SENATE BILL 73
By Watson

HOUSE BILL 1181

By Garrett

AN ACT to amend Tennessee Code Annotated, Title 4; Title 12; Title 43; Title 45; Title 47; Title 48; Title 50; Title 61; Title 66 and Title 67, relative to commerce.

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

SECTION 1. This act is known and may be cited as the "Tennessee Information Protection Act."

SECTION 2. Tennessee Code Annotated, Title 47, Chapter 18, is amended by adding the following as a new part:

47-18-3201. Part definitions.

As used in this part:

(1) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. As used in this subdivision (1), "control" or "controlled" means:

(A) Ownership of, or the power to vote, more than fifty percent (50%) of the outstanding shares of a class of voting security of a company;

(B) Control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(C) The power to exercise controlling influence over the management of a company;

(2) "Authenticate" means to verify using reasonable means that a consumer who is entitled to exercise the rights in § 47-18-3203, is the same consumer who is exercising those consumer rights with respect to the personal information at issue;

(3) "Biometric data":

(A) Means data generated by automatic measurement of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retina or iris, or other unique biological patterns or characteristics that are used to identify a specific individual; and

(B) Does not include a physical or digital photograph, video recording, or audio recording or data generated from a photograph or video or audio recording; or information collected, used, or stored for healthcare treatment, payment, or operations under HIPAA;

(4) "Business associate" has the same meaning as defined by HIPAA;

(5) "Child" means a natural person younger than thirteen (13) years of age;

(6) "Consent":

(A) Means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal information relating to the consumer; and

(B) Includes a written statement, including a statement written by electronic means, or an unambiguous affirmative action;

(7) "Consumer" means a natural person who is a resident of this state acting only in a personal context;

(8) "Controller" means the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal information;

(9) "Covered entity" has the same meaning as defined by HIPAA;

(10) "De-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to that individual;

(11) "Health record":

(A) Means a written, printed, or electronically recorded material that:

(i) Was created or is maintained by a healthcare entity described in or licensed under title 68 in the course of providing healthcare services to an individual; and

(ii) Concerns the individual and the services provided; and

(B) Includes the substance of a communication made by an individual to a healthcare entity described in or licensed under title 68 in confidence during or in connection with the provision of healthcare services or information otherwise acquired by the healthcare entity about an individual in confidence and in connection with the provision of healthcare services to the individual;

(12) "HIPAA" means the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d et seq.);

(13) "Identified or identifiable natural person," "natural person," and "individual" mean a human being who can be readily identified, whether directly or indirectly;

(14) "Institution of higher education" means a public or private institution of higher education;

(15) "Nonprofit organization" means:

(A) A corporation organized under the Tennessee Nonprofit Corporation Act, compiled in title 48, chapter 51;

(B) An organization exempt from taxation under the Internal Revenue Code, codified in 26 U.S.C. §§ 501-530; or

(C) A public utility organized under the laws of this state;

(16) "Personal information":

(A) Means information that identifies, relates to, or describes a particular consumer or is reasonably capable of being directly or indirectly associated or linked with, a particular consumer;

(B) Includes:

(i) Identifiers such as a real name, alias, unique identifier, online identifier, internet protocol address, email address, account name, social security number, driver license number, passport number, or other similar identifiers;

(ii) Information that identifies, relates to, describes, or could be associated with, a particular individual, including, but not limited to, signature, physical characteristics or description, address, telephone number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or other financial, medical, or health insurance information;

(iii) Characteristics of protected classifications under state or federal law;

(iv) Commercial information, including records of personal property, products, or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;

(v) Biometric data;

(vi) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement;

(vii) Geolocation data;

(viii) Audio, electronic, visual, thermal, olfactory, or similar information;

(ix) Professional or employment-related information;

(x) Education information that is not publicly available information, or that is personally identifiable information as defined in 20 U.S.C. § 1232g and 34 C.F.R. § 99.1 et seq.; and

(xi) Inferences drawn from the information identified in this subdivision (16)(B) to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes; and

(C) Does not include information that is:

(i) Publicly available information; or

(ii) De-identified or aggregate consumer information;

(17) "Precise geolocation data":

(A) Means information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a natural person with precision and accuracy within a radius of one thousand seven hundred fifty feet (1,750'); and

(B) Does not include the content of communications or data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility;

(18) "Process" or "processing" means an operation or set of operations performed, whether by manual or automated means, on personal information or on sets of personal information, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal information;

