SB 351 - PGCEX - FAV.pdf
Uploaded by: Alsobrooks, Angela
Position: FAV

THE PRINCE GEORGE'S COUNTY GOVERNMENT

OFFICE OF THE COUNTY EXECUTIVE

BILL:	**Senate Bill 351 – State Government – Protection of Information – Revisions (Maryland Data Privacy Act)**
SPONSOR:	**Chair, Education, Health, and Environmental Affairs Committee (By Request - Departmental - Information Technology)**
HEARING DATE:	**March 31, 2021**
COMMITTEE:	**Education, Health, and Environmental Affairs**
CONTACT:	**Intergovernmental Affairs Office, 301-780-8411**
POSITION:	**SUPPORT**

The Office of the Prince George's County Executive **SUPPORTS Senate Bill 351 – State Government – Protection of Information – Revisions (Maryland Data Privacy Act)**, which 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 public institutions of higher education from the bill's requirements as well as other existing requirements related to the protection of personal information and the Office of the Attorney General 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.

With the advent of most transactions that are used in conducting business in government (as well as in all facets of life) require people to input their name, address, SSN, driver license number, passport number and other information to validate the person is who they are and residency. Documentation requirements have increased under federal 'REAL ID laws for certain transactions. Such information collected by government are required to be kept from unauthorized discloser, and today's information systems have built in security to minimize exposure, and only if legal practices are followed, such as the individual gives permission willingly if it is necessary. Bad actors, those who troll the Internet, or may work in an organization and have access to such information can use it to 'steal' a person's identification, clone them, and establish bogus transactions under person's name, diverting it for

nefarious purposes. The U.S. Department of Justice establish the Privacy Act in 1974, and State and local laws have been using and making clear through their legislative processed governing Privacy updates and specifics for the data they collect, use and are custodians of.

SB 351 provide revisions to the Maryland Data Privacy Act with definitions and clarity of Personally Identifiable Information (PII) and what it consists of in combinations to include financial information, account numbers and the like, how PII can be used in identifying or creating identities of persons, and, clarity regarding certain information sources used for certain purposes not covered under the ACT that is publicly disclosable, and that disclosure by persons cannot be done under duress.

This further established that IT/cyber security procedures and practices used by units of the State are consistent with the Maryland Department of Information Technology polices and regulation.

Some reasons for support are that:

- Updates are needed as new ways of extracting information come about, and that as new IT systems are used for governmental purposes, those are implemented with the privacy requirement built in and in contracts. This is import update so that government entities that handle PII are knowledgeable and can strengthen internal procedures as needed, being stewards of the public's data and information, and protecting the public from illegal acts.

- Personal Data is involved in 58% of data breaches in 2020; 64% of Americans have never checked to see if they were affected by a data breach; 30% of breaches are by internal actors (*this information from Internet published sources*). These statistics do not include the amount of PII still in paper processes in many units of government.

- This legislation is because it is aligned with legislation and best practices that have been put in place in other state, such as the California Consumer Privacy Act (CCPA) which was enacted in 2018 and took effect on January 1, 2020.

The main purpose of the CCPA is to give Californians more control over their personal information, by granting them a number of fundamental rights: to know what personal information is being collected about them; to access this information; to know whether it is sold and to whom; to ask that their personal data be deleted, and to refuse to allow that it keeps being sold; and to receive equal service and price, even if they have exercised the previous right to opt-out.

This legislation will serve as an important step toward providing Marylanders with up-to-date knowledge controls and align Maryland and its units of government with industry best practices being adopted across the country.

For the reasons stated above, the Office of the Prince George's County Executive **SUPPORTS Senate Bill 351 AS AMENDED** and asks for a **FAVORABLE** report.

SB351_DoIT_MichaelLeahy_HGO.pdf
Uploaded by: Mulford, Patrick
Position: FAV

Date: March 31, 2021
Bill: Senate Bill 351 - State Government - Protection of Information - Revisions (Maryland Data Privacy Act).
Position: Support

The Honorable Shane E. Pendergrass, Chair
Health and Government Operations Committee
House Office Building, Room 241
Annapolis, Maryland 21401

Dear Chair Pendergrass:

The Department of Information Technology (DoIT) supports Senate Bill 351 - State Government - Protection of Information - Revisions (Maryland Data Privacy Act). Within state government, the goal should be to limit the amount of Personally Identifiable Information (PII) collected and ensure Marylanders understand why their information is being collected, for what purposes and how it is being used. Citizens must also have confidence that their government is taking the proper precautions to ensure the confidentiality and integrity of their information. Senate Bill 351 requires compliance with certain standards and guidelines to ensure that all personal data is being collected and managed in a secure manner.

