HOUSE BILL NO. 5989

April 12, 2022, Introduced by Reps. Anthony, Rogers, Sneller, Brenda Carter, Sowerby, Hope, Aiyash, Kuppa, Weiss, Stone, Steckloff, Hood, Haadsma, LaGrand and Breen and referred to the Committee on Communications and Technology.

A bill to establish the privacy rights of consumers; to require certain persons to provide certain notices to consumers regarding the processing and sale of personal data; to prohibit certain acts and practices concerning the processing and sale of personal data; to establish standards and practices regarding the processing and sale of personal data; to provide for the powers and duties of certain state governmental officers and entities; to create the consumer privacy fund; and to provide remedies.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

Sec. 1. This act may be cited as the "consumer privacy act".

Sec. 2. As used in this act:

(a) "Affiliate" means a person that controls, is controlled by, or is under common control with another person or shares common branding with another person. As used in this subdivision, "control" or "controlled" means any of the following:

(*i*) Ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a person.

(*ii*) Control in any manner over the election of a majority of the directors or of individuals exercising similar functions of a person.

(*iii*) The power to exercise controlling influence over the management of a person.

(b) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual. Biometric data does not include a physical or digital photograph, a video or audio recording or data generated from the video or audio recording, or information collected, used, or stored for health care treatment, payment, or operations under the health insurance portability and accountability act of 1996, Public Law 104-191.

(c) "Child" means an individual who is less than 18 years of age.

(d) "Consent" means a clear affirmative act signifying a consumer's, or, if the consumer is a child, the consumer's parent's or legal guardian's, freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a

statement written by electronic means, or any other unambiguous affirmative action.

(e) "Consumer" means an individual who is a resident of this state acting in an individual or household context. The term does not include an individual who is acting in a commercial or employment context.

(f) "Controller" means a person that, alone or jointly with others, determines the purpose and means of processing personal data.

(g) "Decisions that produce legal or similarly significant effects concerning a consumer" means decisions made by the controller that result 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, such as food and water.

(h) "Deidentified data" means data that cannot reasonably be linked to an identified or identifiable individual, or a device linked to the identified or identifiable individual.

(i) "Fund" means the consumer privacy fund created in section 15.

(j) "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly.

(k) "Person" means an individual, partnership, corporation, association, or other legal entity.

(*l*) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual. The term does not include publicly available data or deidentified data.

(m) "Precise geolocation data" 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 an individual with precision and accuracy within a radius of 1,750 feet. 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.

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

(o) "Processor" means a person that processes personal data on behalf of a controller.

(p) "Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to a consumer's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(q) "Sell", "selling", "sale", or "sold" means the exchange of personal data for monetary or other valuable consideration by a controller to a third party.

(r) "Sensitive data" means a category of personal data that includes all of the following:

(*i*) Personal data that reveal racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status.

(*ii*) The processing of genetic or biometric data for the purposes of providing a product or service requested by a consumer.

(*iii*) Personal data collected from a known child.

(*iv*) Precise geolocation data.

(s) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests. Targeted advertising does not include any of the following:

(*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.

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

(t) "Third party" means a person other than a consumer, controller, processor, or an affiliate of the processor or the controller.

Sec. 3. (1) A consumer has all of the following rights:

(a) To know what personal data are being collected about them.

(b) To know whether their personal data are sold or disclosed and to whom.

(c) To say no to any of the following:

(*i*) The sale of personal data.

(*ii*) The processing of personal data for purposes of targeted advertising.

(*iii*) The processing of personal data for purposes of profiling in furtherance of decisions that produce legal or similarly

significant effects concerning the consumer.

(d) To access the personal data that have been collected about them.

(e) To request that a business delete any personal data that were collected from that consumer or about that consumer.

(f) To request that a business correct any personal data about them that are inaccurate.

(g) To not be discriminated against for exercising the privacy rights described in this act.

(h) To obtain a copy of their personal data that they previously provided to a 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 hinderance, where the processing is carried out by automated means.

(2) A consumer may invoke their rights under this section 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 consumer rights under this section on behalf of the child.

Sec. 5. This act applies to a person to which both of the following apply:

(a) Conducts business in this state or produces products or services that are targeted to residents of this state.

(b) During a calendar year, either of the following applies:

(*i*) The person controls or processes personal data of not less than 100,000 consumers.

(*ii*) The person controls or processes personal data of not less than 25,000 consumers and derives over 50% of gross revenue from the sale of personal data.

Sec. 7. (1) Except as otherwise provided in this act, a controller shall comply with a consumer's request to exercise the consumer's rights under section 3. A controller shall do all of the following:

(a) Respond to a consumer within 45 days of receipt of a request submitted under section 3.

(b) If the controller declines to take action regarding a consumer's request under section 3, inform the consumer within 45 days of receipt of the request of the justification for declining to take action and instructions for how to appeal the decision under subsection (3).

(c) Provide information in response to a consumer request under section 3 free of charge, up to 2 times annually per consumer. If a request is 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 has the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of a request.

(2) If a controller is unable to authenticate a consumer request using commercially reasonable efforts, the controller is not required to comply with a request to initiate an action described under section 3 and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

(3) 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 under subsection (1). All of the following apply to the

appeal process under this subsection:

(a) The appeal process must be conspicuously available and similar to the process for submitting requests to initiate action under section 3.

