February 8, 2023

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

Written Testimony of SIA in Opposition to SB 192, Regarding Facial Recognition Technology

Dear Chair Smith, Vice-Chair Waldstreicher 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 192 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 nearly 40 companies headquartered in our state. Among many other companies, our members include the leading providers of facial recognition software available in the U.S as well as other biometric technologies.

Support for Ensuring Responsible, Ethical and Non-Discriminatory Use
We believe all technology products must only be used for purposes that are lawful, ethical, and non-discriminatory. Many advanced technologies offer both tremendous benefits and the potential for misuse. We support policies ensuring facial recognition is only used for appropriate purposes and in acceptable ways, consistent with *SIA's Principles for the Responsible and Effective Use of Facial Recognition Technology*.[1]

We support rules that ensure this technology is being leveraged by law enforcement investigators in a way that is lawful, effective, accurate and non-discriminatory. For over a decade, Maryland communities have benefitted from effective use of these tools by agencies throughout the state to quickly develop leads in criminal investigations as well as for public welfare purposes, without a single instance of misidentification or misuse – and every indication it is being used appropriately and effectively. Detailed in the attachment below are just some examples documented by Maryland law enforcement agencies of many successes using the technology, showing the clear benefit public safety.

At the same time, some public concerns have surfaced over whether the technology is accurate, and how it might be used in the absence of uniform rules. We believe establishing foundational safeguards in statute, combined with more thorough requirements in agency procedural rules, is the most effective approach to building greater public trust and ensuring effective and accountable use of this technology by law enforcement over time. Interest in such an approach is growing, as some states and localities that briefly experimented with bans on the technology have quickly reversed course to overturn blanket restrictions once the impact became clear – including Virginia and the City of New Orleans in 2022.

There is growing consensus among law enforcement professionals on the necessity of facial recognition tools, as well as appropriate processes and rules surrounding their use. However, it is essential that these are based on an accurate understanding of the technology and its place within existing investigative procedures, while drawing from the best available subject matter expertise and existing polices.

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

Support for Greater Transparency and Uniform Rules – Not Eliminate Current Capabilities
We are concerned that provisions in this bill would extend beyond these objectives to eliminate or degrade the effectiveness of essential investigative tools, with a significant negative impact on public safety. For example, limiting agencies to "a single facial recognition technology" to query mugshots and local driver's license photos – and only to investigate a narrow set of crimes – will serve only 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 SB 192, inappropriately prohibits queries involving photos of minors, which would bar current internet and dark web search tools essential to investigating human trafficking and child sexual exploitation. Additionally, 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. Such provisions would be harmful to public safety and are completely unnecessary to the aims of achieving greater transparency and establishing core rules for use.

Consensus on Core Rules
The Committee should instead consider establishing a statewide policy and core rules for which there is widespread consensus among Maryland law enforcement professionals and other community stakeholders, which will build public trust, guard against the possibility of future misuse and fully preserve proven benefits. This includes:

- Establishing a statewide standard for state and local agency policies on authorized use of the technology.
- Prohibiting use of facial recognition match results as the sole basis to make an arrest, establish probable cause or make a positive identification.
- Prohibiting use of the technology to identify individuals engaged in constitutionally protected activities, or based solely on their race, color, religious beliefs, sexual orientation, gender, disability, national origin and other classifications protected by law from discrimination.
- Ensuring potential match results from the software can never be used as evidence against a defendant.
- Requiring an agency program coordinator responsible for policy adherence and routine usage audits.

Understanding Law Enforcement Use of Facial Recognition Technology
In U.S. law enforcement, facial recognition technology is typically used in the beginning stages of a criminal investigation, when there is a lawfully obtained image of a person of interest who cannot be identified in a timely manner by other means. This is a post-incident investigative tool to aid identification – not "surveillance." The purpose is to generate or follow leads only, not to confirm an identity. The image can be from any available source that provides adequate quality for comparison, such as security camera footage or cell phone cameras. This photo is compared against an available database of images using facial recognition software, which returns any potential match candidates over a preset similarity score threshold. Personnel then determine whether any returned matches represent leads that should be investigated further. At that point, other investigative techniques outside of facial comparison are used to find and confirm further information needed to positively identify a person and, if a suspect, needed to establish probable cause to make an arrest or obtain a search warrant.