(19) "Processor" means a natural or legal entity that processes personal information on behalf of a controller;

(20) "Profiling" means a form of automated processing performed on personal information to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements;

(21) "Protected health information" has the same meaning as defined by HIPAA;

(22) "Pseudonymous data" means personal information that cannot be attributed to a specific natural person without the use of additional information, so long as the additional information is kept separately and is subject to appropriate

technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable natural person;

(23) "Publicly available information" means information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience;

(24) "Sale of personal information":

(A) Means the exchange of personal information for monetary or other valuable consideration by the controller to a third party; and

(B) Does not include:

(i) The disclosure of personal information to a processor that processes the personal information on behalf of the controller;

(ii) The disclosure of personal information to a third party for purposes of providing a product or service requested by the consumer;

(iii) The disclosure or transfer of personal information to an affiliate of the controller;

(iv) The disclosure of information that the consumer:

(a) Intentionally made available to the general public via a channel of mass media; and

(b) Did not restrict to a specific audience;

(v) The disclosure or transfer of personal information to a third party as an asset that is part of a merger, acquisition,

bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets; or

(vi) The disclosure of personal information to a third party at the direction, and with the consent, of the consumer;

(25) "Sensitive data" means a category of personal information that includes:

(A) Personal information revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;

(B) The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;

(C) The personal information collected from a known child; or

(D) Precise geolocation data;

(26) "State agency" means an agency, institution, board, bureau, commission, council, or instrumentality of state government in the executive branch;

(27) "Targeted advertising":

(A) Means displaying to a consumer an advertisement that is selected based on personal information obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests; and

(B) Does not include:

(i) Advertisements based on activities within a controller's own websites or online applications;

(ii) Advertisements based on the context of a consumer's current search query, visit to a website, or online application;

(iii) Advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(iv) Personal information processed solely for measuring or reporting advertising performance, reach, or frequency;

(28) "Third party" means a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller; and

(29) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(A) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from the information's disclosure or use; and

(B) Is the subject of efforts that are reasonable under the circumstances to maintain the information's secrecy.

47-18-3202. Scope.

This part applies to persons that conduct business in this state or produce products or services that are targeted to residents of this state and that:

(1) During a calendar year, control or process personal information of at least one hundred thousand (100,000) consumers; or

(2) Control or process personal information of at least twenty-five thousand (25,000) consumers and derive more than fifty percent (50%) of gross revenue from the sale of personal information.

47-18-3203. Personal information rights – Consumers.

(a)

(1) A consumer may invoke the consumer rights authorized pursuant to subdivision (a)(2) at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke the consumer rights authorized pursuant to subdivision (a)(2) on behalf of the child regarding processing personal information belonging to the known child.

(2) A controller shall comply with an authenticated consumer request to exercise the right to:

(A) Confirm whether a controller is processing the consumer's personal information and to access the personal information;

(B) Correct inaccuracies in the consumer's personal information, taking into account the nature of the personal information and the purposes of the processing of the consumer's personal information;

(C) Delete personal information provided by or obtained about the consumer. A business is not required to delete information that it maintains or uses as aggregate or de-identified data, provided that such data in the possession of the business is not linked to a specific consumer;

(D) Obtain a copy of the consumer's personal information that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means;

(E) Request that a controller that sold personal information about the consumer, or disclosed the information for a business purpose, to disclose to the consumer:

(i) The categories of personal information about the consumer the business sold;

(ii) The categories of third parties to which the personal information about the consumer was sold by category of personal information for each category of third parties to which the personal information was sold; and

(iii) The categories of personal information about the consumer that the business disclosed for a business purpose; and

(F) Opt out of a controller's selling personal information about the consumer.

(b) Except as otherwise provided in this part, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to subdivision (a)(2) as follows:

(1) A controller shall respond to the consumer without undue delay, but in all cases within forty-five (45) days of receipt of a request submitted pursuant to subsection (a). The response period may be extended once by forty-five (45) additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial forty-five-day response period, together with the reason for the extension;

(2) If a controller declines to take action regarding the consumer's request, then the controller shall inform the consumer without undue delay, but in

all cases and at the latest within forty-five (45) days of receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision pursuant to subsection (c);

(3) Information provided in response to a consumer request must be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded, technically infeasible, excessive, or repetitive, then the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, technically infeasible, excessive, or repetitive nature of the request; and

(4) If a controller is unable to authenticate the request using commercially reasonable efforts, then the controller is not required to comply with a request to initiate an action under subsection (a) and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

(c) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision pursuant to subdivision (b)(2). The appeal process must be made available to the consumer in a conspicuous manner, must be available at no cost to the consumer, and must be similar to the process for submitting requests to initiate action pursuant to subsection (a). Within sixty (60) days of receipt of an appeal, a controller shall inform the consumer in writing of action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, then the controller shall also provide the consumer with an online

mechanism, if available, or other method through which the consumer may contact the attorney general and reporter to submit a complaint.

