NED CAREY
Legislative District 31A
Anne Arundel County

Economic Matters Committee

Subcommittees

Alcoholic Beverages
Chair, Unemployment Insurance

House Chair
Joint Committee on
Unemployment Insurance Oversight

Chair
Anne Arundel County Delegation

The Maryland House of Delegates
6 Bladen Street, Room 161
Annapolis, Maryland 21401
410-841-3047 · 301-858-3047
800-492-7122 *Ext.* 3047
Ned.Carey@house.state.md.us

THE MARYLAND HOUSE OF DELEGATES
ANNAPOLIS, MARYLAND 21401

HB 237 - Consumer Law – Personal Information Protection Act – Revisions – as amended

SPONSOR TESTIMONY

Cross-file: SB 201

House Economic Matters Committee, February 26, 2020

Chairman Davis, Vice Chair Dumais and Members of the Committee,

House Bill 237 is a bill that strengthens the Maryland Personal Information and Protection Act (MPIPA) in response to changes in the type of data being collected about consumers.

The data collection landscape changed dramatically since the last update of MPIPA in 2017, and consumers are giving new and even more personal information in order to take advantage of new technology that provide apps and services that can enhance their lives.

This bill, accordingly, expands the definition of personal information in the statute to include activity tracking data and genetic information.

Parking apps can help you find a parking space in a highly trafficked, unfamiliar city, offering time-savings and a sense of safety. Genetic testing services such as 23andMe can connect you with relatives and help you discover your lineage. At the same time, your DNA, your minute-by-minute location and your private communications and connections with friends and family are among the most personal and sensitive pieces of information that companies can collect about you, and should clearly be included under the definition of personal information.

HB 237 also streamlines the industry response to data breaches by expediting the notification process, giving consumers the power to make changes before they experience a problem as a result of the breach.

- Many businesses (data owners or licensees) store and protect their data through a third party (maintainer of data). This bill changes the time frame for a maintainer to notify the owner/licensee from 45 days to a maximum of 10. This requires the maintainer of the data and the owner of the data to start the dialogue early and remain in contact throughout investigation.

- Consumer notification and trigger: Once a data owner or licensee discovers or receives notice that there has been a data breach, they currently have 45 days to notify consumers AFTER they've concluded their investigation. This bill, as amended, requires them to give notice no more than 45 days from the time they are made aware of the breach. **This is a necessary change**, as many companies were extending their investigations over a period of months to even as much as three years. By the time the consumer is notified, it has become moot. There are provisions in the bill that allow for a pause if notification would impede a criminal investigation or undermine national security.

This bill also strives to ensure consumers actually receive notification by no longer allowing the substitute notice to be the primary means of notification, such as setting up a webpage for consumers to check if their information was compromised. Data owners and licenses are required to notify consumers directly by written notice, electronic mail or hard mail. The only exception is if the company has neither the email or address or any other means of notifying consumers.

These updates are necessary to protect Maryland consumers in this rapidly changing cyber environment.

For this reason, **I ask for a favorable report on HB 237 as amended.**

As a footnote: We've gotten some pushback from industry that believe the definition of "activity-tracking data" is overly broad and could include data that has been de-identified or pseudonymized. This concern is clearly addressed by the existing language in the definition of personal information, specifically 14-3501(F)(1)(i), which excludes encrypted, de-identified and pseudonymized data from the definition.