THE SENATE
THIRTY-SECOND LEGISLATURE, 2023
STATE OF HAWAII

S.B. NO. 974

JAN 2 0 2023

A BILL FOR AN ACT

RELATING TO CONSUMER DATA PROTECTION.

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

SECTION 1. The Hawaii Revised Statutes is amended by adding a new chapter to title 26 to be appropriately designated and to read as follows:

"**CHAPTER**

CONSUMER DATA PROTECTION ACT

§ -1 Definitions. As used in this chapter, unless the context otherwise requires:

"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. Solely for the purposes of this definition, "control" or "controlled" means:

(1) Ownership of, or the power to vote, more than fifty per cent of the outstanding shares of any class of voting security of a company;

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

(3) Power to exercise controlling influence over the management of a company.

"Authenticate" means to verify through reasonable means that a consumer attempting to exercise the consumer rights specified in section -3 is the actual consumer with the consumer rights with respect to the personal data at issue.

"Biometric data" means data generated by automatic measurements of an individual's biological characteristics, including fingerprints, voiceprints, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual. The term "biometric data" does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act.

"Business associate" shall have the same meaning as the term is defined in title 45 Code of Federal Regulations section 160.103.

"Child" means any natural person younger than thirteen years of age.

"Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" includes a written statement, including statement written by electronic means, or any other unambiguous affirmative action. "Consent" does not include:

(1) Acceptance of general or broad terms of use or document containing general or broad descriptions of personal data processing along with other unrelated information;

(2) Hovering over, muting, pausing, or closing a given piece of content; or

(3) Agreement obtained through the use of dark patterns.

"Consumer" means a natural person who is a resident of the State acting only in an individual or household context. The

term "consumer" does not include a natural person acting in a commercial or employment context.

"Controller" means the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data.

"Covered entity" shall have the same meaning as the term is defined in title 45 Code of Federal Regulations section 160.103.

"Dark patterns" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice. "Dark patterns" includes any practice referred to by the Federal Trade Commission as a "dark pattern".

"De-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to the person.

"Department" means the department of the attorney general.

"Fund" means the consumer privacy special fund established pursuant to section -12.

"Health Insurance Portability and Accountability Act" means the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, as amended.

"Identified or identifiable natural person" means a natural person who can be readily identified, directly, or indirectly.

"Institution of higher education" means:

(1) The University of Hawaii system, or one of its campuses; or

(2) A private college or university authorized to operate in the State pursuant to chapter 305J.

"Nonprofit organization" means any:

(1) Corporation incorporated pursuant to chapter 414D;

(2) Organization exempt from taxation under section 501(c)(3), (6), or (12) of the Internal Revenue Code of 1986, as amended; or

(3) Electric utility cooperative association subject to chapter 421C.

"Personal data" means any information that is linked or could be reasonably linkable to an identified or identifiable natural person. The term "personal data" does not include de-identified data or publicly available information.

"Precise geolocation data" means information derived from technology, including 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 1,750 feet. The term "precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

"Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, including the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

"Processor" means a natural or legal person that processes personal data on behalf of a controller.

"Profiling" means any form of automated processing performed on personal data 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.

"Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information that is:

(1) Stored separately; and

(2) Subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

"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.

"Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. The term "sale of personal data" does not include:

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

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

(3) The disclosure or transfer of personal data to an affiliate of the controller;

(4) The disclosure of personal data in which the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party;

(5) 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; or

(6) The disclosure or transfer of personal data to a third party as an asset that is part of an actual or proposed merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

"Sensitive data" means a category of personal data. "Sensitive data" includes:

(1) Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sexual history, sexual orientation, or citizenship or immigration status;

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

(3) The personal data collected from a known child; or

(4) Precise geolocation data.

"Targeted advertising" means displaying to a consumer advertisements based on personal data obtained or inferred from that consumer's activities over time and across non-affiliated websites or online applications to predict the consumer's preferences or interests. The term "targeted advertising" does not include:

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

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

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

(4) Processing personal data processed solely for measuring or reporting advertising performance, reach, or frequency.

"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.

§ -2 Scope; exemptions. (a) This chapter applies to persons that conduct business in the State or produce products or services that are targeted to residents of the State and:

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

(2) Control or process personal data of at least twenty-five thousand consumers and derive over twenty-five per cent of gross revenue from the sale of personal data.

