SB192 Position Paper.pdf
Uploaded by: Andrew Northrup
Position: FAV

MARYLAND OFFICE OF THE PUBLIC DEFENDER

NATASHA DARTIGUE
PUBLIC DEFENDER

KEITH LOTRIDGE
DEPUTY PUBLIC DEFENDER

MELISSA ROTHSTEIN
CHIEF OF EXTERNAL AFFAIRS

ELIZABETH HILLIARD
ACTING DIRECTOR OF GOVERNMENT RELATIONS

POSITION ON PROPOSED LEGISLATION

BILL: SB192 Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions

FROM: Maryland Office of the Public Defender

POSITION: Favorable

DATE: 02/07/2023

Thank you Mr. Chairman, Senator Sydnor and distinguished members of the committee for allowing us to weigh in on this bill. The Maryland Office of the Public Defender's position on this bill is Favorable..

Since this bill was introduced last year the need to regulate this technology has become more urgent. In December, I became aware of the first demonstrable misidentification by this technology, and I am afraid that this may be the tip of the iceberg.

It is important to recognize that this technology is new, and the standards for its use are still being developed. Protocols and procedures for using this technology in a reliable and accurate manner have yet to be fully developed.

The act of taking a still surveillance photograph and comparing it to a database of individuals requires a number of tasks for which the analyst is provided little or no guidance. As everyone knows, the quality of a surveillance video can vary greatly based upon a number of factors which may include:

1. Quality of the camera
2. Lighting
3. Distance of subject from the camera; and
4. Angle of the face in relation to the camera

Poor quality videos can lead to inaccurate candidate lists. Currently there are no standards as to what the quality of the video must be before it is suitable to be uploaded and searched by the algorithm.

While this discusses the input into the machine, there are two times when human beings make decisions that affect the analysis, and these are decisions that individuals are not qualified to make.

First, human beings decide how and when images are processed. If an image is a high-quality head on shot from a camera, very little processing may be needed. However, for lower quality photographs, the photographs may be lightened, darkened or be processed in more involved ways with tools like

Photoshop. There are currently no standards or guidelines as to how or the amount of processing that can be applied to an image before it is uploaded or as to how processing affects the candidate list generated by the algorithm. (As an aside, I can say that when conducting fingerprint searches, the way that a fingerprint image is processed before uploading to be searched by AFIS can change the candidate lists dramatically.)

The second time is when a person looks at the list of candidates to determine if any of them is the correct person. While this may seem counterintuitive, we are not as good at recognizing faces as we would like to believe. While we like to think that any layperson can look at an image and select the proper candidate, that the task is not so straightforward. Studies show that even people who are experienced and trained are far from perfect. There are currently no standards for training and the individuals making the decisions about facial recognition do not take proficiency tests to determine their ability to complete the test reliably and accurately.

The bottom line is that the technology currently is not, nor can it be used in an accurate and reliable manner for the reasons stated above.

Ideally this technology would not be used until it has been thoroughly validated and vetted. However, short of that, this bill is an important first step to regulate this area of technology with a high potential of misuse.

For these reasons, the Maryland Office of the Public Defender urges this Committee to issue a favorable with amendments report on Senate Bill 192.

Submitted by: Maryland Office of the Public Defender, Government Relations Division.

Authored by: Andrew Northrup, Forensics Division, (312) 804-9343, andrew.northrup@maryland.gov.

SB0192 Facial Recognition Technology FAV.pdf
Uploaded by: Cecilia Plante
Position: FAV

MARYLAND LEGISLATIVE COALITION

TESTIMONY FOR SB0192

Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions

Bill Sponsor: Senator Sydnor
Committee: Judicial Proceedings
Organization Submitting: Maryland Legislative Coalition
Person Submitting: Cecilia Plante, co-chair
Position: FAVORABLE

I am submitting this testimony in favor of SB0192 on behalf of the Maryland Legislative Coalition. The Maryland Legislative Coalition is an association of activists - individuals and grassroots groups in every district in the state. We are unpaid citizen lobbyists, and our Coalition supports well over 30,000 members.

In today's world, we seem to be edging towards a more Orwellian world where too much of a person's privacy is handed over to electronic monitoring devices. It is in many ways chilling to know that someone with the right access can monitor your whereabouts as you go through your day. With all the new technology, there must be limits, where the software can be used effectively for its intended purpose, but without stomping all over the rights of individuals who are ancillary to that purpose.

In that vein, our members welcome the restraints placed on the use of facial recognition technology in this bill. It limits the use of the results generated by facial recognition technology as evidence to cases where it is used in connection with a warrant or preliminary hearing in a criminal matter. Facial recognition may not be used as the sole basis to establish probable cause. Further, the bill significantly limits when the technology can be used during investigations and in analysis of videos or recordings of members of the public who are not the target of criminal investigations.

We believe these are common-sense measures that will not harm the usefulness of the technology, while protecting the rights and privacy of the public.

We support this bill and recommend a **FAVORABLE** report in committee.

Sydnor_SB 192 Testimony Fav.pdf
Uploaded by: Charles E. Sydnor III
Position: FAV

CHARLES E. SYDNOR III, ESQ.
Legislative District 44
Baltimore County

Judicial Proceedings Committee
Executive Nominations Committee

Joint Committees
Administrative, Executive, and Legislative Review
Children, Youth, and Families

Senate Chair
Legislative Ethics

Chair
Baltimore County Senate Delegation

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

James Senate Office Building
11 Bladen Street, Room 216
Annapolis, Maryland 21401
410-841-3612 · 301-858-3612
800-492-7122 *Ext.* 3612
Charles.Sydnor@senate.state.md.us

Testimony Regarding SB 192:
Criminal Procedure – Facial Recognition Technology –
Requirements, Procedures, and Prohibitions
Before the Judicial Proceedings Committee
February 8, 2023

Good afternoon Chairman Smith, members of the Judicial Proceedings Committee.

