Department of Legislative Services

Maryland General Assembly
2017 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

Senate Bill 1200 (Senator Rosapepe, *et al.*)

Finance Economic Matters

Internet Consumer Privacy Rights Act of 2017

This bill prohibits an Internet service provider (ISP) from selling or transferring (for marketing purposes) a consumer's personally identifying information to a person without the consumer's express and affirmative permission. Likewise, an ISP may not send or display to a consumer an advertisement that has been selected to be sent or displayed (directly and exclusively by the ISP) because of the consumer's browsing history without the consumer's express and affirmative permission. An ISP may not refuse to provide its services to a consumer because of the consumer's refusal to provide the express and affirmative permission as specified under the bill. Violation of the bill is an unfair and deceptive trade practice under the Maryland Consumer Protection Act (MCPA), subject to MCPA's civil and criminal penalty provisions, except for provisions that allow a private right of action.

Fiscal Summary

State Effect: The bill's imposition of existing penalty provisions does not have a material impact on State finances or operations. If the Consumer Protection Division of the Office of the Attorney General receives fewer than 50 complaints per year stemming from the bill, the additional workload can be handled 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: Minimal.

Analysis

Bill Summary:

Exemptions from the Provisions

The bill does not apply to an ISP that transmits a consumer's personally identifying information (1) in response to a subpoena, summons, warrant, or court order that appears on its face to have been issued in accordance with lawful authority; (2) to the consumer to whom the information pertains; or (3) to provide the underlying Internet service. If a federal law, regulation, or rule that prohibits an ISP from engaging in the same conduct prohibited by the bill takes effect, the bill terminates.

Monitoring of Implementation by the Joint Committee on Cybersecurity, Information Technology, and Biotechnology

The Joint Committee on Cybersecurity, Information Technology, and Biotechnology must (1) monitor the enforcement of the bill and its impact on consumers, ISPs, and other businesses in the State and (2) include its findings and any recommended changes that are needed in its annual report that is due by December 1, 2018.

Monitoring Federal Actions Related to Consumer Privacy and Internet Service Providers

The Attorney General must monitor federal actions regarding the adoption and enactment of laws, regulations, and rules relating to the conduct of ISPs. If a federal law, regulation, or rule is adopted and enacted, the Attorney General must notify (and provide a copy to) the Department of Legislative Services.

Definitions

The bill defines "browsing history" as information that shows that a consumer has accessed a specific website. An "Internet service provider" is a person that provides access to the Internet.

"Personally identifying information" means the following information relating to a consumer using an ISP to access the Internet:

- the consumer's name;
- the consumer's Social Security number (SSN);
- the consumer's address;

- the Internet protocol address associated with an electronic device that belongs to the consumer; or
- the consumer's browsing history.

Current Law/Background: State law does not generally regulate the sale, sharing, or transfer of personally identifying information by ISPs. 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 information of breaches.

In addition, the Social Security Number Privacy Act (Chapter 521 of 2005) prohibits specified disclosures of an individual's 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.

2016 Federal Communications Commission Rules on Internet Privacy and 2017 Repeal

In 2016, the Federal Communications Commission (FCC) adopted rules that required broadband 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.

Regulation of Internet Privacy in Other States

According to a March 2017 *New York Times* article, as a result of federal actions related to the repeal of FCC privacy rules, some state legislatures have considered their own laws related to consumer privacy. For example, Illinois has considered several bills related to privacy rights, including a "right to know" bill that would provide information to consumers about how information collected by companies such as Google and Facebook is shared with other businesses. The article also notes that several other states have recently updated or enacted new laws related to online privacy.

Unfair or Deceptive Trade Practices under the Maryland Consumer Protection Act

An unfair 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 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 $1,000 for the first violation and up to $5,000 for each subsequent 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.

In addition to any action by the Consumer Protection Division or the Attorney General, any person may bring an action to recover for injury or loss sustained as a result of an alleged unfair or deceptive trade practice. A person who is awarded damages may also seek reasonable attorney's fees, which may be awarded by the court. If the court rules that a suit brought under this provision is frivolous, the court may order the offending party to pay the reasonable attorney's fees of the other party.

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Office of Attorney General; Judiciary (Administrative Office of the Courts); Public Service Commission; Federal Communications Commission; Congress.gov; *New York Times*; Department of Legislative Services

Fiscal Note History: First Reader - April 5, 2017
md/kdm Third Reader - April 10, 2017
Revised - Amendment(s) - April 10, 2017

Analysis by: Eric Pierce

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