Susan C. Lee
Legislative District 16
Montgomery County

Majority Whip

Judicial Proceedings Committee

Joint Committee on
Cybersecurity, Information Technology,
and Biotechnology

Chair
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

March 16, 2022

Senate Finance Committee

Senate Bill 643 – FAVORABLE– Personal Information Protection Act

Senate Bill 643 is a data breach notification update for Maryland's Personal Information and Protection Act (MPIPA). The provisions of this legislation aim to improve the security of how information that is sensitive about individuals is stored, and then how notice is provided to affected consumers. To meet the threshold of security required to be exempt from any notification requirements under law, a business merely has to put the personal information behind a firewall or encrypt it. If you use EITHER of those methods for to protect personal information, this law will not apply to you, however, if you fail to protect data, and it is breached, you would have to disclose that fact and provide notice to the parties who could be harmed.

Currently, MPIPA requires notice "as soon as reasonably practicable, but not later than 45 days after the business *concludes* [its] investigation" into the breach. This bill triggers the notification clock to start counting when a business *discovers* a breach. Many other states use this same trigger including but not limited to Colorado, Florida, New Mexico, Ohio, Tennessee, Vermont, Washington, and Wisconsin. SB 643 also updates the notice timeline when there is an investigation, but an amendment clarifies there would still be the underlying threshold of 45 days. Amendments further clarify that the notification requirements for genetic information that is de-identified to satisfy industry implementation concerns.

This is not a rehash of the larger consumer protection issue of control over your data, this bill wouldn't prevent doctor evil from using your DNA to make a mini-me, but it would require him to put that data behind a firewall. Other laws may apply to attempted world domination. There is a need to protect how data is used, but this bill is only about how data is stored, and the minimum requirement of notice if it has been compromised. The new provision about genetic data is focused on encouraging encryption of your genetic information, and then letting you know if it has been acquired by someone unlawfully.

This is and has been a consensus bill for some time, but we are bending backwards even more now with this year's version. There are pro-industry group changes like the clarification that you need both the name and the personal information to trigger a notification requirement that is ambiguous in the current law. The statute merely requires reasonable protection of personal data, and notification to consumers and Consumer Protection Division at the Attorney General's office if there is a data breach.

The cross-file HB 962 has already passed the House and the amendment that was attached to further the compromise can be viewed here and will also be uploaded for the committee's file of course. This was a compromise in 2020, and again last year, but this session we have the time to get it passed so that at least data is protected by the companies that have control over it, because it is not yet controlled by the consumer until we pass more sweeping legislation like the Online Consumer Protection and Child Safety Act. This is the low hanging fruit that could create a rot if we don't pick it quickly.

For these reasons, I respectfully request a favorable report on SB 643 as amended to conform to the House cross-file language.