(b) Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions.

(c) If the appeal is denied, the controller shall provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint.

Sec. 9. (1) A controller shall do all of the following:

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

(b) Except as otherwise provided in this chapter, not process personal data for purposes that are not reasonably necessary to or compatible with the disclosed purposes for which such personal data are processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

(c) Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices must be appropriate to the volume and nature of the personal data at issue.

(d) Obtain a consumer's consent to process sensitive data before processing the consumer's sensitive data.

(e) Subject to federal law, obtain consent to process a child's personal data before processing the child's personal data.

(2) Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes all of the following:

(a) The categories of personal data processed by the controller.

(b) The purpose for processing personal data.

(c) How consumers may exercise their consumer rights under this act, including how a consumer may appeal a controller's decision with regard to the consumer's request.

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

(e) The categories of third parties, if any, with whom the controller shares personal data.

(3) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose that it sells personal data to third parties or that it processes personal data for targeted advertising, as well as the manner in which a consumer may exercise the right to opt out of the sale or processing of personal data described in this subsection.

(4) A controller shall establish, and shall describe in a privacy notice, 1 or more secure and reliable means for consumers to submit a request to exercise their consumer rights under this act. Such means must take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such 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 to exercise consumer rights under this act but may require a consumer to use an existing account.

Sec. 11. (1) A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

(a) The processing of personal data for purposes of targeted advertising.

(b) The sale of personal data.

(c) The processing of personal data for purposes of profiling if the profiling presents a reasonably foreseeable risk of any of the following:

(*i*) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers.

(*ii*) Financial, physical, or reputational injury to consumers.

(*iii*) A physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, where the intrusion would be offensive to a reasonable person.

(*iv*) Other substantial injury to consumers.

(d) The processing of sensitive data.

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

(2) Data protection assessments conducted under subsection (1) must identify and weigh the benefits that may flow, directly and indirectly, from the processing or selling of personal data to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of a consumer associated with the processing or selling of person data, as mitigated by safeguards that can be employed by the controller to reduce the

risks. The use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and selling of personal data and the relationship between the controller and the consumer whose personal data will be processed or sold, must be factored into the data protection assessment by the controller.

(3) The attorney general may request that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general under section 13, and the controller shall make the data protection assessment available to the attorney general. The attorney general may evaluate the data protection assessment for compliance with the responsibilities set forth in section 9. Data protection assessments are exempt from disclosure under the freedom of information act, 1976 PA 442, MCL 15.231 to 15.246. The disclosure of a data protection assessment pursuant to a request from the attorney general does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

Sec. 13. (1) The attorney general has exclusive authority to enforce the provisions of this act.

(2) The attorney general may investigate on his or her own initiative any person that is subject to this act. Before initiating an action under this act, if the attorney general has reasonable cause to believe that a person subject to this act has engaged in, is engaging in, or is about to engage in a violation of this act, the attorney general may require the person or an officer, member, employee, or agent of the person to appear at a time and place specified by the attorney general to give information under oath and to produce books, memoranda, papers,

records, documents, or other relevant evidence in the possession or control of the person ordered to appear.

(3) When requiring the attendance of a person or the production of documents under subsection (2), the attorney general shall issue an order setting forth the time when and the place where attendance or production is required and shall serve the order on the person in the manner provided for service of process in civil cases at least 5 days before the date fixed for attendance or production. The order issued by the attorney general has the same force and effect as a subpoena. On application of the attorney general, the order issued by the attorney general may be enforced by a court having jurisdiction over the person, Ingham County circuit court, or the circuit court of the county where the person receiving the order resides or is found in the same manner as though the notice were a subpoena. If a person fails or refuses to obey the order issued by the attorney general under this subsection, the court may issue an order requiring the person to appear before the court, to produce documentary evidence, or to give testimony concerning the matter in question. Failure to obey the order of the court is punishable by that court as contempt.

(4) Before initiating an action under this act, the attorney general shall provide a controller or processor 30 days' written notice identifying the specific provisions of this act the attorney general alleges have been or are being violated. If within the 30-day period the controller or processor cures the noticed violation and provides the attorney general an express written statement that the alleged violations have been cured and that no further violations will occur, no action must be initiated against the controller or processor.

(5) If a controller or processor continues to violate this act following the cure period in subsection (4) or breaches an express written statement provided to the attorney general under subsection (4), the attorney general may initiate an action in the name of this state and may seek an injunction to restrain any violations of this act and civil fines of up to $7,500.00 for each violation of this act.

(6) The attorney general may recover reasonable expenses incurred in investigating and preparing an action under this section, including attorney fees.

(7) Nothing in this act provides the basis for, or is subject to, a private right of action for violations of this act or under any other law.

Sec. 15. (1) The consumer privacy fund is created within the state treasury.

(2) The state treasurer may receive money or other assets from any source for deposit into the fund. The state treasurer shall direct the investment of the fund. The state treasurer shall credit to the fund interest and earnings from fund investments.

(3) Money in the fund at the close of the fiscal year remains in the fund and does not lapse to the general fund.

(4) The department of attorney general is the administrator of the fund for auditing purposes.

(5) The department of attorney general shall expend money from the fund, upon appropriation, to enforce the provisions of this act.

(6) All civil fines, expenses, and attorney fees collected under this act must be paid into the fund.