Department of Legislative Services

Maryland General Assembly
2023 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 33 (Delegate Love, *et al.*)
Economic Matters

Commercial Law - Consumer Protection - Biometric Data Privacy

This bill generally requires each "private entity" in possession of "biometric data" to develop a publicly available written policy establishing a retention schedule and guidelines for permanently destroying the biometric data on the earliest of (1) the date on which the initial purpose for collecting or obtaining the biometric data has been satisfied; (2) within three years after the individual's last interaction with the private entity; or (3) within 30 days after the private entity receives a verified request to delete the data submitted by the individual (or the individual's representative). Absent a valid warrant or subpoena, each private entity in possession of biometric data must comply with the retention schedule and destruction guidelines. The bill establishes various other standards and requirements related to biometric data, including authorizing an individual to bring a civil action against a private entity that violates the bill's requirements. Violation of the bill is an unfair, abusive, or deceptive trade practice under the Maryland Consumer Protection Act (MCPA), subject to MCPA's civil and criminal penalty provisions.

Fiscal Summary

State Effect: The bill's imposition of existing penalty provisions does not have a material impact on State finances or operations. The Office of the Attorney General (OAG), Consumer Protection Division, can handle the bill's requirements with existing resources.

Local Effect: The bill's imposition of existing penalty provisions does not have a material impact on local government finances or operations.

Small Business Effect: Potential meaningful.

Analysis

Bill Summary: "Biometric data" means data generated by automatic measurements of the biological characteristics of an individual, such as a fingerprint, a voiceprint, an eye retina, an eye iris, or any other unique biological patterns or characteristics that is used to identify a specific individual. Biometric data does not include (1) a physical or digital photograph; (2) a video or audio recording; or (3) information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. A "private entity" is any individual, partnership, corporation, limited liability company, association, or other group, however organized; it does not include an entity (or an affiliate) subject to and in compliance with the federal Gramm-Leach-Bliley Act (*e.g.*, a financial institution such as a bank) or an entity acting only as a "processor" for another entity.

A "processor" is an entity that processes, stores, or otherwise uses biometric data on behalf of a private entity.

Private Entities and Processors – Duties and Prohibitions

Each private entity in possession of biometric data must store, transmit, and protect the biometric data from disclosure (1) using the reasonable standard of care within the private entity's industry and (2) in a manner that is as protective as (or more protective than) the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

Upon request of an individual (or an individual's legally authorized representative), a private entity that collects, uses, discloses, or rediscloses biometric data must disclose to the individual, free of charge, the biometric data and any information related to its use, as specified.

A private entity that collects biometric data is prohibited from selling, leasing, or trading an individual's biometric data. In addition, such entities may not collect, use, disclose, redisclose, or otherwise disseminate an individual's biometric data unless the individual (or the individual's legally authorized representative) provides consent or the disclosure or redisclosure is required (1) by a valid warrant or subpoena; (2) to comply with federal, State, or local laws, rules; or regulations; or (3) to cooperate with law enforcement, as specified.

A private entity may collect, use, disclose, redisclose, or otherwise disseminate an individual's biometric data without complying with the above requirements if the private entity does so for fraud prevention or security purposes and posts conspicuous written

notice of the collection at each point of entry, as specified. This authorization may only be used if it is directly tied to the services being provided by the private entity.

The bill prohibits a private entity from conditioning the provision of a service on the collection, use, disclosure, transfer, sale, or processing of biometric data unless the data is strictly necessary to provide the service. Additionally, the bill prohibits a private entity from charging different prices (or rates) for goods or services or providing a different level or quality of a good or service to any individual who exercises the individual's rights under the bill.

A private entity that contracts with a processor to process (or store) biometric data is prohibited from allowing the processor to collect, store, process, use, disclose, or take any action for monetary consideration on (or with) the biometric data except for purposes for which the entity received consent. The bill also expressly prohibits a processor from taking such actions, except as authorized by a contract with a private entity that legally possesses the data.

A private entity is not required to make publicly available a written policy required by the bill if the policy (1) applies only to the employees of the private entity and (2) is used solely for internal company operations.

Current Law: The Maryland Personal Information Protection Act (MPIPA) defines "personal information" as, among other things, biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account in combination with an individual's first name or first initial and last name, when the name or data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable.

MPIPA imposes certain duties on a business to protect an individual's personal information. A business in possession of personal information must implement and maintain reasonable security procedures and practices to protect the information from unauthorized access, use, modification, or disclosure. If a data breach occurs, the business must conduct, in good faith, a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been (or will be) misused. If the business determines that personal information likely has been (or will be) misused, the owner or licensee of the computerized data must notify an affected individual as soon as practicable, but not later than 45 days after the business discovers or is notified of the breach. For a business that only maintains personal data, the business must notify the owner or licensee of the breach as soon as practicable but not later than 10 days after the business

discovers or is notified of the breach. Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security.

When a breach occurs, a business must also provide notice to OAG that includes (1) the number of Maryland residents affected by the breach; (2) a description of the breach, including when and how the breach occurred; (3) any steps the business has taken or plans to take relating to the breach; and (4) the form of notice and a sample of the notice that will be sent to individuals affected by the breach. The Act also establishes a specific notification process for breaches involving email account information.

Violation of MPIPA is an unfair, abusive, or deceptive trade practice under MCPA, subject to MCPA's civil and criminal penalty provisions.

Maryland Consumer Protection Act

An unfair, abusive, or deceptive trade practice under MCPA includes, among other acts, any false, falsely disparaging, or misleading oral or written statement, visual description, or other representation of any kind which has the capacity, tendency, or effect of deceiving or misleading consumers. The prohibition against engaging in any unfair, abusive, or deceptive trade practice encompasses the offer for or actual sale, lease, rental, loan, or bailment of any consumer goods, consumer realty, or consumer services; the extension of consumer credit; the collection of consumer debt; or the offer for or actual purchase of consumer goods or consumer realty from a consumer by a merchant whose business includes paying off consumer debt in connection with the purchase of any consumer goods or consumer realty from a consumer.

The Consumer Protection Division is responsible for enforcing MCPA and investigating the complaints of aggrieved consumers. The division may attempt to conciliate the matter, issue a cease and desist order, or file a civil action in court. A merchant who violates MCPA is subject to a fine of up to $10,000 for each violation and up to $25,000 for each repetition of the same violation. In addition to any civil penalties that may be imposed, any person who violates MCPA is guilty of a misdemeanor and, on conviction, is subject to a fine of up to $1,000 and/or imprisonment for up to one year.

Small Business Effect: Any small businesses in the State that handle biometric data may need to develop a written policy establishing a retention schedule and guidelines for permanently destroying biometric data within the time period required by the bill (to the extent that such businesses have not already developed such policies and procedures). The bill also prohibits private entities (including processors) from selling, leasing, trading, or otherwise profiting from an individual's biometric data, which may significantly impact any small businesses that currently engage in such activities.

Additional Information

Prior Introductions: Similar legislation has been introduced within the last three years. See SB 335 and HB 259 of 2022; SB 16 and HB 218 of 2021; and HB 307 of 2020.

Designated Cross File: SB 169 (Senator Feldman, *et al.*) - Finance.

Information Source(s): Judiciary (Administrative Office of the Courts); Department of Legislative Services

Fiscal Note History: First Reader - February 7, 2023
js/jkb

Analysis by: Eric F. Pierce

Direct Inquiries to:
(410) 946-5510
(301) 970-5510