March 2, 2021

The Honorable Senator Smith
Chair, Judicial Proceedings Committee
2 East
Miller Senate Office Building
Annapolis, Maryland 21401

Written Testimony of SIA in Opposition to Senate Bill 587 Facial Recognition Privacy Protection Act

Dear Chairman Smith and Members of the Judicial Proceedings Committee:

On behalf of the Security Industry Association (SIA) I am writing to express our concerns with the proposed bill, which could negatively impact security applications of facial recognition and others that help protect public safety. SIA is a nonprofit trade association representing companies that provide a broad range of security products and services in the U.S and throughout Maryland, including 27 companies headquartered in our state. Our members include many of the leading developers of facial recognition software as well as companies offering products that incorporate this technology into a wide variety of government, commercial and consumer products.

Support for Ensure Responsible, Ethical Use
We believe all technology products must only be used for purposes that are lawful, ethical, and non-discriminatory. Since many advanced technologies both tremendous benefits and the potential for misuse, we support policies ensuring facial recognition it is only used for appropriate purposes and in acceptable ways.[1]

We support the intention of the bill to establish safeguards for government use of the technology. However, we believe its current structure as drafted will unnecessarily limited proven uses of the technology in ways that benefit Marylanders. Additionally, confusing terminology used throughout the bill will make it difficult for agencies to comply. Significant revisions would be required to address these issues.

Flawed Definition of Ongoing Surveillance
Public concerns about facial recognition technology have centered around law enforcement uses that might raise privacy and civil liberties concerns. However, the definition of "ongoing surveillance" appears to prohibit beneficial non-law enforcement uses in security systems used to protect state or local government facilities that may include areas open to the public, such as courthouses, and other public buildings. In these cases, security staff can be alerted to the presence of known individuals that are potentially dangerous, but the situation may not yet rise to the level of an emergency or where law enforcement should be involved. Additionally, much like how it is commonly used to unlock an electronic device, facial recognition enabled access control systems allow an authorized user to unlock a door or to access a secured area. In these instances, individuals could enter a premises multiple times or move throughout areas where their identity is connected to a particular place and time, potentially triggering the "ongoing surveillance" definition. Requiring a law enforcement purpose appears to take the technology off the table for these types of uses, which can

[1] See SIA's recommendations - https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/

positively impact the day-to-day safety and security of government personnel and members of the public visiting buildings and other government facilities.

Third-Party Testing

The requirement to provide an application programming interface (API) for the third-party testing could provide an unfair advantage to larger companies using software as a service business model – which may make free or trial versions publicly available. This requirement would disrupt agencies using technology that is not cloud based – like the Maryland Image Repository Systems (MIRS). It would also disadvantage small U.S. developers of facial recognition designed for government use, most of which have not made their technology publicly available to ensure it is only used for specific purposes. These developers should have the alternative option of participating in the National Institute of Standards and Technology (NIST) Facial Recognition Vendor Test (FRVT) program to meet this requirement. FRVT is the global gold standard for scientific, independent evaluations of facial recognition algorithm performance, including comprehensive measurements of differences across demographic groups. This program run by the federal government is available to developers at no cost.

A Note on the Science Regarding Facial Recognition Accuracy

Additionally, you may have heard the oft-repeated claim in media reports about racial "bias" in the technology. What this really refers to is the performance of the software in successfully comparing and matching photos of the same person. While it is true some versions of the technology have struggled to provide consistent performance across racial and other demographic factors, the claim that all facial recognition technology is less accurate across the board in matching photos of black and female subjects does not accurately reflect the current state of the science.

The National Institute of Standards and Technology (NIST), the leading scientific authority worldwide on the accuracy of facial recognition algorithms, found in its Demographic Effects report in 2019 that the leading facial recognition technologies it tested had "undetectable" differences[2] in accuracy across racial groups, after rigorous tests against millions of images. This would simply not be the case if demographic differences were "inherent" in the technology. These leading technologies are the same ones used in most of today's government and law enforcement applications, reaching the accuracy of fingerprint technology on many measurements, the gold standard for identification.

At the same time, lower performing algorithms among the nearly 200 that NIST tested did show measurable differences of several percentage points in performance across demographics – and this is an issue utmost importance to our industry which is continually addressed. It is critical to understand though, that most still had overall accuracy rates around 99% for all categories.

Widely misconstrued in media accounts is a 2018 report[3] where the claim is that it showed a 35% error rate for facial recognition on photos of black women. In fact, those researchers tested older "face gender classification technologies." Such software used to classify the race, gender, age, etc. of an unknown person in a photo – a technology that is not used for identification, or in law enforcement. Facial recognition, on the other hand, compares two or more images for similarities to help identify a specific person based on their unique facial features. By conflating these technologies and citing research that did not actually evaluate facial recognition accuracy at all, many media reports inaccurately assigned racial disparities[4] to facial recognition that really dealt with a different technology.

Americans Support Current Uses of Facial Recognition

[2] https://www.securityindustry.org/report/what-nist-data-shows-about-facial-recognition-and-demographics/
[3] https://www.media.mit.edu/projects/gender-shades/overview/
[4] https://itif.org/publications/2019/01/27/note-press-facial-analysis-not-facial-recognition

Finally, leading independent polling firm Schoen Cooperman Research recently conducted a nationwide poll on Americans' views of facial recognition technology, commission by SIA.[5] The survey found 68% of Americans believe facial recognition can make society safer, 70% believe it is accurate in identifying people of all races and ethnicities and 66% of believe law enforcement's use of facial recognition is appropriate. The results are consistent with other polling that indicates little public support for banning or heavily restricting this important technology.

On behalf of SIA and its members, we share the goal of ensuing responsible use of advanced technologies and would support policies ensuring that facial recognition is only used for appropriate purposes and in non-discriminatory ways. However, for the reasons above, we urge the Committee not to approve this bill in its current form. We stand ready to provide any additional information or expertise needed as you consider these issues.

Sincerely,

Respectfully,

Jake Parker
Senior Director, Government Relations
Security Industry Association
Silver Spring, MD
jparker@securityindustry.org

https://www.securityindustry.org/advocacy/policy-priorities/facial-recognition/

CC: Member of the Judicial Proceedings Committee

[5] https://www.securityindustry.org/2020/10/07/extensive-new-poll-finds-most-americans-support-facial-recognition/