It's critical to understand this investigatory use in context. Other non-technological methods are also routinely used to search for leads using the same type of photo, such as suspect lookouts, public announcements or soliciting anonymous tips. Any leads that result must be confirmed in the same manner. However, as the importance of limiting human bias in police work as well as unnecessary interactions with citizens becomes increasingly clear, biometric technology makes the process of generating and investigating leads faster and more accurate than relying only on human analysis alone. This is also one reason why facial recognition has 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 help make identifications in these cases. For

example, the Thorn organization's Spotlight tool is credited with helping rescue more than 17,000 children[2] from trafficking over the last four years.

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. Unfortunately, the claims *most* cited in media accounts are either irrelevant, obsolete, nonscientific or misrepresented.[3] Most facial recognition algorithms used in systems available to law enforcement have been 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 has remained the world standard for objective, third-party scientific evaluation, providing an "apples to apples" comparison of the performance of facial recognition technologies. The range of tests periodically conducted under the NIST program include those with relevance to law enforcement applications, including use of image sets from operational settings (actual mugshots) and of varying quality (webcam, etc.) 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.

NIST has documented massive improvements in overall accuracy in recent years. Even five years ago, it noted[4] the software was at least 20 times more accurate than it was in 2014, and later found "close to perfect" performance[5] by high-performing algorithms with "miss rates" against a database of 12 million images averaging 0.1%, as well as "undetectable" differences in accuracy across racial groups among top-tier technology after rigorous tests against millions of images. On this measurement, the accuracy of facial recognition is reaching that of automated fingerprint comparison,[6] which is generally viewed as the gold standard for identification. A more recent analysis of NIST test data in 2022 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%.[7]

Conclusion

We share the goal of ensuing responsible use of advanced technologies and support policies ensuring that facial recognition is used for appropriate purposes and in non-discriminatory ways. However, for the reasons above, we urge the Committee not to approve HB 223 in its current form. We stand ready to provide any additional information or expertise needed as you consider these issues.

Respectfully,

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

[2] https://www.thorn.org/spotlight/
[3] https://www.securityindustry.org/2021/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/
[4] https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities
[5] https://www.nist.gov/system/files/documents/2019/09/11/nistir_8271_20190911.pdf#page=49
[6] https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8034.pdf
[7] https://www.securityindustry.org/2021/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/

MARYLAND SUCCESS STORIES

Shared by Maryland law enforcement agencies utilizing facial recognition technology[8]

VICTIM IDENTIFICATION

- Following police response to a **shooting/robbery in Prince George's County, Maryland**, and 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

- Local law enforcement 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.

- **An unknown person in Annapolis, MD was posting plans to commit suicide on open sources.** Reports were made to the police by concerned persons who saw this post. Due to what was written, police believed a suicide was eminent and attempted to identify this person using a still image from open sources. This image was used with facial recognition technology and generated a lead through a driver's license photo. Through further investigation, the suicidal person was identified and the police and a crisis team were sent to the person's address. Police were able to locate the suicidal person and they were provided with assistance.

SOLVING SEX CRIMES

- In 2016 in **Glen Burnie, MD** a police officer with the Metropolitan Police Department in Washington, DC created a social media account where he exchanged approximately 53,000 messages with thousands of other users. **The officer used his account to send messages to other users, including minors, offering to pay them to engage in specific sex acts with him and to negotiate over the prices he would pay for sex.** He exchanged approximately 200 texts and messages with a 14-year-old girl. In the messages, he offered to pay the victim to engage in sex acts with him. In 2017, he exchanged approximately 54 messages with a 15-year-old girl. In the messages, he also offered to pay the second victim to engage in sex acts with him. In both exchanges, he discussed the sex acts they would engage in, and where they would meet. Both victims were

[8] See- https://mgaleg.maryland.gov/cmte_testimony/2022/jpr/1HbG3DHhu0qHaElQQEYRJV6xC0o9TglCS.pdf

students in the ninth grade at the time of the offenses. On January 9, 2017, in the back seat of his vehicle, he pointed a handgun at the second victim and demanded that she give him the money he had just paid her. After the victim reported this to police, facial recognition and images from social media were used to develop a lead in determining his identity. Through further investigation, the officer was identified, and he was federally indicted on charges of sex trafficking of minors and enticement of minors to engage in prostitution, involving sexual contact with two minor girls. He ultimately plead guilty in this case and his employment as a police officer was terminated.

- **In 2021, an unknown subject went to the front door of a residence and began sexually stimulating himself in front of a security camera.** The use of facial recognition by Montgomery County Police Department provided an investigative lead – a person that had conducted the same behavior in front of a 72-year-old female neighbor two years prior. Upon further investigation, the case resulted in a confession by the suspect and criminal charges related to the indecent exposure.