(b) This chapter shall not apply to any:

(1) Government entity;

(2) Nonprofit organization; or

(3) Institution of higher education.

(c) The following information and data are exempt from this chapter:

(1) Protected health information as defined in title 45 Code of Federal Regulations section 160.103;

(2) Nonpublic personal information, as defined in the Gramm-Leach-Bliley Act (15 U.S.C. chapter 94);

(3) Confidential rewards described in title 42 United States Code section 290dd-2;

(4) Identifiable private information for purposes of the protection of human subjects under title 45 Code of Federal Regulations part 46; identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use; identifiable private information collected as part of a clinical investigation under title 21 Code of Federal Regulations parts 50 and 56; personal data used or shared in research conducted in accordance with the requirements set forth in this chapter; and

other research conducted in accordance with applicable law;

(5) Information and documents created for purposes of the Health Care Quality Improvement Act of 1986 (42 U.S.C. chapter 117);

(6) Patient safety work product for purposes of the Patient Safety and Quality Improvement Act (42 U.S.C. sections 299b-21 to 299b-26);

(7) Information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to the Health Insurance Portability and Accountability Act;

(8) Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as information exempt under this subsection that is maintained by a covered entity or business associate as defined in the Health Insurance Portability and Accountability Act or a program or a qualified service organization as defined in title 42 Code of Federal Regulations section 2.11;

(9) Information used only for public health activities and purposes as authorized by the Health Insurance Portability and Accountability Act;

(10) The collection, maintenance, disclosure, sale, communication, or use of any 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 the activity is regulated by and authorized under the Fair Credit Reporting Act (15 U.S.C. sections 1681 to 1681x);

(11) Personal data collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act of 1994 (18 U.S.C. chapter 123);

(12) Personal data regulated by the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g);

(13) Personal data collected, processed, sold, or disclosed in compliance with the Farm Credit Act of 1971, P.L. 92-181, as amended; and

(14) Data processed or maintained:

(A) In the course of an individual applying to, 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 chapter used for emergency contact purposes; or

(C) As necessary to retain to administer benefits for another individual relating to the individual under subparagraph (A) and used for the purposes of administering those benefits.

(d) Controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act (15 U.S.C. chapter 91) shall be deemed compliant with any obligation to obtain parental consent under this chapter.

§ -3 Personal data rights; consumers. (a) A consumer may invoke the consumer rights specified in this subsection at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A child's parent or legal guardian may invoke the same consumer rights on behalf of the child regarding processing personal data belonging to the child. A controller shall comply with an authenticated consumer request to exercise the right:

(1) To confirm whether or not a controller is processing the consumer's personal data and to access the personal data;

(2) To correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

(3) To delete personal data provided by, or inferred or obtained about, the consumer;

(4) To obtain a copy of the consumer's personal data processed by the controller in a format that:

(A) Is portable;

(B) To the extent technically feasible, is readily usable; and

(C) Allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means; and

(5) To opt-out of the processing of the personal data for purposes of:

(A) Targeted advertising;

(B) The sale of personal data; or

(C) Profiling in furtherance of decisions made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, including food and water.

(b) A consumer may exercise rights under this section by secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with section -4 to exercise the rights of the consumer to opt-out

of the processing of the consumer's personal data for purposes of subparagraph (a)(5) on behalf of the consumer. In the case of processing personal data of a known child, the parent or legal guardian of the child may exercise the child's consumer rights on the child's behalf. In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship, or other protective arrangement, the guardian or conservator of the consumer may exercise the consumer's rights on the consumer's behalf.

(c) Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer rights specified in subsection (a) as follows:

(1) A controller shall respond to the consumer without undue delay, but in all cases within forty-five days of receipt of the request submitted pursuant to the methods described in subsection (a). The response period may be extended once by forty-five 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, the controller, without undue delay, but no later than forty-five days of receipt of the request, shall inform the consumer in writing of the justification for declining to take action and instructions for appealing the decision pursuant to subsection (c);

(3) Information provided in response to a consumer request shall be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded, excessive, or repetitive, 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 shall bear the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request; and

(4) If a controller is unable to authenticate the request using commercially reasonable efforts, the controller

shall not be 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; provided that no controller shall be required to authenticate an opt-out request, except that a controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that the request is fraudulent; provided further that if a controller denies an opt-out request because the controller believes that the request is fraudulent, the controller shall send a notice to the person who made the request disclosing that the controller believes the request is fraudulent, why the controller believes the request is fraudulent, and that the controller shall not comply with the request.