(d) A consumer's opt-out, as described in subdivision (a)(2)(F), prohibits the controller from selling personal information regarding the consumer.

47-18-3204. Data controller responsibilities – Transparency.

(a) A controller shall:

(1) Limit the collection of personal information to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer;

(2) Except as otherwise provided in this part, not process personal information for purposes that are beyond what is reasonably necessary to and compatible with the disclosed purposes for which the personal information is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;

(3) Establish, implement, and maintain reasonable administrative, technical, and physical data security practices, as described in § 47-18-3213, to protect the confidentiality, integrity, and accessibility of personal information. The data security practices must be appropriate to the volume and nature of the personal information at issue;

(4) Not be required to delete information that it maintains or uses as aggregate or de-identified data, provided that such data in the possession of the business is not linked to a specific consumer;

(5) Not process personal information in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising the consumer rights contained in

this part, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, this subdivision (a)(5) does not require a controller to provide a product or service that requires the personal information of a consumer that the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the right to opt out pursuant to § 47-18-3203(a)(2)(F) or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program; and

(6) Not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing the data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.).

(b) A provision of a contract or agreement that purports to waive or limit the consumer rights described in § 47-18-3203 is contrary to public policy and is void and unenforceable.

(c) Upon receipt of an authenticated consumer request, a controller shall provide the consumer with a reasonably accessible, clear, and meaningful privacy notice that includes:

(1) The categories of personal information processed by the controller;

(2) The purpose for processing personal information;

(3) How consumers may exercise their consumer rights pursuant to § 47-18-3203, including how a consumer may appeal a controller's decision with regard to the consumer's request;

(4) The categories of personal information that the controller sells to third parties, if any;

(5) The categories of third parties, if any, to whom the controller sells personal information; and

(6) The right to opt out of the sale of personal information to third parties and the ability to request deletion or correction of certain personal information.

(d) If a controller sells personal information to third parties or processes personal information for targeted advertising, then the controller shall clearly and conspicuously disclose the processing, as well as the manner in which a consumer may exercise the right to opt out of the processing.

(e)

(1) A controller shall provide, and shall describe in a privacy notice, at least one (1) of the following methods for consumers to submit a request to exercise consumer rights under this part:

(A) A toll-free telephone number;

(B) An email address;

(C) A web form; or

(D) A clear and conspicuous link on the controller's main internet homepage to an internet webpage that enables a consumer to exercise the rights provided under this section.

(2) Regardless of method, the controller shall ensure the method is capable of authenticating the identity of the consumer making the request. Controllers shall not require a consumer to create a new account in order to exercise consumer rights pursuant to § 47-18-3203, but may require a consumer to use an existing account.

47-18-3205. Responsibility according to role – Controller and processor.

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this part. The assistance must include:

(1) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests pursuant to § 47-18-3203; and

(2) Providing necessary information to enable the controller to conduct and document data protection assessments pursuant to § 47-18-3206.

(b) A contract between a controller and a processor governs the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract is binding and must clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract must also include requirements that the processor shall:

(1) Ensure that each person processing personal information is subject to a duty of confidentiality with respect to the data;

(2) At the controller's direction, delete or return all personal information to the controller as requested at the end of the provision of services, unless retention of the personal information is required by law;

(3) Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this part;

(4) Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; alternatively, the processor may arrange

for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this part using an appropriate and accepted control standard or framework and assessment procedure for the assessments. The processor shall provide a report of each assessment to the controller upon request; and

(5) Engage a subcontractor pursuant to a written contract in accordance with subdivision (b)(3) that requires the subcontractor to meet the obligations of the processor with respect to the personal information.

(c) This section does not relieve a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship as described in subsection (b).

(d) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal information is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal information remains a processor.

47-18-3206. Data protection assessments.

