Susan C. Lee
Legislative District 16
Montgomery County

Majority Whip

Judicial Proceedings Committee

Joint Committee on
Cybersecurity, Information Technology,
and Biotechnology

Chair Emeritus
Maryland Legislative Asian American
and Pacific Islander Caucus

President Emeritus
Women Legislators of the
Maryland General Assembly, Inc.

THE SENATE OF MARYLAND
Annapolis, Maryland 21401

James Senate Office Building
11 Bladen Street, Room 223
Annapolis, Maryland 21401
410-841-3124 · 301-858-3124
800-492-7122 *Ext.* 3124
Susan.Lee@senate.state.md.us

February 12, 2020

Senate Finance Committee

Senate Bill 201 – Commercial Law – Personal Information Protection Act – Revisions

Senate Bill 201 strengthens the Maryland Personal Information Protection Act (MPIPA) in response to changes in the type of data being collected about consumers and the seemingly constant slew of data breaches. When our data is used for services we seek, the misuse of that data must compel service providers to notify us as soon as possible, or they are doing all consumers a disservice. Privacy is of critical importance in the 21st century and personally identifiable data that can be used to steal and take over an identity is of the highest importance. This bill is outlining simply the process to notify a potential victim of identity theft to be on guard from a service they likely paid, only to have their trust abused.

SB201 recognizes the dramatic changes in the data collection landscape since the previous update of MPIPA and, accordingly, expands the definition of personal information in the statute to include activity tracking data, including behavioral data and geo-location data, as well as genetic information and non-public social media data. 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. These categories of information should clearly be included under the definition of personal information.

SB201 strives to streamline the industry response to data breaches and empower consumers by expediting the notification process. The way many businesses store and protect their data is through a third party, essentially a company that maintains data. Under current law, if a company that maintains data discovers or is notified of a breach, they have, at maximum, 45 days to notify the owner/licensee of that data; our bill changes that cap to 10 days. This is reasonable because

there is not much the maintainers of the data are required to do at this point but tell the licensee of the data. The investigation into whether there was harm would come later.

Once a data owner or licensee discovers of receives notice that there has been a data breach, they currently have 45 days to notify consumers. Our bill changes that cap to 30 days. Under current law, the company is not required to notify consumers that a breach has occurred unless they make an affirmative determination that harm is likely to result from that breach. This bill switches that standard so that a company is required to notify consumers that a breach has occurred unless that make an affirmative determination that harm is unlikely to result from the breach.

Prior to consumer notification, the licensee or owner of data must report to the Office of the Attorney General a description of the breach and how it occurred, the scope of the breach and the number of Marylanders effected, and a draft of the notification that the company plans to share with affected consumers. Any sensitive information would be shielded from PIA requests.

The process of consumer notification is also changed under this bill. Data owners and licensees are now required to notify consumers by written notice, electronic mail or hard mail; licensees are no longer able to provide only substitute notice (i.e. setting up a webpage where consumers to check if their information was compromised). Imagine being a consumer whose personal information, from your credit history to your social security number, was compromised in the Equifax breach. Would you feel comfortable re-entering all of your personal information on a website set up by the company that had just compromised that information? Direct notification to consumers that harm has been is necessary and is not an undue burden on industry.

The bill also adds a requirement that a business that *maintains* the personal information of a Maryland resident implement reasonable security procedures that are appropriate given the nature and size of the business collecting that information. This requirement already exists for data owners and licenses; adding the requirement for maintenance of data is simply a clarification.

For all of these reasons, I respectfully request a favorable report on SB201.