(d) 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 subsection (c)(2); provided that the

appeal process shall be similar to the process for submitting requests to initiate action pursuant to subsection (a). Within sixty days of receipt of an appeal, a controller shall inform the consumer in writing of its decision, including a written explanation of the reasons for the decision. If the appeal is denied, the controller shall also provide the consumer with an online method, if available, or other method through which the consumer may contact the department to submit a complaint.

§ -4 Authorized agent; designation; powers. A consumer may designate another person to serve as the consumer's authorized agent, act on the consumer's behalf, or opt-out of the processing of the consumer's personal data for one or more of the purposes specified in subdivision section -3(a)(5). The consumer may designate an authorized agent by way of, among other things, a technology, including an internet link, browser setting, browser extension, or global device setting, indicating the consumer's intent to opt-out of the processing. A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and

the authorized agent's authority to act on the consumer's behalf.

§ -5 Data controller responsibilities; transparency.

(a) A controller shall:

(1) Limit the collection of personal data to data that 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 chapter, not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which the personal data 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 to protect the confidentiality, integrity, and accessibility of personal data. The data security practices shall be appropriate to the volume and nature of the personal data at issue;

(4) Provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy to use as the mechanism by which the consumer provided the consumer's consent and, upon revocation of the consumer's consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of the request;

(5) Not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances in which a controller has actual knowledge, and willfully disregards, that the consumer is at least thirteen years of age but younger than sixteen years of age; provided that no controller shall discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer;

(6) Not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers; and

(7) 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 Children's Online Privacy Protection Act (15 U.S.C. chapter 91);

provided that nothing in this subsection shall be construed as requiring a controller to provide a product or service that requires the personal data 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 offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts or club card program.

(b) Any provision of a contract or agreement that purports to waive or limit in any way consumer rights pursuant to

section -3 shall be deemed contrary to public policy and shall be void and unenforceable.

(c) Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

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

(2) The purpose for processing personal data;

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

(4) The categories of personal data that the controller shares with third parties, if any;

(5) The categories of third parties, if any, with whom the controller shares personal data; and

(6) An active electronic mail address or other online mechanism that the consumer may use to contact the controller.

(d) If a controller sells personal data to third parties or processes personal data for targeted advertising, 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) A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights under this chapter. Those means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of the requests, and the ability of the controller to authenticate 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 section -3 but may require a consumer to use an existing, active account.

(f) A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, 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; provided that nothing in this chapter shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect

or maintain or to 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 consumer's right to opt-out pursuant to section -3 or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

§ -6 Responsibility according to role; controller and processor. (a) In meeting its obligations under this chapter, a processor shall adhere to the instructions of a controller and shall assist the controller. The assistance shall include:

(1) Consideration of 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 section -3;

(2) Consideration of account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing

the personal data and in relation to the notice of security breach pursuant to section 487N-2 in order to meet the controller's obligations; and

(3) The provision of necessary information to enable the controller to conduct and document data protection assessments pursuant to section -7.

(b) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and 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 shall also include requirements that the processor shall:

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

(2) At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data 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 chapter;

(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 chapter using an appropriate and accepted control standard or framework and assessment procedure for the assessments. The processor shall provide a report of the assessment to the controller upon request; and

(5) Engage any subcontractor pursuant to a written contract in accordance with subsection (c) that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(c) Nothing in this section shall be construed to relieve a controller or a processor from the liabilities imposed on the

controller or processor by virtue of the controller's or processor's role in the processing relationship as defined by this chapter.

(d) A determination regarding 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 data is to be processed. A person who is not limited in the processing of personal data pursuant to a controller's instructions, or who fails to adhere to these instructions, shall be deemed to be a controller and not a processor with respect to the specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data shall remain a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor shall be deemed to be a controller.

§ -7 Data protection assessments. (a) The data protection assessment requirements of this section shall apply to processing activities created or generated after January 1, 2025.

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

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

(2) The sale of personal data;

(3) The processing of personal data 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 intrusion 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) Any processing activities involving personal data that present a heightened risk of harm to consumers.

(c) Data protection assessments conducted pursuant to subsection (b) shall identify and evaluate the benefits, direct or indirect, that a controller, consumer, other stakeholders, and the public may derive from processing against the potential risks to the rights of consumers 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 data is processed, shall be factored into this assessment by the controller.

