March 10, 2022

The Honorable William Smith
Chairman
Senate Judicial Proceedings Committee
Maryland Senate
Annapolis, Maryland 21401

Written Testimony of SIA in Opposition to HB 762, Regarding Facial Recognition Technology

Dear Chairman Smith and Members of the Senate Judicial Proceedings Committee:

On behalf of the Security Industry Association (SIA) I am writing to express our concerns with Senate Bill 762, as currently written. SIA is a nonprofit trade association in Silver Spring, MD that represents companies providing a broad range of security products and services in the U.S and throughout Maryland, including more than 30 companies headquartered in our state. Among many other companies, our members include the leading providers of facial recognition software available in the U.S.

Support for Ensure Responsible, Ethical and Non-Discriminatory Use

We believe all technology products must only be used for purposes that are lawful, ethical, and non-discriminatory. Since many advanced technologies offer 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. Public concerns about facial recognition technology have centered around law enforcement and fears the technology might be used inaccurately or inappropriately, or in ways that raise privacy and civil liberties concerns. We believe establishing foundational safeguards in statute, combined with more detailed requirements in agency procedural rules, is the most effective approach to ensuring effective and accountable use of this technology by law enforcement. We support such policies consistent with *SIA's Principles for the Responsible and Effective Use of Facial Recognition Technology*,[1] and many comprehensive use policies put in place by leading agencies in Maryland and around the country.

SB 762 Should Establish Rules, Not Eliminate Current Capabilities

While the intention of the bill is to establish safeguards for law enforcement use of the technology, several provisions will also have the effect of eliminating current investigative tools being leveraged successfully by Maryland law enforcement. These are critical at a time of rising crime throughout the state, where shootings for example, have increased nearly 40% over the past year.

As written, the bill would deny investigators one method – but not others – of analyzing information that is already available to them. It's limitation to queries against mugshot or driver's license photos using "a single facial recognition technology," would only serve to hamper and delay investigations versus provide any public benefit. Investigators routinely query open-source information and records held by other agencies to help identify victims, witnesses or suspects that may have no prior criminal history or are from outside Maryland, especially when other methods result in dead ends. Related to this, the total prohibition on queries involving photos of minors will eliminate internet and dark web search tools essential to investigating human trafficking and child sexual exploitation. Additionally, while well

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

intentioned to limit “surveillance” use of the technology, the total prohibition on “live or real-time” use does not allow an exception for emergency situations when protecting lives demands being able to quickly identify a person of interest, such as during a terrorist attack. These harmful prohibitions simply must be addressed to avoid a significant negative impact on public safety in Maryland.

Support for Core Limitations and Transparency, Accountability Requirements
Facial recognition technology has been successfully utilized by Maryland law enforcement for over a decade, without a single instance of misidentification, misuse or false arrest. In fact, there are many documented success stories were the technology has been leveraged to help solve violent crime as well as assist citizens in need across our state, several of which have been shared with the Committee by Maryland law enforcement organizations. At the same time, there is a clear need for rules and other mechanisms that help address public concerns by helping ensure these technology tools are being leveraged in a lawful, effective, accurate and non-discriminatory manner that benefits our residents and communities. We support the core provisions of the bill that address primary public concerns as well as impose stringent transparency and accountability requirements on agencies using the technology, which:

- Prohibit law enforcement from using facial recognition match results as the sole basis to make an arrest, establish probable cause or make a positive identification.
- Ensure use of facial recognition technology in an investigation is discoverable in court proceedings.
- Exclude facial recognition results from use as evidence against a defendant.
- Prohibit use on images of individuals engaged in constitutionally protected activities, or based on their race, color, religious beliefs, sexual orientation, gender, disability and national origin.
- Require a statewide standard for agency policies on use of the technology.
- Require annual reporting and periodic audits from agencies using the technology that provide public transparency regarding how the technology is being used and the extent.

Third-Party Testing
Additionally, we understand that an amendment may be offered to the bill that would require providers of technology used by Maryland law enforcement to make the same technology available to any third party for testing. Not only would this make it difficult, if not impossible for law enforcement to be able to obtain and use needed technology, it is completely unnecessary as the accuracy of facial recognition technologies used in today’s law enforcement applications is evaluated by the U.S. government’s National Institute of Standards and Technology (NIST).