- **In 2021, an unconscious subject was reported in Montgomery County.** Responding officers found a disoriented pregnant female subject who was unable to recall anything from the past two days. Eventually, the female victim was able to recall potentially being drugged, and later, an unknown suspect forcing oral and vaginal sex. Facial recognition was used to generate a lead from a photo of the suspect available from security cameras nearby. This case is still ongoing as of this writing, so no further information can be provided.

SOLVING VIOLENT CRIME

- **Local law enforcement investigated a violent assault on public transportation in Baltimore.** Images of the suspect and the incident were obtained through security camera footage from the coach. Information was disseminated to law enforcement partners seeking assistance with the case. A comparison was made with a law enforcement database, and an investigative lead was developed and provided to the investigating agency. Upon further investigation it led to the arrest of the assailant who was identified by the victim.

- **In Annapolis, MD the "Capitol Gazette Killer" Jarrod Ramos** was angered by a story the *Capital Gazette* ran about him in 2011 and brought a lawsuit against the paper for defamation, which a judge later dismissed. In 2018, **Ramos entered the newspaper's headquarters in Annapolis, Maryland with a shotgun and killed five employees, leaving two others critically injured**. Anne Arundel County Police faced a perfect storm of problems when they took the suspected gunman into custody: the man had no identification, he wouldn't speak to investigators, and a fingerprint database was not immediately returning any matches. Detectives obtained an image of Ramos and used facial recognition which generated a lead in the case. Through further investigation, detectives were able to positively identify Ramos and search warrants were conducted at this residence. He plead guilty in the case and was sentenced to five consecutive life sentences.

- **In 2015, two suspects armed with guns walked into a Towson liquor store and announced a robbery,** taking aim at a 68-year-old clerk. The clerk, fearing for his life, pulled out a gun and shot one of the people robbing the store, who was later pronounced dead at the scene. The second person involved in the robbery got away. The police then went to work to identify the second suspect. Through social media, detectives were able to find an image of a person of interest who was a friend of the other person involved in the robbery. The police entered this photograph into facial recognition which returned a tentative lead. Through further investigation the second person involved in the

armed commercial robbery was positively identified. He was successfully prosecuted and convicted of attempted robbery. He was sentenced to twenty years in jail.

- **In 2020, a Facebook user claimed on open-source media he was ready to attack and kill law enforcement ("tyrants") for "Liberty or Valhalla."** The same Facebook user also commented online on a Montgomery County Police press release and implied utilizing hydrofluoric acid containers above entry points to injure law enforcement. The subject later went on Facebook Live and announced his intent to livestream the execution of a law enforcement officer in Texas. Facial recognition was used by Montgomery County Police to quickly generate a lead from open-source photos. Through additional investigation, investigators were able to identify this individual and located him in Texas. After a lengthy pursuit, he was arrested and charged with Terrorist Threats against an Officer, Evading Detention with a Vehicle, and Unlawfully Carrying a Weapon.

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 a law enforcement database 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 unique tattoos on his neck and left hand. Facial recognition was used to generate a lead in the case. Upon further investigation, the individual was subsequently identified and charged.

- **Throughout 2019 and 2020, local law enforcement conducted a homicide/gang investigation involving a violent group responsible for multiple homicides, drug distribution, kidnapping, and robbery in Anne Arundel County.** Digital images of persons of interest were obtained and with the assistance of facial recognition, law enforcement was able to generate leads regarding three individuals involved. Through further investigation, individuals were positively identified and probable cause was established to obtain a wiretap warrant. Though subsequent monitoring of communications, law enforcement was able to prevent at least three shootings, as well as interrupt a kidnapping. As a result of the investigation over a dozen people were indicted and successfully prosecuted, multiple firearms were recovered including an assault rifle, drugs and a significant amount of U.S. currency were also seized.

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 FIREARMS TRAFICKING

- Local **law enforcement in Maryland requested assistance with a firearms trafficking investigation in Prince George's County**, providing an image of a suspect. The image was run against a law enforcement database 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.

SOLVING BURGLARIES

- **In Crownsville, MD officers responded to a residential burglary captured on a home security camera.** Using facial image from the video, officers queried a law enforcement database using facial recognition which provided a lead in the case. Upon further investigation, the person in the video was positively identified. He was charged and convicted of the burglary and other charges.

SOLVING DAMAGE TO MULTIPLE POLICE VEHICLES

- Maryland National Capital Park Police had a cruiser tampered with and images from nearby security cameras were obtained. Investigators searched Prince George's County Police data and found similar cases. A good facial image of the person of interest was obtained from security camera footage, and use of facial recognition generated a lead. Upon further investigation, the suspect was subsequently identified by investigators and charged. The suspect was connected to over 20 cases in five jurisdictions: Prince George's County Police, Park Police, Montgomery County Police, Charles County Sheriffs and Metropolitan (DC) Police.

