

Department of Legislative Services  
Maryland General Assembly  
2018 Session

FISCAL AND POLICY NOTE  
Third Reader - Revised

House Bill 1654  
Economic Matters

(Delegate Frick, *et al.*)

Rules

---

Commercial Law - Internet Privacy and Net Neutrality

---

This bill establishes requirements related to Internet privacy in the State, including (1) the use, disclosure, sale, or provision of consumer data; (2) the protection of consumer data; and (3) enforcement of the bill's requirements by the Consumer Protection Division in the Office of the Attorney General. The bill also prohibits the use of State funds to procure services from an Internet service provider (ISP) that blocks specified content, impairs or degrades lawful Internet traffic, or engages in commercial traffic preferencing, as specified by the bill. **The bill takes effect June 1, 2018.**

---

Fiscal Summary

**State Effect:** The bill does not materially affect State finances or operations.

**Local Effect:** The bill does not materially affect local government finances or operations.

**Small Business Effect:** Minimal.

---

Analysis

**Bill Summary:** The bill expresses the intent of the General Assembly that, if the State or a municipality provides broadband Internet access services (BIAS), the State or the municipality may not impose restrictions prohibiting the exercise of free speech.

*Internet Privacy*

A "BIAS" is a mass-market retail service by wire or radio that provides the capability to transmit data to (and receive data from) all or substantially all Internet endpoints.

The bill prohibits a BIAS provider from using, disclosing, selling, or providing access to customer personal information unless the provider obtains opt-in consent that the customer has not revoked. To obtain opt-in consent, a provider must develop a mechanism that meets requirements specified by the bill.

A customer's decision remains in effect until the customer alters his or her decision. A BIAS provider may not (1) refuse to serve a customer who does not provide this consent or (2) charge a customer a different price based on whether he or she has provided consent.

### *Exceptions*

The bill specifies certain circumstances in which a BIAS provider *may* use, disclose, sell, or provide access to customer personal information without opt-in consent. Those circumstances include (1) use of information derived from or necessary for the provision of BIAS; (2) compliance with legal processes or laws, court orders, or administrative orders; (3) billing or collection of payments; (4) protection from fraudulent, abusive, or unlawful use of (or subscription to) the BIAS provider's network; and (5) location information related to emergency services.

In addition, a BIAS provider is generally authorized to use, disclose, sell, or provide access to personal information in order to advertise or market communications-related services to the customer. A BIAS provider must also disclose customer personal information to a customer or any person designated by the customer, upon written request of the customer.

### *Protection of Data*

The bill requires a BIAS provider to implement reasonable measures (based on an assessment of specified criteria) to protect customer personal information from unauthorized use, disclosure, sale, access, destruction, or modification. In addition, the bill generally prohibits a BIAS provider from retaining customer personal information for longer than reasonably necessary. A BIAS provider may retain customer personal information longer than reasonably necessary to comply with provisions in the bill or when the data is part of an aggregate personal information dataset.

### *Notification Requirements*

A BIAS provider must provide a customer notice of the bill's requirements that is (1) in the language that the BIAS provider primarily uses to conduct business with the customer and (2) continuously available through all methods that the BIAS provider uses to manage accounts.

### *Use of Aggregate Data*

The bill does not restrict a BIAS provider from (1) generating an aggregate customer personal information dataset using personal information or (2) using, disclosing, selling, or authorizing access to that dataset.

### *Waiving of Rights*

A term in a contract that purports to waive the rights established by the bill is void and unenforceable.

### *State Procurement – Net Neutrality*

The bill defines “reasonable network management” to mean a practice that primarily is used for and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband Internet access service. It does not include other business practices.

A State agency may not procure services from an ISP that:

- blocks lawful content, applications, services, or nonharmful devices, subject to reasonable network management;
- impairs or degrades lawful Internet traffic on the basis of Internet content, application, or service, or use of a nonharmful device, subject to reasonable network management; or
- engages in commercial traffic preferencing, including specified actions, either in exchange for consideration from a third party or to benefit an affiliated entity.

### **Current Law:**

#### *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 information 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.

### *State Procurement – Net Neutrality*

State law does not restrict the use of State funds to procure Internet services.

## **Background:**

### *Internet Privacy*

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 the National Conference of State Legislatures, about half the states have introduced measures in response to the repeal of federal Internet privacy protections. As of late 2017, two states – Nevada and Minnesota – require ISPs to keep certain information private unless given permission by the customer to disclose the information.

#### *Net Neutrality*

In December 2017, FCC approved a repeal of existing “net neutrality” regulations that had been in place for two years and that barred ISPs from restricting Internet traffic on their services. FCC also reclassified broadband Internet service as an “information service” rather than a “telecommunications service,” thereby limiting FCC’s authority to regulate broadband service in the future. The order included a preemption clause that prevents states from adopting their own net neutrality rules, although some states dispute whether the preemption clause is valid. The repeal is scheduled to take effect April 23, 2018.

With the repeal of the net neutrality rules, ISPs can slow down or block access to some websites. They can also accept fees from companies to make their content load faster than other sites.

According to *Consumer Reports*, 26 states have introduced legislation to mitigate the effects of the repeal of net neutrality, and several governors have signed executive orders to enact their own net neutrality rules. As of April 4, 2018, Washington is the only state to successfully enact net neutrality legislation. The executive orders that have been signed in several states generally use the power of state contracting to require or pressure ISPs to abide by the principles of net neutrality in the respective states. In addition, the Attorneys General of 22 states (including Maryland) have filed a lawsuit seeking to block the FCC's order. That lawsuit is pending.

---

### **Additional Information**

**Prior Introductions:** None.

**Cross File:** None.

**Information Source(s):** Maryland Association of Counties; Office of the Attorney General (Consumer Protection Division); Board of Public Works; Department of Budget and Management; Department of Information Technology; Maryland Institute for Emergency Medical Services Systems; Department of General Services; Department of State Police; Maryland Department of Transportation; Congress.gov; Federal Communications Commission; *Federal Register*; New York Attorney General's Office; FastCompany.com; *Consumer Reports*; Department of Legislative Services

**Fiscal Note History:** First Reader - March 6, 2018  
md/kdm Third Reader - April 9, 2018  
Revised - Amendment(s) - April 9, 2018  
Revised - Updated Information - April 9, 2018

---

Analysis by: Eric F. Pierce

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