For over 20 years, the NIST Face Recognition Vendor Test Program, located here in Gaithersburg, MD, remains the world standard for objective, third party scientific evaluation, which provides an “apples to apples” comparison of the performance of facial recognition technologies. Despite claims that might be made to the contrary, the range of tests periodically conducted under the NIST program include those with relevance to law enforcement applications (notably the “Investigation Performance” tests), against images of varying quality (including mugshots, webcam, and “wild” images) and demographics, and using data sets similar to or larger in size than what would be available to law enforcement agencies (up to 12 million images). This federal program is used to validate technologies for U.S. government applications where highly accurate performance is critical to our national and homeland security.

Developers of facial recognition for law enforcement participate in the NIST program but do not make their technology publicly available, to ensure it is only used for intended purposes and does not fall into the wrong hands. For this reason, the requirement to provide an application programming interface (API) for third-party testing would specifically benefit specific vendors that already offer could-based “general purpose” software to the public. The result will be disruption for agencies using platforms that do not use cloud-based matching software – including Maryland’s current criminal records database. For these reasons, if a third-party testing requirement is added to the bill, we strongly urge that it specify participation in the NIST Face Recognition Vendor Test Program would satisfy this requirement.

The Accuracy of Facial Recognition

Calls for restricting use of the technology have often stemmed from misconceptions regarding its performance. While there is evidence that some, especially older versions of facial recognition technology have struggled to perform consistently across various demographic factors**,** the oft-repeated claim that it is *inherently* less accurate in matching photos of Black and female subjects simply does not reflect the current state of the science. In fact, the evidence *most* cited in the media is either irrelevant, obsolete, non-scientific or misrepresented.[2] An analysis of NIST test data from 2021 shows that each of the top 150 algorithms are over 99% accurate across Black male, white male, Black female and white female demographics, remarkable uniformity at high accuracy levels. For the top 20 algorithms, accuracy of the highest performing demographic versus the lowest varies only between 99.7% and 99.8%. For 17 of these algorithms, accuracy for white female, Black male and Black female are nearly identical at 99.8%, while they are least accurate for the white male demographic at 99.7%.[3]

The Case for Law Enforcement Use of Facial Recognition

In U.S law enforcement, facial recognition is used for a comparison search of records when the identity of the subject in an image is unknown, typically at the beginning stages of an investigation. It is used as a post-incident investigative tool to aid identification – not "surveillance." The purpose is to generate or follow leads only and not to make a positive identification. Investigators compare "probe" images (such as photos lawfully obtained from a crime scene, no different from latent prints) against images in an established database for possible matches. However, unlike fingerprint and DNA matching, any potential facial recognition match result is not considered evidence. If an analyst using the software determines an image from a database likely matches a submitted image, investigators should use other means outside of facial comparison to provide confirming evidence needed to establish probable cause.

If the technology is not available, investigators will search arrest records by physical traits such as race and gender, as well as arrest history and other info, to narrow down search fields and possible identities before a visual examination of the photos in the records. However, as the importance of limiting human bias in police work becomes increasingly clear, biometric technology makes identification processes faster and more accurate than relying only on human analysis, subject descriptions, broadcasting suspect lookouts, public announcements or soliciting anonymous tips. Leading research[4] tells us facial recognition is better at matching photos than humans can unassisted and that the highest accuracy results are achieved when combining technology and trained personnel.

Facial recognition has also been an indispensable tool for years in investigations of child sexual exploitation and human trafficking. There are several organizations that provide the technology to law enforcement investigators in Maryland as part of tools developed for searching online information to make identifications in these cases. For example, the Thorn organization's Spotlight tool is credited with helping rescue more than 17,000 children[5] from trafficking over the last four years. According to the National Child Projection Task Force,[6] facial recognition technology is key to its mission of bringing exploited children to safety and sexual predators to justice, as it assists investigations around the country.

[2] See - https://www.securityindustry.org/2021/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/

[3] ibid.

[4] https://www.nist.gov/news-events/news/2018/05/nist-study-shows-face-recognition-experts-perform-better-ai-partner

[5] https://www.thorn.org/spotlight/

[6] https://baltimore.legistar.com/View.ashx?M=F&ID=9438739&GUID=911C7E85-D97A-4325-A008-77AE42D1098E

Conclusion

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 SB 762 it its current form, and instead first work to correct the issues identified above. We stand ready to provide any additional information or expertise needed as you consider these issues.

Respectfully,

Jacob Parker

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