Under this legislation, certain state agencies would be required to collect, process and share PII in a manner that is consistent with the requirements set forth by DoIT, including:

- Identifying and documenting the governmental purpose for the collection of such data;
- Notifying an individual when PII is being collected and describing the purpose for the collection;
- Implementing reasonable data handling procedures to ensure the confidentiality, integrity, and availability of all PII is maintained;
- Incorporating privacy requirements into agreements with any third parties that handle PII while under contract with the State;
- Ensuring that PII collected is accurate, relevant, timely, and complete;
- Only collecting PII that is relevant to the legally authorized purpose of the collection;
- Allowing an individual to access their PII and allowing them to correct or amend the collected PII; and
- Informing the individual or public of the practices and activities regarding the use of their PII including any rights the individual or public has to decline, correct or review the PII.

The Maryland Data Privacy Act modernizes the way state government agencies secure and manage PII. The bill requires agencies to mirror DoIT procedures for ensuring that PII is protected from unauthorized access, use, modification, or disclosure. Citizens must also be advised whether the disclosure of certain PII is voluntary or required, how that information is

shared with third parties, and be provided an opt-out provision when possible. This proposal does not address private industry and broadly excludes uses related to public safety, public health, state security, and the investigation and prosecution of criminal offenses. To the extent that current laws and policies are being followed, there will be no fiscal impact because of this legislation.

This bill is essentially the same bill that DoIT submitted last year with one minor change that substitutes a specific requirement for security standards such as the Federal Information Processing Standards with security protections that are consistent with DoIT policies and regulations. DoIT policies and regulations follow federal standards but we did not want the legislation to force the use of a certain standard if federal standards were to change over time.

There were very minor amendments to the bill in the Senate including exempting the Maryland 529 Board from certain provisions in the bill because they act as a private entity. Another amendment informs the local governments that they are able to request support from DoIT to develop best practices regarding cybersecurity. DoIT supports these amendments and for the reasons stated above respectfully requests a favorable report on Senate Bill 351 as amended.

Best,

Michael G. Leahy

SB0351-HGO_MACo_OPP.pdf
Uploaded by: Butler, Alex
Position: UNF

MARYLAND Association of COUNTIES

Senate Bill 351

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

MACo Position: **OPPOSE**

To: Health and Government Operations Committee

Date: March 31, 2021

From: Alex Butler

The Maryland Association of Counties (MACo) **OPPOSES** SB 351. This bill alters Maryland's Data Privacy Act in several ways that make it difficult for local governments to implement. MACo believes that all provisions of this bill should pertain only to state agencies.

SB 351 would alter the list of data that requires protection under the Maryland Data Privacy Act. Instead of being a list of types of data to protect, government officials would have to evaluate each type of data in each situation to determine if it might be combined with something else that could reveal identity. This is impractical and will lead to inconsistency. It is unclear how a local government will be able to explain to software and IT vendors which information is subject to the law's privacy requirements.

The bill expands Maryland's Data Privacy Act to govern when information can be shared within the government itself. The bill does this by adding a prohibition on sharing "personally identifiable information" within a government unless it is for a public safety, public health, or similar listed purpose. This directly conflicts with the Maryland Public Information Act, which governs when certain personal information can be shared between one unit of government and another. However, language in SB 351 purports that it does not alter or supersede the Public Information Act. The Maryland Data Privacy Act should not contain any language on data sharing.

Additionally, the bill as written would retroactively impact all contracts after July 1, 2014. This would impact contracts that local governments have already formed and acted upon.

These changes to the Maryland Data Privacy Act would make it much more difficult for local governments to implement and therefore MACo respectfully requests an **UNFAVORABLE** report on SB 351.

