



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 established the Privacy Act in 1974, and State and local laws have been using and making clear through their legislative processes 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 policies 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.