SECURITY INDUSTRY ASSOCIATION

February 18, 2022

The Honorable Luke Clippinger
Chairman
House Judiciary Committee
Maryland House of Delegates
Annapolis, Maryland 21401

Written Testimony of SIA in Opposition to HB 1046, Regarding Facial Recognition Technology

Dear Chairman Clippinger and Members of the Judiciary Committee:

On behalf of the Security Industry Association (SIA) I am writing to express our concerns with House Bill 1046, 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 developers of facial recognition software available in the U.S., as well as those that integrate this technology into government, commercial and consumer products.

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 over time. We support such policies consistent with *SIA's Principles for the Responsible and Effective Use of Facial Recognition Technology*,[1] and many thorough use policies put in place by leading agencies in Maryland and around the country.

HB 1046 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 eliminate 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. The bill'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.

As written the bill would prohibit one method – but not others – of analyzing the same available information. The prohibition on "live or real-time" use of the technology 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. Additionally, the complete prohibition on queries to help identify minors will eliminate Maryland law enforcement

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

capabilities essential to investigating human trafficking and child sexual exploitation. These harmful prohibitions in the bill simply must be removed to avoid a significant negative impact on public safety in Maryland.

Core Limitations and Transparency, Accountability Requirements

Facial recognition technology has been utilized by Maryland law enforcement for over a decade, without a single instance of misidentification, misuse or false arrest. Listed below in the appendix are just a few of many success stories. At the same time, there is a clear need for rules that help build public trust that technologies 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 to analyze images of individuals engaged in constitutionally protected activities, or based solely 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.**

Third-Party Testing

Additionally, we understand that an amendment may be offered 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 facial recognition technologies for use for law enforcement applications have been evaluated by the U.S. Government's National Institute of Standards and Technology (NIST). NIST tests and evaluates the speed, accuracy and performance of these technologies across a number of measurements including demographics. Algorithms utilized for these systems are periodically updated as necessary based on subsequent NIST evaluations. For over 20 years, the NIST Facial Recognition Vendor Test Program, located here in Gaithersburg, MD, remains the world standard for objective, third party scientific evaluation.

It is not clear what third parties are intended by the amendment or what objectivity or scientific expertise would be required. Developers of facial recognition for law enforcement use have generally not made their technology publicly available, to ensure it is only used for specific purposes and does not fall into the wrong hands. The requirement to provide an application programming interface (API) for third-party testing could also provide an unfair advantage to companies offering could-based "general purpose" software to the public. This requirement would disrupt agencies using technology that do not use cloud-based matching software – such as Maryland's mugshot repository.

The Accuracy of Facial Recognition Technology

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, nonscientific or misrepresented.[2] An analysis of NIST test data in 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,

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

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 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.

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 HB 1046 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

[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

APPENDIX - MARYLAND SUCCESS STORIES

VICTIM IDENTIFICATION

- Following police response to a **shooting/robbery in Prince George's County, Maryland**, the victim could not be identified and remained in critical condition. Therefore, notification to his family had not been made. Images obtained from the victim's cell phone screen were queried and a lead was developed. Using other known images of the candidate, it was learned the candidate had a birth mark on his temple this information was shared with investigating officers who confirmed that the birthmark was present. The investigators were then able to contact the victim's family, and they responded to the hospital. While the victim ultimately succumbed to his injuries, quick work by investigators aided by facial recognition technology enabled the family to make it to the hospital before he passed.

RESPONDING TO HEALTH EMERGENCIES

- Maryland-National Capital Park Police responded to a **health emergency involving an individual at the College Park Airport**, with no shirt, shoes or mask, stating that they wanted to "fly to outer space/the stars" but the subject left the area before units arrived. An officer was able to locate the subject after subsequent calls from concerned citizens nearby; however, they had no identification and could not communicate coherently. An image was taken of the subject and queried, producing a potential matching female identity. At first, officers on the scene believed it was not a match because the individual was male. Upon further investigations the lead proved correct, as the transgender man's identity was confirmed by his father, who had been contacted in another state. The man had reportedly not been the same since taking LSD the previous week. He was reunited with a family member and then taken to a local hospital for evaluation.

PREVENTING IDENTITY THEFT

- A string of **fraudulent vehicle purchases in Montgomery County, Maryland,** were carried out using information obtained via identity theft**,** harming both the identity victims and dealerships that lost property. The suspects had created false identification documents used to purchase the vehicles, combining their own image with the personally identifiable information of a victim. These images were queried, leads were developed, and identities were confirmed through additional investigation and five arrests were made. Some of the suspects were arrested when they arrived to pick up a vehicle, since by that time they had already provided their false identification with their true image.

SOLVING VIOLENT CRIME

- Local law enforcement investigated a **violent assault on public transportation in Maryland**. Images of the suspect and the incident were obtained through video surveillance footage from the coach. Information was disseminated to law enforcement partners seeking assistance with the case. A comparison was made with regional booking and arrest photos. An investigative lead was developed and provided to the investigating agency, which upon further investigation led to the arrest of the assailant who was identified by the victim.

FIGHTING ORGANIZED CRIME AND GANG VIOLENCE

- Local **law enforcement in Maryland requested assistance with a firearms trafficking investigation**, providing an image of a suspect. The image was run against regional booking and arrest photos, and a potential lead was developed. Upon further investigation, detectives positively identified the suspect and executed a search warrant that resulted in the seizure of drugs, guns and ammunition.

- A retailer reached out to law enforcement with information about an **organized theft crew that had been targeting stores throughout Virginia, D.C. and Maryland**. An image provided showed a male with a rose tattoo on his neck and a skull tattoo on his left hand. The image against regional booking and arrest photos and a potential lead with the same tattoos was developed. Upon further investigation, the individual was subsequently identified and charged.