(a) A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal information:

(1) The processing of personal information for purposes of targeted advertising;

(2) The sale of personal information;

(3) The processing of personal information for purposes of profiling, where the profiling presents a reasonably foreseeable risk of:

(A) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

(B) Financial, physical, or reputational injury to consumers;

(C) A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where the intrusion would be offensive to a reasonable person; or

(D) Other substantial injury to consumers;

(4) The processing of sensitive data; and

(5) Processing activities involving personal information that present a heightened risk of harm to consumers.

(b) Data protection assessments conducted pursuant to subsection (a) must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that can be employed by the controller to reduce the risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal information will be processed, must be factored into this assessment by the controller.

(c) The attorney general and reporter may request that a controller disclose a data protection assessment that is relevant to an investigation conducted by the attorney general and reporter, and the controller shall make the data protection assessment available to the attorney general and reporter. The attorney general and reporter may evaluate the data protection assessment for compliance with the responsibilities set forth in § 47-18-3204. Data protection assessments are confidential and not open to public

inspection and copying. The disclosure of a data protection assessment pursuant to a request from the attorney general and reporter does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and information contained in the assessment.

(d) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(e) Data protection assessments conducted by a controller for the purpose of compliance with other laws, rules, or regulations may comply with this section if the assessments have a reasonably comparable scope and effect.

(f) Data protection assessment requirements apply to processing activities created or generated on or after July 1, 2024, and are not retroactive.

47-18-3207. Processing de-identified data – Exemptions.

(a) The controller in possession of de-identified data shall:

(1) Take reasonable measures to ensure that the data cannot be associated with a natural person;

(2) Publicly commit to maintaining and using de-identified data without attempting to reidentify the data; and

(3) Contractually obligate recipients of the de-identified data to comply with this part.

(b) This section does not require a controller or processor to:

(1) Reidentify de-identified data or pseudonymous data;

(2) Maintain data in identifiable form, or collect, obtain, retain, or access data or technology, in order to be capable of associating an authenticated consumer request with personal information; or

(3) Comply with an authenticated consumer rights request, pursuant to § 47-18-3203, if:

(A) The controller is not reasonably capable of associating the request with the personal information or it would be unreasonably burdensome for the controller to associate the request with the personal information;

(B) The controller does not use the personal information to recognize or respond to the specific consumer who is the subject of the personal information, or associate the personal information with other personal information about the same specific consumer; and

(C) The controller does not sell the personal information to a third party or otherwise voluntarily disclose the personal information to a third party other than a processor, except as otherwise permitted in this section.

(c) The consumer rights contained in §§ 47-18-3203 and 47-18-3204 do not apply to pseudonymous data in cases where the controller is able to demonstrate information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing that information.

(d) A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address breaches of those contractual commitments.

47-18-3208. Limitations.

(a) This part does not restrict a controller's or processor's ability to:

(1) Comply with federal, state, or local laws, rules, or regulations;

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(3) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;

(4) Investigate, establish, exercise, prepare for, or defend legal claims;

(5) Provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer prior to entering into a contract;

(6) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

(7) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activity, or illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for such action;

(8) Engage in public- or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entity that determines whether:

(A) Deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;

(B) The expected benefits of the research outweigh the privacy risks; and

(C) The controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including risks associated with reidentification; or

(9) Assist another controller, processor, or third party with the obligations under this part.

(b) The obligations imposed on controllers or processors under this part do not restrict a controller's or processor's ability to collect, use, or retain data to:

(1) Conduct internal research to develop, improve, or repair products, services, or technology;

(2) Effectuate a product recall;

(3) Identify and repair technical errors that impair existing or intended functionality; or

(4) Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(c) The obligations imposed on controllers or processors under this part do not apply where compliance by the controller or processor with this part would violate an evidentiary privilege under the laws of this state. This part does not prevent a controller or processor from providing personal information concerning a consumer to a person

covered by an evidentiary privilege under the laws of this state as part of a privileged communication.

(d)

(1) A controller or processor that discloses personal information to a third-party controller or processor, in compliance with the requirements of this part, is not in violation of this part if:

(A) The third-party controller or processor that receives and processes the personal information is in violation of this part; and

(B) At the time of disclosing the personal information, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation.

(2) A third-party controller or processor receiving personal information from a controller or processor in compliance with the requirements of this part is likewise not in violation of this part for the violations of the controller or processor from which it receives such personal information.

