HB 259

Department of Legislative Services

Maryland General Assembly
2022 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

House Bill 259 (Delegate Love, *et al.*)
Economic Matters Finance

Commercial Law - Consumer Protection - Biometric Data Privacy

This bill generally establishes various standards and requirements related to "biometric data," including (1) requiring 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, as specified; (2) prohibiting a private entity that collects biometric data from selling, leasing, or trading an individual's biometric data; and (3) authorizing an individual to bring a civil action against a private entity that violates specified requirements of the bill. Violation of the bill is an unfair, abusive, or deceptive trade practice under the Maryland Consumer Protection Act (MCPA), generally 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, 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:

Select Definitions

"Biometric data" means data generated by automatic measurements of the biological characteristics of an individual (such as a fingerprint, a voiceprint, an eye retina or iris, or

any other unique biological patterns or characteristics) that is used to identify a specific individual. 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 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

In general, each private entity in possession of biometric data must 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.

A private entity in possession of biometric data for fraud prevention or security purposes is not required to delete an individual's biometric data in accordance with the above provisions if the individual is part of the State Voluntary Exclusion Program.

Further, 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.

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 that the private entity stores, transmits, and protects other confidential and sensitive information.

A private entity that collects biometric data is prohibited from selling, leasing, or trading an individual's biometric data. 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 biometric data.

Generally, private 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) gives consent or the disclosure or redisclosure is required:

- by a valid warrant or subpoena;
- to comply with federal, State, or local laws, rules, or regulations; or
- to cooperate with law enforcement concerning conduct or activity that the private entity or processor reasonably (and in good faith) believes violates federal, State, or local laws, rules, or regulations.

A private entity *may* collect, use, disclose, redisclose, or otherwise disseminate an individual's biometric data if the private entity (1) collects, uses, discloses, rediscloses, or otherwise disseminates the biometric data for fraud prevention or security purposes and (2) posts conspicuous written notice of the data collection at each point of entry, as specified. The collection, use, disclosure, redisclosure, or other dissemination must be directly tied to the services being provided by the private entity. Additionally, the private entity may collect, use, disclose, redisclose, or otherwise disseminate only what is strictly necessary for fraud prevention and security purposes.

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, free of charge, the biometric data and any information related to its use to the individual, as specified. A private entity may not be required to provide an individual (or the individual's authorized representative) with the required information more than twice during any consecutive 12-month period.

Civil Actions

An individual who is affected by the bill's prohibition against selling, leasing, or trading an individual's biometric data is authorized to bring an action against a private entity in accordance with provisions in MCPA.

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.

Under MPIPA, when a business is destroying a customer's, employee's, or former employee's records containing personal information, the business must take reasonable steps to protect against unauthorized access to or use of the personal information, taking specified considerations into account.

To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of a Maryland resident must implement and maintain reasonable and appropriate security procedures and practices. A business that uses a nonaffiliated third party as a service provider and discloses personal information about a Maryland resident under a written contract with the third party must require, by contract, that the third party implement and maintain reasonable security procedures and practices that are (1) appropriate to the nature of the disclosed information and (2) reasonably designed to help protect the information from unauthorized access, use, modification, disclosure, or destruction. This provision applies to a written contract that is entered into on or after January 1, 2009.

A business that owns, licenses, or maintains computerized data that includes personal information of a Maryland resident, upon the discovery or notification of a breach of the security of a system, must conduct, in good faith, a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused as a result of the breach. If, after the investigation, the business reasonably believes that the breach has resulted or will result in the misuse of personal information of a Maryland resident, the owner or licensee of the data must notify the individual of the breach. Generally, the notice to the individual must be given as soon as reasonably practicable (but no later than 45 days after the business conducts the required investigation). If the business determines that notification is not required, the business must maintain the records related to the determination for three years.

A business that maintains computerized data that includes personal information that it does not own or license must notify the owner or licensee of the personal information of a breach and share information relevant to the breach as soon as reasonably practicable (but no later than 45 days) after the business discovers or is notified of the breach. Such a third-party business may not charge a fee for providing the information needed for the required notification to the owner or licensee of the data. Moreover, the owner or licensee may not use information relative to the breach for purposes other than (1) providing notification of

the breach; (2) protecting or securing personal information; or (3) providing notification to national information security organizations created for information sharing and analysis of security threats, to alert and avert new or expanded breaches.

Required notifications may be delayed (1) if a law enforcement agency determines that it will impede a criminal investigation or jeopardize homeland or national security or (2) to determine the scope of the breach, identify the individuals affected, or restore the system's integrity.

Consumer notification must include a description of categories of information acquired by the unauthorized user, the business' contact information, and contact information for the major consumer reporting agencies and specified government agencies. The notification may be given by mail or telephone; electronic mail or other forms of notice may be used if specified conditions are met. Prior to consumer notification, a business must notify the Office of the Attorney General of the breach after it discovers or is notified of the breach.

In the case of a breach of a security system involving an individual's email account – but no other specified personal information – the business may comply with the required notification in electronic or other form. The notification must direct the individual whose personal information has been breached to promptly (1) change the individual's password and security question or answer, as applicable, or (2) take other appropriate steps to protect the email account, as well as all other online accounts for which the individual uses the same user name or email and password (or security question or answer). Generally, the required notification may be given to the individual by any method described in § 14-3504 of the Commercial Law Article. However, the required notification may not be given by sending notification by email to the affected account. The notification *may*, however, be given by a clear and conspicuous notice delivered to the individual online while the individual is connected to the affected email account from an Internet protocol address or online location from which the business knows the individual customarily accesses the account.

A waiver of the notification requirements is void and unenforceable. Compliance with the notification requirements does not relieve a business from a duty to comply with any federal legal requirements relating to the protection and privacy of personal 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, or trading an individual's biometric identifiers, which may significantly impact any small businesses that currently engage in such activities.

Additional Information

Prior Introductions: HB 218 of 2021, a similar bill, was heard in the House Economic Matters Committee but subsequently withdrawn. Its cross file, SB 16, received a hearing in the Senate Finance Committee, but no further action was taken. HB 307 of 2020, a similar bill as amended in the House, was heard in the Senate Finance Committee, but no further action was taken.

Designated Cross File: SB 335 (Senator Feldman, *et al.*) - Finance.

Information Source(s): Office of the Attorney General (Consumer Protection Division); Judiciary (Administrative Office of the Courts); Department of Legislative Services

Fiscal Note History: First Reader - January 31, 2022
fnu2/jkb Third Reader - April 6, 2022
Revised - Amendment(s) - April 6, 2022

Analysis by: Eric F. Pierce

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