Department of Legislative Services

Maryland General Assembly
2020 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 957 (Senator Lee, *et al.*)
Finance

Maryland Online Consumer Protection Act

This bill establishes numerous personal information privacy rights for consumers in the State. Specifically, the bill establishes for consumers the right to (1) know whether (and what) personal information is collected or disclosed by a business; (2) access (and obtain a copy of) personal information collected by a business; (3) have personal information deleted by a business; (4) stop a business from disclosing information to third parties; and (5) equal service and pricing, regardless of whether the consumer has exercised his or her rights under the bill. 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 takes effect January 1, 2021.**

Fiscal Summary

State Effect: The bill's imposition of existing enforcement and penalty provisions is not expected to have a material impact on State finances or operations, although penalty revenues may increase minimally. The Office of the Attorney General (OAG), Consumer Protection Division, can likely handle additional enforcement and the bill's other 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:

Applicability Provisions

The bill applies to any for-profit business that collects the personal information of an individual or consumer and satisfies one or more of the following thresholds:

- has annual gross revenues of more than $25 million;
- annually buys, receives (for commercial purposes), sells, or shares (for commercial purposes), alone or in combination, the personal information of 100,000 or more consumers, households, or devices; or
- derives at least one-half of its annual revenues from selling consumers' personal information.

For purposes of the bill, "business" means a sole proprietorship, partnership, limited liability corporation, corporation, association, or any other legal entity operated for-profit or the financial benefit of its owners.

The bill also applies to any entity that (1) controls (or is controlled by) a business subject to the bill's requirements and (2) shares a name, service mark, or trademark with the business.

The bill defines "personal information" as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked (directly or indirectly) with a particular consumer or the consumer's device. "Personal information" does not include (1) publicly available information that is lawfully made available from government records; (2) de-identified consumer information; or (3) aggregate consumer information.

Required Disclosures

The bill requires a business that collects a consumer's personal information to clearly and conspicuously notify a consumer (at or before the point of collection) of (1) the categories of personal information the business will collect; (2) the business purposes for which the categories of personal information may be used; (3) the categories of third parties to which the business discloses personal information; and (4) the business purposes for third-party disclosure, as specified.

In addition, the business must notify a consumer of his or her right to request (1) a copy of the consumer's personal information; (2) deletion of the consumer's personal information; and (3) to opt out of third-party disclosure.

Right to Request a Copy of Personal Information

The bill allows a consumer to request that a business that collects a consumer's personal information disclose:

- the specific personal information the business has collected about that consumer;
- the sources from which the consumer's personal information was collected;
- the names of third parties to which the business disclosed the consumer's personal information; and
- the business purposes for third-party disclosure.

A business that receives a verifiable consumer request must promptly take steps to provide (free of charge) the required information. The bill specifies the manner in which the information may be provided and establishes that a business may only be required to provide personal information to the same consumer once in a six-month period. If requests from a consumer are excessive, a business may either charge a reasonable fee or refuse to act on the request and notify the consumer of the reason for refusing the request. A business is prohibited from requiring a consumer to create an account with the business in order to make a request.

Access to Personal Information

The bill requires a business to make available to consumers two or more designated methods for submitting requests, including (if the business maintains a website) a link on the homepage of the website. A business must also provide a toll-free telephone number for such requests (unless the business maintains a direct relationship with the consumer).

Generally, within 45 days of receiving a verifiable consumer request for a copy of personal information, a business must deliver (free of charge) the required information in a readily useable format that allows the consumer to transmit the information from one entity to another entity without hindrance.

If applicable, the bill requires a business to include specified information in its online privacy policy or, if the business does not have an online privacy policy but does have a business website, on its business website. The information must be updated once every 12 months. A business must ensure that an individual responsible for handling consumer inquiries regarding privacy practices is informed of the bill's requirements and how to direct consumers to exercise their rights.

Right to Delete Personal Information

The bill allows a consumer to request that a business delete all personal information about the consumer that the business has collected. If a business receives such a request, the business must delete the consumer's personal information from its records and direct service providers to delete the personal information as well. The bill also identifies the instances in which a business or service provider is not required to comply with a request to delete a consumer's personal information.

Right to Request Information Not Be Sold to Third Parties

The bill allows a consumer to demand that a business not disclose the consumer's personal information to third parties. (However, in no circumstances may a business disclose the personal information of a consumer to a third party if the business has actual knowledge or willfully disregards that the consumer is younger than age 16.) A business that receives this direction from a consumer may not disclose the consumer's personal information to third parties unless the consumer later provides express authorization. In addition, a business may not subsequently request authorization to disclose the consumer's personal information to third parties for at least 12 months.

A business must provide a clear and conspicuous link on the homepage of the business to an Internet webpage that enables a consumer (or an authorized person) to opt out of the third-party disclosure of the consumer's personal information. Although a business may require authentication for a request made pursuant to these provisions, the business may not require a consumer to create an account in order to exercise this right.

Right to Receive Equal Service

The bill prohibits discrimination against a consumer based on the consumer's decision to exercise his or her rights under the bill. For these purposes, discrimination includes:

- denying goods or services to the consumer;
- charging different prices or rates for goods or services (including through the use of discounts or other benefits, or imposing penalties);
- providing a different level or quality of goods or services to the consumer; or
- suggesting that the consumer will receive a different price or rate for goods or services (or a different level or quality of goods or services).

Exceptions to the Bill's Requirements

The bill's requirements may not restrict the ability of any business or third party to (1) comply with federal, state, or local laws; (2) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, or local authority; (3) cooperate with a law enforcement agency concerning conduct or activity that the business, service provider, or third party reasonably (and in good faith) believes may violate federal, state, or local law; (4) exercise legal rights or privileges; or (5) engage in news-gathering activities protected by the First Amendment.