(e) This part does not impose an obligation on controllers and processors that adversely affects the rights or freedoms of a person, such as exercising the right of free speech pursuant to the First Amendment to the United States Constitution, or applies to the processing of personal information by a person in the course of a purely personal activity.

(f) A controller shall not process personal information for purposes other than those expressly listed in this section unless otherwise allowed by this part. Personal information processed by a controller pursuant to this section may be processed to the extent that the processing is:

(1) Reasonably necessary and proportionate to the purposes listed in this section; and

(2) Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. Personal information collected, used, or retained pursuant to subsection (b) shall, where applicable, take into account the nature and purpose or purposes of the collection, use, or retention. The data is subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal information and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal information.

(g) If a controller processes personal information pursuant to an exemption in this section, then the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with subsection (f).

(h) Processing personal information for the purposes expressly identified in subdivisions (a)(1)-(9) does not solely make an entity a controller with respect to the processing.

47-18-3209. Investigative authority.

If the attorney general and reporter has reasonable cause to believe that an individual, controller, or processor has engaged in, is engaging in, or is about to engage in a violation of this part, then the attorney general and reporter may issue a civil investigative demand.

47-18-3210. Exemptions.

(a) This part does not apply to:

(1) A body, authority, board, bureau, commission, district, or agency of this state or of a political subdivision of this state;

(2) A financial institution, an affiliate of a financial institution, or data subject to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.);

(3) An individual, firm, association, corporation, or other entity that is licensed in this state under title 56 as an insurance company and transacts insurance business;

(4) A covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States department of health and human services, 45 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and the federal Health Information Technology for Economic and Clinical Health Act (P.L. 111-5);

(5) A nonprofit organization;

(6) An institution of higher education;

(7) Protected health information under HIPAA;

(8) Health records for purposes of title 68;

(9) Patient identifying information for purposes of 42 U.S.C. § 290dd-2;

(10) Personal information:

(A) Processed for purposes of:

(i) Research conducted in accordance with the federal policy for the protection of human subjects under 45 C.F.R. Part 46;

(ii) Human subjects research conducted in accordance with good clinical practice guidelines issued by The International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use; or

(iii) Research conducted in accordance with the protection of human subjects under 21 C.F.R. Parts 6, 50, and 56; or

(B) Processed or sold in connection with research conducted in accordance with the requirements set forth in this part, or other research conducted in accordance with applicable law;

(11) Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986 (42 U.S.C. § 11101 et seq.);

(12) Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act (42 U.S.C. § 299b-21 et seq.);

(13) Information derived from the healthcare-related information listed in this subsection (a) that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;

(14) Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this subsection (a) that is maintained by a covered entity or business associate as defined by HIPAA or a program or a qualified service organization as defined by 42 U.S.C. § 290dd-2;

(15) Information used only for public health activities and purposes as authorized by HIPAA;

(16) The collection, maintenance, disclosure, sale, communication, or use of personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of a consumer report, but

only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);

(17) Personal information collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721 et seq.);

(18) Personal information or educational information regulated by the federal Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g et seq.);

(19) Personal information collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (12 U.S.C. § 2001 et seq.);

(20) Data processed or maintained:

(A) In the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role;

(B) As the emergency contact information of an individual under this part used for emergency contact purposes; or

(C) That is necessary to retain to administer benefits for another individual relating to the individual under subdivision (a)(20)(A) and used for the purposes of administering those benefits;

(21) Information collected as part of public- or peer-reviewed scientific or statistical research in the public interest; or

(22) An insurance producer licensed under title 56.

(b) Controllers and processors that comply with the verifiable parental consent requirements of the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) are deemed compliant with an obligation to obtain parental consent under this part.

(c) This part does not require a controller, processor, third party, or consumer to disclose trade secrets.

47-18-3211. Contracts.

(a) A provision of a contract or agreement that waives or limits a consumer's rights under this part, including, but not limited to, a right to a remedy or means of enforcement, is contrary to public policy, void, and unenforceable.

(b) This part does not prevent a consumer from declining to request information from a controller, declining to opt out of a controller's sale of the consumer's personal information, or authorizing a controller to sell the consumer's personal information after previously opting out.

(c) This part applies to contracts entered into on or after the effective date of this act.

47-18-3212. Enforcement – Civil penalty – Expenses.

(a) The attorney general and reporter has exclusive authority to enforce this part.

