Department of Legislative Services

Maryland General Assembly
2021 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

Senate Bill 351 (Chair, Education, Health, and Environmental Affairs Committee)(By Request - Departmental - Information Technology)

Education, Health, and Environmental Affairs Health and Government Operations

State Government – Protection of Information – Revisions (Maryland Data Privacy Act)

This departmental bill expands and enhances the security protocols that govern the collection, processing, sharing, and disposal of personal information by the State (Executive Branch only) and local governments. However, the bill excludes (1) public institutions of higher education from the bill's requirements as well as other existing requirements related to the protection of personal information and (2) the Office of the Attorney General (OAG), the Maryland 529 Board, and local government entities from some of the bill's *specific* cybersecurity and best practice requirements. Public institutions of higher education must submit an annual report to the Governor on their cybersecurity activities, as specified. **The reporting requirement for public institutions of higher education terminates December 31, 2024.**

Fiscal Summary

State Effect: General fund expenditures increase, likely significantly, for the Department of Information Technology (DoIT) to assist State agencies with coming into compliance with the bill's cybersecurity requirements, as discussed below. Revenues are not affected.

Local Effect: Local government expenditures may increase in order to comply with the data security requirements established by the bill that apply to units of local government, as discussed below. Revenues are not affected. **This bill may impose a mandate on a unit of local government.**

Small Business Effect: DoIT has determined that this bill has minimal or no impact on small business (attached). The Department of Legislative Services (DLS) concurs with this assessment. (The attached assessment does not reflect amendments to the bill.)

Analysis

Bill Summary: The bill generally:

- alters and expands the current statutory definition of "personal information," which is redefined as "personally identifiable information" (PII), and makes conforming changes;
- redefines the reasonable security procedures and practices that each affected unit of State government must employ to protect PII and makes conforming changes;
- excludes certain types of data from the bill's requirements; and
- establishes additional responsibilities related to PII for affected units of State government.

A more extensive discussion of the bill's provisions is provided below.

Applicability

The bill's requirements and existing personal information protection requirements apply only to the collection, processing, and sharing of PII by a unit of State or local government. The requirements do not apply to the collection, processing, or sharing of PII for the purposes of (1) public health; (2) public safety; (3) State security; (4) State personnel or retirement and pension system management; or (5) the investigation and prosecution of criminal offenses. Additionally, the requirements do not apply to the sharing of PII between the Maryland Department of Health and any State or federal agency as required by law or regulation.

The requirements may not be construed to (1) alter or supersede the Public Information Act; (2) affect the authority of a unit to make determinations regarding the disclosure of public records consistent with the act; or (3) require a unit to provide access to public records not disclosable under the act.

The Secretary of Information Technology may adopt regulations to carry out the bill's requirements.

Personally Identifiable Information and Security Requirements

Requirements that currently apply to "personal information" instead apply to PII. The "reasonable security procedures and practices" that must be used to protect PII are altered to mean protections that are consistent with DoIT's policies and regulations.

"PII" is defined to mean information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information associated with a particular individual, including (in addition to the unique personal identifiers and financial account numbers that are covered under the existing definition of personal information):

- characteristics of classifications protected under federal or State law;
- biometric information, as specified;
- geolocation data;
- Internet or other electronic network activity information, as specified; and
- information from multiple sources that can be used together or with other information to establish an individual's identity.

"PII" does not include voter registration information, information publicly disclosed by the individual without being under duress or coercion, or data rendered anonymous in a specified manner.

Additional Responsibilities for Units of State and Local Government

Units of State government, units of local government, the Maryland 529 Board, and OAG must undertake activities comprising the collection, processing, and sharing of PII in good faith; however, OAG, the Maryland 529 Board, and units of local government are not required to do so using the same processes and systems specified for units of State government. Even so, a unit of local government may request support from DoIT when developing best practices regarding security.

Except for OAG, the Maryland 529 Board, and local governments, the bill requires agencies to employ reasonable security procedures and practices to protect PII and to, among other requirements:

- implement specified best practices related to collection of PII, privacy, data protection, and data governance;
- share specified information with an individual regarding the unit's legitimate government purpose to collect the information and whether the sharing of that information is voluntary;
- establish a process for an individual to access specified information concerning his or her own PII, as specified; and
- provide specified notice to an individual when the unit intends to share that individual's PII, including the opportunity for the individual to opt out of sharing information with third parties.