(d) The department may request, pursuant to a civil investigative demand, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the department, and the controller shall make the data protection assessment available to the department. The department may evaluate the data protection assessment for compliance with the responsibilities set forth in section -5. Data protection assessments shall be confidential and exempt from public inspection and copying under chapter 92F. The disclosure of a data protection assessment pursuant to a request

from the department shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

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

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

§ -8 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 re-identify the data; and

(3) Contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter.

(b) Nothing in this chapter shall be construed to require a controller or processor to:

(1) Re-identify de-identified data or pseudonymous data; or

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

(c) Nothing in this chapter shall be construed to require a controller or processor to comply with an authenticated consumer rights request pursuant to section -3 if all of the following are true:

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

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

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

(d) The consumer rights specified in section -3(a)(1) to (4) and section -5 shall not apply to pseudonymous data in cases in which the controller is able to demonstrate that any additional information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that:

(1) Ensure that the personal data is not attributed to an identified or identifiable natural person; and

(2) Prevent the controller from accessing the information.

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

§ -9 Limitations. (a) Nothing in this chapter shall be construed to 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, county, 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 county 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 before 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 activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any of those actions;

(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 independent oversight entity that determines:

(A) If the 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) If the controller has implemented reasonable safeguards to mitigate privacy risks associated

with research, including any risks associated with reidentification;

(9) Assist another controller, processor, or third party with any of the obligations under this subsection; or

(10) Process personal data for reasons of public interest in the area of public health, community health, or population health, but only to the extent that processing is:

(A) Subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed; and

(B) Under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law.

(b) The obligations imposed on controllers or processors under this chapter shall 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, 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 chapter shall not apply where compliance by the controller or processor with this chapter would violate an evidentiary privilege under state law. Nothing in this chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under state law as part of a privileged communication.

(d) A controller or processor that discloses personal data to a third-party controller or processor in compliance with the

requirements of this chapter shall not be deemed to be in violation of this chapter if the third-party controller or processor that receives and processes the personal data is in violation of this chapter; provided that, at the time of the disclosure of the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. A third-party controller or processor that receives personal data from a controller or processor in compliance with the requirements of this chapter shall not be deemed to be in violation of this chapter if the controller or processor from which the third-party controller or processor receives the personal data is in violation of this chapter.

(e) Nothing in this chapter shall be construed to:

(1) Impose an obligation on controllers and processors that adversely affects the rights or freedoms of any person, including the right of free expression pursuant to the First Amendment to the Constitution of the United States; or

(2) Apply to the processing of personal data by a person in the course of a purely personal or household activity.

(f) Personal data processed by a controller pursuant to this section shall not be processed for any purpose other than those expressly listed in this section unless otherwise allowed by this chapter. Personal data 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 data collected, used, or retained pursuant to subsection (b) where applicable, shall consider the nature and purpose or purposes of the collection, use, or retention. The data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to

consumers relating to the collection, use, or retention of personal data.

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

(h) An entity's processing of personal data for the purposes expressly identified in subsection (a) shall not be the sole basis for the department to consider the entity as a controller with respect to the processing.

§ -10 Investigative authority; civil investigative demand. (a) Whenever the department has reasonable cause to believe that any person has engaged in, is engaging in, or is about to engage in any violation of this chapter, the department may either require or permit the person to file with the department a statement in writing or otherwise, under oath, as to all facts and circumstances concerning the subject matter. The department may also require any other data and information as the department may deem relevant to the subject matter of an investigation of a possible violation of this chapter and may

make such special and independent investigations as the department may deem necessary in connection with the matter.

(b) In connection with the investigation, the department may issue a civil investigative demand to witnesses by which the department may:

(1) Compel the attendance of the witnesses;

(2) Examine the witnesses under oath before the department or a court of record;

(3) Subject to subsection (d), require the production of any books or papers that the department deems relevant or material to the inquiry; and

(4) Issue written interrogatories to be answered by the witness served or, if the witness served is a corporation, partnership, association, governmental agency, or any person other than a natural person, by any officer or agent, who shall furnish the information as is available to the witness.

The investigative powers of this subsection shall not abate or terminate by reason of any action or proceeding brought by the department under this chapter.