(b) The attorney general and reporter may develop reasonable cause to believe that a controller or processor is in violation of this part, based on the attorney general and reporter's own inquiry or on consumer or public complaints. Prior to initiating an action under this part, the attorney general and reporter shall provide a controller or processor sixty-days' written notice identifying the specific provisions of this part the attorney general and reporter alleges have been or are being violated. If within the sixty-day period, the controller or processor cures the noticed violation and provides the attorney general and reporter an express written statement that the alleged violations

have been cured and that no further violations shall occur, then the attorney general and reporter shall not initiate an action against the controller or processor.

(c) If a controller or processor continues to violate this part following the cure period in subsection (b) or breaches an express written statement provided to the attorney general and reporter under subsection (b), then the attorney general and reporter may bring an action in a court of competent jurisdiction seeking any of the following relief:

(1) Declaratory judgment that the act or practice violates this chapter;

(2) Injunctive relief, including preliminary and permanent injunctions, to prevent an additional violation of and compel compliance with this part;

(3) Civil penalties, as described in subsection (d);

(4) Reasonable attorney's fees and investigative costs; or

(5) Other relief the court determines appropriate.

(d) A court may impose a civil penalty of up to fifteen thousand dollars ($15,000) for each violation of this part. A civil penalty imposed under this section must be assessed using the following criteria:

(1) Each provision of this part violated is a separate violation; and

(2) Each consumer affected is a separate violation.

(e) When calculating civil penalties, the court may consider all of the following:

(1) The number of affected consumers;

(2) The severity of the violation;

(3) The size, nature, and complexity of the controller or processor's business;

(4) The sensitivity of the information in question; and

(5) The precautions taken by the controller or processor to prevent a violation.

(f) Appropriate relief may be awarded to each identified consumer affected by a violation of this part, regardless of whether actual damages were suffered.

(g) If the court finds the controller or processor willfully or knowingly violated this part, then the court may, in its discretion, award treble damages.

(h) A violation of this part shall not serve as the basis for, or be subject to, a private right of action, including a class action lawsuit, under this part or other law.

(i) The attorney general and reporter may recover reasonable expenses incurred in investigating and preparing a case, including attorney fees, in an action initiated under this part.

47-18-3213. Privacy program.

(a)

(1) A controller or processor shall create, maintain, and comply with a written privacy program that reasonably conforms to the National Institute of Standards and Technology (NIST) privacy framework entitled "A Tool for Improving Privacy through Enterprise Risk Management Version 1.0."

(2) When a subsequent revision to the NIST privacy framework is published, a controller or processor shall reasonably conform its privacy program to the revised framework not later than one (1) year after the publication date stated in the most recent revision.

(b) A controller or processor's privacy program shall provide an individual with the substantive rights required by this part.

(c) The scale and scope of a controller or processor's privacy program under subsection (a) is appropriate if it is based on all of the following factors:

(1) The size and complexity of the controller or processor's business;

(2) The nature and scope of the activities of the controller or processor;

(3) The sensitivity of the personal information processed;

(4) The cost and availability of tools to improve privacy protections and data governance; and

(5) Compliance with a comparable state or federal law.

(d) A controller or processor's privacy program must also disclose the commercial purposes for which the controller or processor collects, controls, or processes personal information.

(e) A controller or processor's failure to maintain a privacy program that reflects the controller or processor's data privacy practices to a reasonable degree of accuracy is considered an unfair and deceptive act or practice under § 47-18-104, except that a consumer is not entitled to a private right of action under § 47-18-109.

(f)

(1) In addition to the requirements of this section:

(A) A controller may be certified pursuant to the Asia Pacific Economic Cooperation's Cross Border Privacy Rules system; and

(B) A processor may be certified pursuant to the Asia Pacific Economic Cooperation's Privacy Recognition for Processors system.

(2) Certifications under this subsection (f) may be considered in addition to the factors in subsection (c).

47-18-3214. Affirmative defense.

A controller or processor has an affirmative defense to a cause of action for a violation of this part if the controller or processor creates, maintains, and complies with a written privacy program as described in § 47-18-3213.

SECTION 3. If a provision of this act or its application to a person or circumstance is held invalid, then the invalidity does not affect other provisions or applications of the act that can be given effect without the invalid provision or application, and to that end, the provisions of this act are severable.

SECTION 4. The headings in this act are for reference purposes only and do not constitute a part of the law enacted by this act. However, the Tennessee Code Commission is requested to include the headings in any compilation or publication containing this act.

SECTION 5. This act takes effect July 1, 2024, the public welfare requiring it.