and applies to conduct occurring on or after that date.