169 Conduit Street, Annapolis, MD 21401
410.269.0043 BALT/ANNAP ◆ 301.261.1140 WASH DC ◆ 410.268.1775 FAX
www.mdcounties.org

SB351-HGO-OPP.pdf
Uploaded by: Mehu, Natasha
Position: UNF

BRANDON M. SCOTT
Mayor

Office of Government Relations
88 State Circle
Annapolis, Maryland 21401

SB 351

March 31, 2021

TO: Members of the House Health and Government Operations Committee

FROM: Natasha Mehu, Director of Government Relations

RE: Senate Bill 351 – Public Information Act – Revisions

POSITION: OPPOSE

Chair Pendergrass, Vice-Chair Peña-Melnyk, and Members of the Committee, please be advised that the Baltimore City Administration **opposes** Senate Bill 351.

This bill alters Maryland's Data Privacy Act in two fundamentally misguided ways, by: 1) adding confusing language that conflicts with the long-standing requirement that this law not impact Maryland's Public Information Act; and 2) changing the definition of "personal information" from a clear list of data elements to a subjective definition dependent on what the information can be used to do "either alone or when combined with other information."

First, the Maryland Data Privacy Act is clear that it is not intended to "alter or supersede the requirements of the Public Information Act." Md. Code, State Gov.'t. § 10- 1302(a)(1). This is important because Maryland's Public Information Act ("PIA") applies to data shared between agencies within the same government. Md. Code, Gen. Prov., § 4-202; *Montgomery County v. Shropshire*, 420 Md. 362, 383 (2011). Bill Section 10-1304 (C) (concerning when governments can collect certain information) is in direct conflict with the PIA because it attempts to regulate intragovernmental data sharing.

Second, the bill defines personal information as that which could be combined with something else to reveal identity. Bill Section 10-1301(D). Currently, the list of data to protect is enumerated in Section 10-1301(c). To alter the definitional paradigm by making government officials the arbiters of what data will *do* when combined with other information is unworkable and will result inconsistencies. The bill provides no guidance on how to evaluate de-identified data that, when coupled with other data, may reveal identity. Government employees will be inconsistent in their individual determinations that other data exists to make the de-identifiable record deemed personal information under this bill.

The PIA does NOT suffer from this infirmity because it defines records solely by their contents; separating the definition of the record from the process of evaluating disclosure. The PIA makes clear that certain records may not be disclosed, even when de-identified. Maryland Public Information Act Manual, p. 3-11 (14th ed., Oct. 2015) ("[w]hat constitutes 'identifying information' . . . will depend on the specifics of each request.")' *accord* 90 Md. Op. Atty. Gen 45, 54-55 (2005) ("report might still be 'about an individual' if the unredacted information 'sharply narrows' the class of individuals to whom the information might apply or 'likely' could be used to identify the individual with 'reasonable certainty'"); *accord Havemann v. Astrue*, Civil Action No. ELH–10–1498, 2012 WL 4378143, * 7 (D. Md. Sept. 24, 2012) (unreported) (holding that in context of certain labor records, zip code should not be disclosed). If there is a desire to further restrict the disclosure of certain information between government agencies, the PIA disclosure process should be amended to effectuate that change. Putting disclosure restrictions in a bill that claims it does not alter the PIA is ineffectual. So, too, would be the exemptions listed in Bill Section 10-1302(A)(2), as they would conflict with the PIA's well-defined scheme for disclosure. Md. Code, Gen. Prov., § 4- 301, *et. seq*.

This confusion is compounded by the requirement in current Section 10-1304(b) that the law is to be applied to all contracts entered into as of July 1, 2014. While this date might have made sense when it was originally enacted, it is now arguably an unconstitutional impairment of existing government contracts. U.S. Constit., Art I, s 10, cl. 1; *see, e.g.*, *Garris v. Hanover Insurance Company*, 630 F.2d 1001, 1004 (4th Cir. 1980) (holding stricter scrutiny of the applies when the government enacts a law that impacts contracts to which it is a party). It is also unworkable because it makes a requirement of a government contract (to protect certain government data) based on the vague and flexible definition of "personal information" as noted above. *See, e.g, Carroll County v. Forty West Builders*, 178 Md. App. 328, 377-78 (2008) ("an enforceable contract must express with definiteness and certainty the nature and extent of the parties' obligations") (citations omitted).

