HB 1389

Department of Legislative Services

Maryland General Assembly
2020 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 1389 (Delegate Love)
Economic Matters

Maryland Personal Information Protection Act – Geolocation Information and Unfair, Abusive, and Deceptive Trade Practices

This bill prohibits a business from collecting, using, storing, or disclosing "geolocation information" from a "location-based application" on a mobile device of an individual unless the business complies with certain disclosure requirements and obtains affirmative consent from a consumer beforehand. 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. The bill applies only prospectively and may not be applied or interpreted to have any effect on (or application to) any location-based applications that were created or modified before the bill's effective date.

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: The bill defines "geolocation information" as information that is (1) generated by (or derived from), in whole or in part, the operation of a mobile device including a smart phone, tablet, or laptop computer; (2) sufficient to determine (or infer)

the precise location of the mobile device; and (3) not the contents of a communication. "Geolocation information" does not include an Internet protocol (IP) address.

"Location-based application" means a software application that is downloaded or installed onto a mobile device and collects, uses, or stores geolocation information.

The bill authorizes a business to collect, use, store, or disclose geolocation information from a location-based application on a mobile device of an individual if, prior to engaging in such activities, the business:

- clearly and conspicuously informs the individual that geolocation information will be collected, used, stored, or disclosed;
- clearly and conspicuously informs the individual in writing of the specific purposes for which the geolocation information will be collected, used, stored, or disclosed; and
- obtains express affirmative consent to collect, use, store, or disclose the individual's geolocation information.

In addition, a business may collect, use, store, or disclose geolocation information from a location-based application on a mobile device without receiving affirmative express consent from the individual if such activities are:

- for the purpose of allowing a parent or legal guardian to locate an unemancipated minor child;
- for the purpose of allowing a court-appointed guardian to locate a legally incapacitated person;
- for the purpose of providing fire, medical, public safety, or other emergency service; or
- for the limited purpose of providing storage, security, or authentication services.

In the event that previously agreed-to terms are materially changed, a business must again obtain affirmative express consent from an individual.

If, after an investigation is conducted pursuant to MCPA, OAG finds that a business has violated the bill's requirements, OAG must notify the business of the violation and the business must remedy the violation within 15 days of being notified. If the business fails to remedy the violation within that period, OAG may then take further action.

Current Law:

Maryland Personal Information Protection Act

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 business must notify the individual of the breach. Generally, the notice 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 OAG 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 IP 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.

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: Many small businesses operate applications that use geolocation information. To the extent that any such businesses are not already in compliance with the disclosure and consent requirements specified by the bill, additional costs may be incurred.

Additional Information

Prior Introductions: None.

Designated Cross File: None.

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

Fiscal Note History: First Reader - February 25, 2020
mr/ljm

Analysis by: Eric F. Pierce

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