(c) When documentary material is demanded by a civil investigative demand, the demand shall not:

(1) Contain any requirement that would be unreasonable or improper if contained in a subpoena duces tecum issued by a court of the State; or

(2) Require the disclosure of any documentary material that would be privileged, or production of which for any other reason would not be required by a subpoena duces tecum issued by a court of the State.

(d) Where the information requested pursuant to a civil investigative demand may be derived or ascertained from the business records of the party upon whom the interrogatory has been served or from an examination, audit, or inspection of the business records, or from a compilation, abstract, or summary based therein, and the burden of deriving or ascertaining the answer is substantially the same for the department as for the party from whom the information is requested, it shall be sufficient for that party to specify the records from which the answer may be derived or ascertained and to afford the department, or other individuals properly designated by the department, reasonable opportunity to examine, audit, or inspect

the records and to make copies, compilations, abstracts, or summaries. Further, the department may elect to require the production pursuant to this section of documentary material before or after the taking of any testimony of the person summoned pursuant to a civil investigative demand, in which event, the documentary matter shall be made available for inspection and copying during normal business hours at the principal place of business of the person served, or at any other time and place, as may be agreed upon by the person served and the department.

(e) Any civil investigative demand issued by the department shall contain the following information:

(1) The statute alleged to have been violated and the subject matter of the investigation;

(2) The date, place, time, and locations at which the person is required to appear to produce documentary material in the person's possession, custody, or control; provided that the date shall not be less than twenty days after the date of the civil investigative demand; and

(3) If documentary material is required to be produced, it shall be described by class so as to clearly indicate the material demanded.

(f) Service of civil investigative demand of the department may be made by:

(1) Delivery of a duly executed copy to the person served, or if a person is not a natural person, to the principal place of business of the person to be served; or

(2) Mailing by certified mail, return receipt requested, of a duly executed copy addressed to the person to be served at the person's principal place of business in the State, or if the person has no place of business in the State, to the person's office.

(g) Within twenty days after the service of a demand upon any person or enterprise, or at any time before the return date specified in the demand, whichever period is shorter, the party may file in the circuit court and serve upon the attorney general a petition for an order modifying or setting aside the demand. The time allowed for compliance with the demand in whole or in part as deemed proper and ordered by the court shall

not run during the pendency of the petition in the court. The petition shall specify each ground upon which the petitioner relies in seeking relief and may be based upon any failure of the demand to comply with the provisions of this chapter or upon any constitutional or other legal right or privilege of the party. This subsection shall be the exclusive means for a witness summoned pursuant to a civil investigative demand pursuant to this section to challenge the civil investigative demand.

(h) The examination of all witnesses under this section shall be conducted by the attorney general, or the attorney general's designee, before a person authorized to administer oaths in the State. The testimony shall be taken stenographically or by a sound recording device and shall be transcribed.

(i) Any person required to testify or to submit documentary evidence shall be entitled, on payment of lawfully prescribed cost, to procure a copy of any document produced by the person and of the person's own testimony as stenographically reported or, in the case of depositions, as reduced to writing by or under the direction of a person taking the deposition.

Any party compelled to testify or to produce documentary evidence may be accompanied and advised by counsel, but counsel may not, as a matter of right, otherwise participate in the investigation.

(j) Any persons served with a civil investigative demand by the department under this chapter, other than any person whose conduct or practices are being investigated or any officer, director, or person in the employ of the person under investigation, shall be paid the same fees and mileage as paid witnesses in the courts of the State. No person shall be excused from attending an inquiry pursuant to the mandate of a civil investigative demand, or from producing a paper, or from being examined or required to answer questions on the ground of failure to tender or pay a witness fee or mileage unless demand is made at the time testimony is about to be taken and as a condition precedent to offering the production or testimony and unless payment is not made upon the demand.

(k) Any natural person who shall neglect or refuse to attend and testify, or to answer any lawful inquiry or to produce documentary evidence, if in the person's power to do so, in obedience of a civil investigative demand or lawful request

of the department or those properly authorized by the department, pursuant to this section, shall be guilty of a misdemeanor.

(l) Any natural person who commits perjury or false swearing or contempt in answering, failing to answer, producing evidence, or failing to produce evidence in accordance with a civil investigative demand or lawful request by the department, pursuant to this section, shall be guilty of a misdemeanor.