In meeting the broad data security requirements that apply to them, OAG, the Maryland 529 Board, or a unit of local government may choose to employ the processes, systems, and best practices required of other units of State government, but they are not generally required to do so under the bill.

Reporting Requirements for Institutions of Higher Education

The bill exempts public institutions of higher education from both the bill's requirements and existing laws governing the protection of PII by government agencies. Instead, by December 1, 2021, and each year thereafter through 2024, each public institution of higher education must submit a report to the Governor that includes (1) a summary of the status of the implementation of any data privacy framework; (2) a description of any barriers or defects to implementation and solutions; (3) the number and disposition of reported breaches, if any; and (4) updates to project cost estimates.

Current Law:

Protection of Personal Information

Chapter 304 of 2013 requires a unit of State or local government (except for the Legislative and Judicial branches of State government) that collects an individual's personal information to implement and maintain reasonable security procedures and practices appropriate to the nature of the information collected and the nature of the unit and its operations. Similarly, a unit that uses a nonaffiliated third party as a service provider (and discloses personal information about an individual) must require that the third party implement and maintain reasonable security procedures and practices.

"Reasonable security procedures and practices" means data security procedures and practices developed, in good faith, and set forth in a written information security policy. "Personal information" means an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:

- a Social Security number;
- a driver's license number, State identification card number, or other individual identification number issued by a unit of State government;
- a passport number or other identification number issued by the United States government;
- an individual Taxpayer Identification Number; or

- a financial or other account number, credit card number, or credit card number that (in combination with a security code, access code, or password) would permit access to an individual's account.

Personal information does not include a voter registration number.

Department of Information Technology

DoIT and the Secretary of Information Technology are, among other things, responsible for (1) developing and enforcing information technology (IT) policies, procedures, and standards; (2) providing technical assistance, advice, and recommendations to any unit of State government; and (3) developing and maintaining a statewide IT master plan. The following agencies/institutions are exempt from oversight by DoIT:

- public institutions of higher education solely for academic or research purposes;
- the Maryland Port Administration;
- University System of Maryland;
- St. Mary's College of Maryland;
- Morgan State University; and
- the Maryland Stadium Authority (exempted by Chapter 150 of 2018).

Public Institutions of Higher Education

Chapter 429 of 2020 expanded and enhanced the security protocols that govern the collection, processing, sharing, and disposal of PII by public institutions of higher education in the State. Among other things, each public institution of higher education must (1) develop and adopt a privacy governance program to govern each system of record; (2) develop and adopt an information security and risk management program for the protection of PII, as specified; (3) publish a privacy notice on its website, as specified; (4) follow specified procedures when destroying PII records; and (5) follow specified procedures when it discovers or is notified of a breach of the security of one of its systems.

Background: DoIT advises that there is no strong legal basis established under current law for the protection of PII. The bill, therefore, expands and enhances the State's regulatory framework for collecting, processing, sharing, disposing of, and protecting personal information and requires most State agencies to implement this framework with DoIT's assistance. DoIT advises that the bill requires agencies to mirror federal procedures for ensuring that PII is protected from unauthorized access, use, modification, or disclosure.

For more information on cybersecurity issues facing both the State and the nation, please see the **Appendix – Cybersecurity**.

State Expenditures:

Compliance Costs for State Agencies

Each State agency that responded to a request for information for the bill advised that either (1) the agency already meets the enhanced security requirements established by the bill or (2) the agency plans to meet the bill's requirements at little to no cost with assistance from DoIT.

DLS does not have the technical expertise to assess each agency's current security infrastructure and protocols and, therefore, cannot independently verify their estimates for coming into compliance with the bill. The public four-year institutions of higher education and Baltimore City Community College can submit the annual report using existing budgeted resources.

