



February 26, 2020

Chair, Dereck Davis
House Committee on Economic Matters
6 Bladen Street Room 231
Annapolis, MD

Dear Chairman Davis:

On behalf of the Security Industry Association (SIA) I am writing to express our concerns with MD HB 307, which establishes requirements & restrictions on private entities use, collection, & maintenance of biometric identifiers & biometric information, while creating a private cause of action for relief on violations of the act.

The Security Industry Association (SIA), which is based in Silver Spring, is a nonprofit trade association representing businesses that provide a broad range of security products for government, commercial and residential users in the U.S., including businesses headquartered in Maryland and many more with employees and significant business operations in the state. Our members include many of the leading manufacturers of biometric technologies, as well as those who are integrating these technologies into a wide variety of building security and life-safety systems.

At the outset, I want to stress that our members intend their technology products only be used for purposes that are lawful, ethical and non-discriminatory. While we generally support the data policies outlined in H.B. 307 as good practice, careful consideration should be given to whether biometric information should be singled out for regulation separate from other personal data it is often associated with, including biographic information like date of birth, physical characteristics, Social Security number, address, employment, health and education history – the type of information that so far has proven to be more vulnerable to compromise and misuse.

Biometric authentication enhances identity protections while increasing the effectiveness of security systems developed by our industry. Many sectors of the business community stand to benefit from technologically advanced equipment that utilizes biometric identifiers for security purposes, such as authentication, for employee access to buildings or computer networks, and security systems that protect buildings, their occupants and the assets contained therein.

At a minimum, an exemption to a notification and consent requirement for safety and security uses is essential. A good example is the security provision included in Washington State's current biometric data law enacted in 2017. This law generally requires notice and consent of an individual before their biometric information is enrolled in a database for commercial use, but provides an express exception where the collection, capture or enrollment and storage of a biometric identifier is in furtherance of a security purpose (RCW 19.375.020, §7). Such an exemption is necessary, because requiring written consent would be unworkable for building systems intended for safety or security applications, as an individual with malicious intent would likely not consent to having their information captured.

An increasingly important benefit of biometric data is that it gives employers the ability to alert staff and other building occupants of immediate threats to the safety of a building's occupants, such as where a disgruntled former employee attempts to enter the workplace. Requiring consent or automatic deletion of data after employment would run contrary to ensuring public safety in this case.

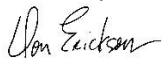
Additionally, a consent requirement makes participation optional, thus limiting the ability to effectively deploy safety and security systems that utilize biometric technologies throughout a building, due to the presence of a mixed population of consenting and non-consenting individuals. Without an exception, a consent requirement would essentially preclude using these technologies for the enhancement of access control, intrusion detection, anti-theft, fire alarm, active shooter and other safety and security purposes throughout a building.

The private right of action in the bill should be replaced with enforcement by the attorney general. This mechanism would preserve the protective intent without the potential catastrophic consequences for businesses subjected to unwarranted lawsuits. This is the approach Washington and Texas have taken with their biometrics laws.

In conclusion, due to the wide-ranging negative consequences for Marylanders and Maryland businesses from implementing a Biometric Information Privacy Act (BIPA)-type approach to regulating use of biometric data, we urge the Committee not to advance H.B. 307 in its current form. Instead, we ask that the issue be thoroughly and thoughtfully studied before any legislation or regulations restricting its use are passed.

SIA and our members welcome the opportunity to work with you to identify the best ways to achieve the objective of safeguarding biometric and other personal data, ensuring it is captured, stored and utilized in a responsible manner than benefits Virginia citizens.

Sincerely,



Don Erickson

Chief Executive Officer

Security Industry Association

Staff contact: Drake Jamali, djamali@securirtyindustry.org