The bill also identifies other instances in which its requirements do not apply and specifies the manner in which research with personal information may be used.

Office of the Attorney General

The bill authorizes OAG to adopt regulations as specified to carry out the bill's requirements. Regulations may include, among other things, provisions for updating unique identifiers, facilitating submission of verifiable consumer requests, establishing consumer notification standards, and establishing necessary exceptions to comply with federal and State laws.

Other Legal/Contractual Provisions

The bill specifies that, wherever possible, law relating to consumers' personal information should be construed to harmonize with the provisions of the bill. However, in the event of a conflict between other laws and the bill, the provisions of the law that afford the greatest protection for the right of privacy for consumers must control.

If a series of steps (or transactions) where component parts of a single transaction are taken with the intent of avoiding the requirements of the bill, a court must disregard the intermediate steps or transactions for purposes of the carrying out the bill.

A provision of a contract (or an agreement of any kind) that purports to waive or limit in any way a consumer's rights under the bill (including a remedy or means of enforcement) is considered contrary to public policy and is void and unenforceable.

Current Law/Background:

Internet Privacy

State law does not generally regulate Internet privacy. However, businesses are required under the Maryland Personal Information Protection Act to take precautions to secure the personal information of customers and to provide notice of breaches.

In addition, the Social Security Number Privacy Act (Chapter 521 of 2005) prohibits specified disclosures of an individual's Social Security number (SSN). However, the law exempts entities that provide Internet access (including "interactive computer service providers" and telecommunications providers) under specified circumstances. More specifically, the law does not apply to an interactive computer service provider's or a telecommunication's provider's *transmission or routing of* (or intermediate temporary storage or caching of) an individual's SSN. In addition, the law does not impose a duty on an interactive computer service provider or a telecommunications provider to monitor its service or to seek evidence of the transmission of SSNs on its service.

Federal Actions Regarding Internet Privacy

In 2016, the Federal Communications Commission (FCC) adopted rules that required broadband Internet service providers (ISPs) to protect the privacy of their customers. According to FCC, the rules established a framework of customer consent required for ISPs to use, sell, and share their customers' personal information. The rules separated the use and sharing of information into three categories and included guidance for both ISPs and customers about the transparency, choice, and security requirements for customers' personal information.

- *Opt In:* For certain sensitive information, ISPs would have been required to obtain affirmative "opt-in" consent from consumers to use and share the information. The rules specified categories of information considered sensitive, including precise geo-location, financial information, health information, children's information, SSNs, web browsing history, app usage history, and the content of communications.
- *Opt Out:* ISPs would have been allowed to use and share other, nonsensitive, information unless the customer "opted out." For example, email address information would have been considered nonsensitive information, and the use and sharing of that information would have been subject to opt-out consent.
- *Exceptions to Consent Requirements:* Customer consent was inferred for certain specified purposes, including the provision of broadband service or billing and collection. For the use of this information, no additional consent would have been required beyond the creation of the customer-ISP relationship.

The rules established other provisions, including:

- transparency requirements for ISPs to provide customers with clear, conspicuous, and persistent notice about the information collected, how it was to be used, and with whom it could have been shared, as well as how customers could change their privacy preferences;
- a requirement that broadband providers engage in reasonable data security practices and guidelines on steps ISPs should consider taking, such as implementing relevant industry best practices, providing appropriate oversight of security practices, implementing robust customer authentication tools, and proper disposal of data; and
- data breach notification requirements to encourage ISPs to protect the confidentiality of customer data and to give consumers and law enforcement notice of failures to protect such information.

The scope of the rules was limited to broadband service providers and other telecommunications carriers. The rules did not apply to the privacy practices of websites and other services over which the Federal Trade Commission, rather than FCC, has authority. In addition, the scope of the rules did not include other services of a broadband provider, such as the operation of a social media website, nor did the rules cover issues such as government surveillance, encryption, or law enforcement.

The rules were originally scheduled to take effect in 2017. However, in early 2017, the U.S. Congress approved a resolution of disapproval nullifying the FCC rule. The President signed the resolution on April 3, 2017.

California Online Privacy Law

The bill is similar to a California law that was enacted in 2018 (the California Consumer Privacy Act of 2018, or CCPA). Among other things, that law establishes that a consumer has the right to request that a business disclose categories and specific pieces of personal information the business has collected about the consumer. Consumers may request that a business delete any personal information that the business has collected about them. In addition, consumers may direct a business not to sell their personal information. The law also prohibits discrimination against a consumer because the consumer exercised his or her rights under the law. CCPA was amended in 2019; the bill also incorporates many of those 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 in OAG 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: The bill establishes numerous requirements for businesses that handle consumer personal information. To the extent that any small businesses meet the bill's thresholds, such businesses are likely to be meaningfully affected. The Department of Legislative Services advises that the exact number of small businesses that may be affected cannot be determined due to insufficient data. However, any small businesses that do meet the bill's criteria as a "business" must comply with the bill's personal information protection requirements and may incur significant costs to do so.

Additional Information

Prior Introductions: SB 613 of 2019, a similar bill, received a hearing in the Senate Finance Committee, but no further action was taken. Its cross file, HB 901, received a hearing in the House Economic Matters Committee, but no further action was taken.

Designated Cross File: HB 784 (Delegates Carey and C. Watson) - Economic Matters.

Information Source(s): Judiciary (Administrative Office of the Courts); California State Legislature; *New York Times*; Department of Legislative Services

Fiscal Note History: First Reader - February 18, 2020
mr/ljm

Analysis by: Eric F. Pierce

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