Department of Information Technology

As previously noted, most State agencies plan to implement the bill's requirements by working with and relying on DoIT. DoIT is likely to incur costs in fiscal 2022 and future years as it continues to evaluate and improve State agency cybersecurity infrastructure; however, the precise impact cannot be reliably estimated at this time. *For illustrative purposes,* the fiscal 2021 operating budget for DoIT included $10 million in general funds for DoIT to enhance cybersecurity in the State. DoIT is using these funds primarily to conduct cybersecurity assessments of State agencies, work to rectify any problems discovered, and assist agencies with enhancing their cybersecurity practices in accordance with the bill. DoIT advises that it expects to receive similar allocations in future years. The estimate does not reflect any reimbursable revenues (or expenditures) that may be realized because DoIT plans to assist agencies at no cost to the agencies. With the experience it gains and the documents it produces from assisting State agencies, DoIT can also likely provide advice and technical assistance to local governments, if requested to do so, using existing resources.

Local Expenditures: As previously discussed, many of the bill's broad data protection requirements apply to local governments while the specific processes, best practices, and systems that must be employed under the bill do not. Additionally, if assistance from DoIT is requested, local governments may be able to adopt the cybersecurity best practices and procedures used by the State instead of developing their own. Even so, some local governments may still experience increased expenditures to comply with the bill's requirements, while others may employ systems that already do so. For example, for a

similar bill in a previous year, the Maryland Association of Counties advised that most local governments would be able to comply with the bill with negligible or minimal increased costs, while at least one county advised that it would have to upgrade multiple information systems.

As previously noted, DLS does not have the technical expertise to assess local governments' current security infrastructures and protocols and, therefore, cannot independently verify any such estimates for coming into compliance with the bill. Local community colleges can submit the annual report with existing resources.

Additional Information

Prior Introductions: Similar legislation has been considered in recent legislative sessions. HB 340 of 2020 passed the House and was referred to the Senate Education, Health, and Environmental Affairs Committee, but no further action was taken. Its cross file, SB 274 of 2020, received a hearing in the Senate Education, Health, and Environmental Affairs Committee, but no further action was taken. HB 716 of 2019 was amended in both the House and the Senate, but the differences were not reconciled.

Designated Cross File: None.

Information Source(s): Department of Information Technology; Department of Commerce; University System of Maryland; Morgan State University; St. Mary's College of Maryland; Maryland Department of Agriculture; Department of Budget and Management; Maryland Department of Disabilities; Maryland Department of the Environment; Department of General Services; Department of Housing and Community Development; Department of Juvenile Services; Department of Natural Resources; Maryland Department of Planning; Department of State Police; Maryland Department of Transportation; Department of Veterans Affairs; Department of Legislative Services

Fiscal Note History: First Reader - January 15, 2021
rh/mcr Third Reader - March 30, 2021
Revised - Amendment(s) - March 30, 2021
Revised - Other - March 30, 2021

Analysis by: Richard L. Duncan

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

Appendix – Cybersecurity

Cybersecurity Issues

In recent years, cybersecurity and privacy issues have received significant attention from the general public and policymakers as a result of the many ransomware attacks, data breaches, and other cyberattacks that have taken place in the nation and the State. Globally, in 2019 and 2020, the Center for Strategic and International Studies identified over 200 cyberattacks and data breaches (many of which involved the United States) involving (1) government agencies; (2) defense and high tech companies; or (3) economic crimes with losses of more than $1 million. For example, in November 2020, Baltimore County Public Schools' information technology (IT) systems were made unusable by a ransomware attack and the personally identifiable information (PII) of 27.7 million Texas drivers was exposed in a data breach.

In 2019, governments in the State experienced numerous cyberattacks and breaches. Most notably, Baltimore City government's computer systems were infected with ransomware that made the systems inaccessible and unavailable for weeks. Similarly, the Maryland Department of Labor's licensing database was breached, and PII of as many as 78,000 licensees may have been accessed by the hackers.

Recent State Action

In June 2019, the Governor signed Executive Order 01.01.2019.07, which creates the Maryland Cyber Defense Initiative to strengthen the State's ability to manage the effects of a cybersecurity incident. The initiative creates the Office for Security Management within the Department of Information Technology (DoIT) and charges the office with responsibility for the direction, coordination, and implementation of an overall cybersecurity strategy for all Executive Branch IT systems. The office is led by the State chief information security officer (SCISO), who is appointed by the Governor. The order also established the Maryland Cybersecurity Coordinating Council to assist SCISO and the office in their duties.