We respectfully request an **unfavorable** report on Senate Bill 351.

SB351Ruley.pdf
Uploaded by: Ruley, Hilary
Position: UNF

BRANDON M. SCOTT
Mayor

Office of Government Relations
88 State Circle
Annapolis, Maryland 21401

SB 351

January 13, 2021

TO: Members of the Senate Education, Health and Environmental Affairs Committee

FROM: Natasha Mehu, Director of Government Relations

RE: Senate Bill 351 – Public Information Act – Revisions

POSITION: OPPOSE

Chair Pinsky, Vice-Chair Kagan, and Members of the Committee, please be advised that the Baltimore City Administration **opposes** Senate Bill 351.

This bill alters Maryland's Data Privacy Act in two fundamentally misguided ways, by: 1) adding confusing language that conflicts with the long-standing requirement that this law not impact Maryland's Public Information Act; and 2) changing the definition of "personal information" from a clear list of data elements to a subjective definition dependent on what the information can be used to do "either alone or when combined with other information."

First, the Maryland Data Privacy Act is clear that it is not intended to "alter or supersede the requirements of the Public Information Act." Md. Code, State Gov.'t. § 10- 1302(a)(1). This is important because Maryland's Public Information Act ("PIA") applies to data shared between agencies within the same government. Md. Code, Gen. Prov., § 4-202; *Montgomery County v. Shropshire*, 420 Md. 362, 383 (2011). Bill Section 10-1304 (C) (concerning when governments can collect certain information) is in direct conflict with the PIA because it attempts to regulate intragovernmental data sharing.

Second, the bill defines personal information as that which could be combined with something else to reveal identity. Bill Section 10-1301(D). Currently, the list of data to protect is enumerated in Section 10-1301(c). To alter the definitional paradigm by making government officials the arbiters of what data will *do* when combined with other information is unworkable and will result inconsistencies. The bill provides no guidance on how to evaluate de-identified data that, when coupled with other data, may reveal identity. Government employees will be inconsistent in their individual determinations that other data exists to make the de-identifiable record deemed personal information under this bill.

The PIA does NOT suffer from this infirmity because it defines records solely by their contents; separating the definition of the record from the process of evaluating disclosure. The PIA makes clear that certain records may not be disclosed, even when de-identified. Maryland Public Information Act Manual, p. 3-11 (14th ed., Oct. 2015) ("[w]hat constitutes 'identifying information' . . . will depend on the specifics of each request.")' *accord* 90 Md. Op. Atty. Gen 45, 54-55 (2005) ("report might still be 'about an individual' if the unredacted information 'sharply narrows' the class of individuals to whom the information might apply or 'likely' could be used to identify the individual with 'reasonable certainty'"); *accord Havemann v. Astrue*, Civil Action No. ELH–10–1498, 2012 WL 4378143, * 7 (D. Md. Sept. 24, 2012) (unreported) (holding that in context of certain labor records, zip code should not be disclosed). If there is a desire to further restrict the disclosure of certain information between government agencies, the PIA disclosure process should be amended to effectuate that change. Putting disclosure restrictions in a bill that claims it does not alter the PIA is ineffectual. So, too, would be the exemptions listed in Bill Section 10-1302(A)(2), as they would conflict with the PIA's well-defined scheme for disclosure. Md. Code, Gen. Prov., § 4- 301, *et. seq*.

This confusion is compounded by the requirement in current Section 10-1304(b) that the law is to be applied to all contracts entered into as of July 1, 2014. While this date might have made sense when it was originally enacted, it is now arguably an unconstitutional impairment of existing government contracts. U.S. Constit., Art I, s 10, cl. 1; *see, e.g., Garris v. Hanover Insurance Company*, 630 F.2d 1001, 1004 (4th Cir. 1980) (holding stricter scrutiny of the applies when the government enacts a law that impacts contracts to which it is a party). It is also unworkable because it makes a requirement of a government contract (to protect certain government data) based on the vague and flexible definition of "personal information" as noted above. *See, e.g., Carroll County v. Forty West Builders*, 178 Md.App. 328, 377-78 (2008) ("an enforceable contract must express with definiteness and certainty the nature and extent of the parties' obligations") (citations omitted).

We respectfully request an **unfavorable** report on Senate Bill 351.