Additional Success Stories from Across the U.S.

Just some of many similar examples

EXONORATING THE INNOCENT

- A Florida man **falsely accused of vehicular homicide was exonerated** only after facial recognition technology made available to public defenders was used to help identify and locate a key witness to the scene of a fatal crash, who confirmed the man was a passenger and not the driver of the vehicle, who was killed in the incident.[9]

- A witness in a **gang-related assault case in northern Virginia** provided cell phone photos of the suspects to police detectives working the case. One of the photos of an unknown suspect was queried against regional booking and arrest photos and an investigative lead was developed. Upon further investigation and confirmation of the identity of the suspect, it was found that the individual was in jail in another jurisdiction at the time of the assault. Use of technology in this case helped quickly clear the individual and avoided unnecessary contact from law enforcement.

FIGHTING HUMAN TRAFFICKING

- Local law enforcement investigators were working to identify a **subject suspected of child sex trafficking in Fairfax County**. Using a photograph from social media of the person believed to be the suspect, a query

[9] https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html

against regional booking and arrest photos resulted in a lead, aiding in the progress of a critical child sex trafficking investigation.[10]

- In California, a law enforcement officer saw a social media post about a missing child from the National Center for Missing and Exploited Children. The officer used the Spotlight investigative tool to return a list of online sex ads featuring the girl. As reported in *Wired*,[11] the **girl who was rescued had been "sold for weeks,"** and the officer's actions initiated a process that "recovered and removed from the girl from trauma."

- Use of facial recognition tools by Kansas Law enforcement u**ncovered the largest forced labor trafficking case in U.S. history**, all through identifying cases of driver's license fraud in the state's database**.**[12]

BRINGING CHILD SEXUAL PREDATORS TO JUSTICE

- A **15-year-old girl in Scranton, Pennsylvania**, was sexually assaulted by an adult male she met online. Beyond seeing him in person, the only additional information she had was from his online profile. Police were able to use facial recognition on one of the digital images to provide some potential matches from a state database, from which the victim was able to identify a likely match. After additional investigative work, authorities obtained a search warrant for the home of the identified suspect, who later admitted to the crime.[13]

- A man accused of **sexually assaulting a 10-year old girl** was apprehended in Oregon after a 16-year manhunt. Using facial recognition technology, the Federal Bureau of Investigation (FBI) was able to identify the suspect after a positive match was found when the suspect sought to acquire a U.S. passport.[14]

- Facial recognition technology was used to help **locate and apprehend a convicted pedophile** who had been on the run for 14 years, returning him to New Mexico to face justice.[15]

CATCHING A SUSPECTED SUBWAY TERRORIST

- New York City Police Department (NYPD) detectives used facial recognition technology to identify a man who sparked terror by leaving a pair of rice cookers in the Fulton Street subway station. Detectives pulled still images of the suspect from security footage and used facial recognition software to compare them to NYPD's arrest database. The system returned several hundred potential matches, and after multiple stages of review and confirmation using other methods, the suspect was identified in just one hour.[16]

FINDING A KILLER TARGETING LGBTQ+ VICTIMS

- Three members of the LGBTQ+ community were shot and killed by a man at a local home in Detroit, Michigan. The Detroit Police used facial recognition, in combination with other investigative tools, to help identify the suspect based on video images from a nearby gas station.[17]

---

[10] https://www.pilotonline.com/opinion/columns/vp-ed-column-parker-0630-20220629-gt5azrqsa5dxrhiaqczis3pdrm-story.html
[11] https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/
[12] https://www.kansascity.com/news/local/article336253/Kansas-Revenue-Department%E2%80%99s-facial-recognition-software-helps-investigators-catch-scores-of-criminals.html
[13] https://apnews.com/e0a56374618840cf88e78637428d63d0
[14] https://nakedsecurity.sophos.com/2017/01/20/alleged-child-molester-caught-after-18-years-thanks-to-facial-recognition/
[15] https://www.fbi.gov/news/stories/long-time-fugitive-neil-stammer-captured/long-time-fugitive-neil-stammer-captured
[16] https://nypost.com/2019/08/25/how-nypds-facial-recognition-software-ided-subway-rice-cooker-kook/
[17] https://www.detroitnews.com/story/news/local/detroit-city/2019/06/06/detroit-man-charged-triple-lgbtq-killings/1373342001/