In that same month, DoIT released the State of Maryland Information Technology Security Manual. The manual currently serves as the primary policy for establishing and defining the State's IT security practices and requirements; all State agencies are required to adhere to the manual.

Legislation enacted in 2020 expands and enhances the cybersecurity protocols that govern the collection, processing, sharing, and disposal of PII by public institutions of higher education in the State beginning on October 1, 2024.

Audits of State Agency Cybersecurity Discover PII Vulnerabilities

Over the 2019 interim, the Office of Legislative Audits (OLA) summarized its recent audit findings related to cybersecurity and PII and reported those findings to the Joint Audit and Evaluation Committee in December 2019. OLA found that, from July 2013 through December 2019, approximately 37.9 million PII records existed in State and local government agencies that were not adequately protected with data security controls. Over that same period, 77 of OLA's audits contained findings related to PII. While DoIT and the State have been improving their protection of PII, a 2020 legislative audit found additional issues. For example, in one instance PII was not adequately restricted to employees who should have access to it and instead was visible to over 5,000 State employees.

OLA has previously emphasized the financial cost associated with data breaches by citing the Ponemon Institute, an independent research organization focused on data protection, and IBM, one of the largest computer manufacturers in the world. The two organizations annually publish a report on global data breaches and their economic impacts. The 2020 Cost of a Data Breach Report found:

- the average total cost of a data breach in the United States is $8.6 million; and
- customer PII has the highest cost per record at $150. *For illustrative purposes*, costs for Texas could total $4.2 billion, as a result of the 27.7 million breached records discussed above.

These costs include detection of the breach, escalation, notifications, response, and lost business.

Cybersecurity Legislation in Other States

The National Conference of State Legislatures (NCSL) advises that 38 states, the District of Columbia, and Puerto Rico introduced or considered about 280 bills or resolutions that dealt significantly with cybersecurity in 2020. Some of the key cybersecurity issues considered included:

- requiring government agencies to implement training or specific types of security policies and practices and improving incidence response and preparedness;

- increasing penalties for computer crime or addressing specific crimes, *e.g.*, ransomware;
- regulating cybersecurity within the insurance industry or addressing cybersecurity insurance;
- creating task forces, councils, or commissions to study or advise on cybersecurity issues; and
- supporting programs or incentives for cybersecurity training and education.

Moreover, NCSL reports that 19 states (including Maryland) adopted or enacted significant cybersecurity-related legislation in 2020. Notably, (1) Delaware granted its Department of Technology and Information the authority to develop and implement a comprehensive security program; (2) Georgia is using funds from its Revenue Shortfall Reserve to enhance cybersecurity technologies; (3) Louisiana enacted 10 pieces of legislation to significantly enhance its cybersecurity framework; and (4) Virginia required its chief information officer to develop and annually update a training program for all state employees in security awareness and in procedures for detecting, assessing, reporting, and addressing information security threats.

Notably, in 2019, 31 states adopted or enacted significant cybersecurity-related legislation. Most notably, (1) New York City enacted the Stop Hacks and Improve Electronic Data Security Act, which amended the state's data breach notification law and imposed more expansive data security requirements on companies; (2) Alabama, Delaware, Mississippi, and New Hampshire enacted legislation establishing a comprehensive security framework that insurance companies must implement; and (3) Oregon enacted legislation requiring manufacturers of "connected devices" to equip those devices with reasonable security features.

ANALYSIS OF ECONOMIC IMPACT ON SMALL BUSINESSES

TITLE OF BILL: State Government – Protection of Information – Revisions (Maryland Data Privacy Act)

BILL NUMBER: SB 351

PREPARED BY: Patrick Mulford

PART A. ECONOMIC IMPACT RATING

This agency estimates that the proposed bill:

x__ WILL HAVE MINIMAL OR NO ECONOMIC IMPACT ON MARYLAND SMALL BUSINESS

OR

___ WILL HAVE MEANINGFUL ECONOMIC IMPACT ON MARYLAND SMALL BUSINESSES

PART B. ECONOMIC IMPACT ANALYSIS

To the extent that small business would either have to spend money or act on this legislation- there is no impact. It is important to note however, that there is value in protecting, to the greatest extent possible, all PII. The theft of PII can cost untold amounts of money.