(m) In any investigation brought by the department pursuant to this chapter, no person shall be excused from attending, testifying, or producing documentary material, objects, or intangible things in obedience to a civil investigative demand or under order of the court on the ground that the testimony or evidence required of the person may tend to incriminate the person or subject the person to any penalty; provided that no testimony or other information compelled either by the department or under order of the court, or any information directly or indirectly derived from the testimony or other information, may be used against the individual or witness in any criminal case. A person may be prosecuted or subjected to penalty or forfeiture for any perjury, false swearing, or

contempt committed in answering, or failing to answer, or in producing evidence or failing to do so in accordance with the order of the department or the court. If a person refuses to testify or produce evidence after being granted immunity from prosecution and after being ordered to testify or produce evidence, the person may be adjudged in contempt by a court of pursuant to section 710-1077. This subsection shall not be construed to prevent the department from instituting other appropriate contempt proceedings against any person who violates this section.

(n) Any state or county public official, deputy, assistant, clerk, subordinate, or employees, and all other persons shall render and furnish to the department, when so requested, all information and assistance in the person's possession or within the person's power. Any officer participating in the inquiry and any person examined as a witness upon the inquiry who shall disclose to any person other than the department the name of any witness examined or any other information obtained upon the inquiry, except as so directed by the department, shall be guilty of a misdemeanor.

(o) The department shall maintain the secrecy of all evidence, testimony, documents, or other results of investigations; provided that:

(1) The department may disclose any investigative evidence to any federal or state law enforcement authority that has restrictions governing confidentiality similar to those contained in this subsection;

(2) The department may present and disclose any investigative evidence in any action or proceeding brought by the department under this chapter; and

(3) Any upon written authorization of the attorney general, an inquiry under this section may be made public.

Violation of this subsection shall be a misdemeanor.

§ -11 Enforcement; civil penalty; expenses. (a) The department shall have exclusive authority to enforce this chapter.

(b) Before initiating any action under this chapter, the department shall provide a controller or processor a thirty-day written notice that identifies the specific provisions of this chapter that the controller or processor has allegedly violated.

If, within the thirty-day period, the controller or processor cures the alleged violation and provides the department with an express written statement that the alleged violation has been cured and that no further violations shall occur, no action shall be initiated against the controller or processor.

(c) If a controller or processor continues to violate this chapter following the cure period in subsection (b) or breaches the express written statement provided to the department pursuant to subsection (b), the department may:

(1) Initiate an action in the name of the State;

(2) Seek an injunction to restrain any violations of this chapter; and

(3) Seek to impose civil penalties of up to $7,500 for each violation under this chapter.

(d) For any action initiated under this chapter, the department may recover reasonable expenses, including attorney fees, that the department incurred in the investigation and preparation of the case.

(e) Nothing in this chapter shall be construed as providing the basis for, or be subject to, a private right of action for violations of this chapter or under any other law.

§ -12 Consumer privacy special fund. (a) There is established in the state treasury the consumer privacy special fund into which shall be deposited:

(1) All civil penalties, expenses, and attorney fees collected pursuant to this chapter;

(2) Interest earned on money in the fund; and

(3) Appropriations made by the legislature.

(b) The fund shall be administered by the department. Moneys in the fund shall be used by the department to administer this chapter.

§ -13 Rules. The department shall adopt rules, pursuant to chapter 91, necessary for the purposes of this chapter."

SECTION 2. There is appropriated out of the general revenues of the State the sum of $ or so much thereof as may be necessary for fiscal year 2023-2024 and the same sum or so much thereof as may be necessary for fiscal year 2024-2025 to be deposited into the consumer privacy special fund.

SECTION 3. There is appropriated out of the consumer privacy special fund the sum of $ or so much thereof as may be necessary for fiscal year 2023-2024 and the same sum

or so much thereof as may be necessary for fiscal year 2024-2025 for consumer data protection.

The sums appropriated shall be expended by the department of the attorney general for the purposes of this Act.

SECTION 4. This Act does not affect rights and duties that matured, penalties that were incurred, and proceedings that were begun before its effective date.

SECTION 5. This Act shall take effect on July 1, 2023.

INTRODUCED BY: 

S.B. NO. 974

Report Title:
Consumers; Data; Privacy; Attorney General; Appropriations

Description:
Establishes a framework to regulate controllers and processors with access to personal consumer data. Establishes penalties. Establishes a new consumer privacy special fund. Appropriates moneys.

The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.