The development of Facial Recognition Technology "(FRT)" began in concept over 50 years ago as a method of computer application. As it evolved through many uses and applications, FRT is no longer an issue that can be fully classified as a new process. Facial Recognition is currently offered by a variety of venders and utilized in private cell phones, computer access applications and other social media outlets (Facebook, Twitter, etc.) Facial recognition systems are also utilized throughout the world today by governments, law enforcement agencies and private companies according to the U. S. Government Office of Accountability. These commonly used systems represent additional access points for this technology; a technology that has gone without significant regulation.

By the time you read this sentence, 20,000 images will be uploaded to social media.[1] There is an ocean of pictures out there and facial recognition technology enables users to find face template matches rapidly.[2] In this ocean of data, what is there to stop law enforcement from going on a fishing expedition? While facial recognition can and will help enforce justice, we need to balance safety concerns against the very real threat that law enforcement will cast a net whenever they

[1] Facial Recognition Technology: Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees. *www.gao.gov* Retrieved September 5, 2021.
[2] Matthew Doktor, *Facial Recognition and the Fourth Amendment in the Wake of Carpenter v. United States*, 89 U. CIN. L. REV. 552, 552 (2021).
[2] Ari B. Rubin, *A Facial Challenge: Facial Recognition Technology and the Carpenter Doctrine*, 27 RICH. J.L. & TECH. 1, 6 (2021).

need a catch. SB 192 sets forth standards that will provide some level of accountability and control over when the facial recognition net is cast.

Undoubtedly there are benefits to use of facial recognition: preventing and addressing unlawful entry at ports,[3] as well as monitoring high-security events, such as the Super Bowl.[4] In the local law enforcement context, police can use FRT to identify a suspect incident to arrest;[5] or may use FRT to determine an unknown person's identity based on a photo of him or her at a crime scene.[6]

However, FRT has also been used maliciously. It was reported in the LA Times "Facial recognition software developed by China-based Dahua, one of the world's largest manufacturers of video surveillance technology, purports to detect the race of individuals caught on camera and offers to alert police clients when it identifies members of the Turkic ethnic group Uighurs.[7] And given this state's movement towards adoption of police body cameras, we have to consider how police using them can quickly and easily amass probe photos of protesters, thus creating a chilling effect. Anyone who attends a protest may be subject to inclusion in the perpetual FRT lineup.[8]

In 2021 this committee passed SB 587 to establish a Task Force on Facial Recognition Privacy Protection. That bill ultimately did not make its way thru the legislative process, but I reached out to everyone who we had included in that legislation and asked them to work with me and Delegate Moon on legislation for this session. Our workgroup consisted of 14-members which included of law enforcement, the Department of Public Safety and Corrections, the Maryland States Attorney Association, the Office of the Public Defender, trade group representative and a vendor, academic researchers, and civil rights advocates. We met virtually to discuss issues connected with the use of facial recognition technology. Invited contributors consisted of everyone from ordinary citizens with concerns, and a researcher from Australia. For more than five months our workgroup met over ten times with the objective of adopting a foundational set of statewide requirements for law enforcement agencies using FRT, and to address the key public concerns about the technology, while preserving the public safety benefits of the technology. Those discussions resulted in last year's SB 762, and the introduction this year of SB 192.

SB 192 sets guardrails for the usage of FRT systems by law enforcement. SB 192 provides that FRT can be used as an investigative tool,[9] and limits the types of crimes that can be investigated using FRT.[10] To limit falsely identifying someone, SB 192 also limits the databases that can be used by law enforcement agencies to those government databases which were disclosed during the

---

[3] *Id.* at 14.
[4] *Id.*
[5] *Id.* at 19.
[6] *Id.* at 20.
[7] Dahua facial recognition touts 'real-time Uighur warnings' - Los Angeles Times (latimes.com)
[8] *Id*. at 16.
[9] however, it cannot be utilized alone as the sole basis to establishment of probable cause in a court proceeding. Other evidence must be used to support probable cause.
[10] This includes crimes of violence, human trafficking and criminal acts involving national security or safety threats.

workgroup meetings to motor vehicle identification images and mugshot photos maintained by local, state or federal law enforcement agencies.

For the greater part of the time our workgroup met, we worked under the assumption that the Department of Public Safety and Correctional Services had the only FRT system in use in Maryland. Therefore, SB 192 assigns it with the responsibility of contracting for and approving a single FRT vendor, for use by all state law enforcement agencies; review and testing of the application programming interface of the vendor; requires the vendor to enable testing of its software for accuracy and mitigation for any performance differences as they apply across various population groups.

As suggested by some of our participants, SB 192 establishes training programs that will be developed and administered to provide for proficiency testing for law enforcement personnel who uses FRT. Additionally, each agency must maintain appropriate records regarding its use of FRT and will annually report its uses to the Governor's Office of Crime Prevention, Youth & Victims Services.

In conclusion, I recognize that facial recognition technology is a complex investigative tool whose value is growing as the practical applications expand. We need to take this strong initial step towards developing and maintaining standards and guidance for the uses of this useful and innovative technology. FRT offers real benefits to our communities and to the law enforcement agencies who utilize it. Transparency, accountability, and civil protections against human bias characteristics need to be developed and maintained now and evolve appropriately as the utilization evolves in its practical applications. For these reasons I urge the Committee to vote in favor of SB 192.

Microsoft FAV Testimony SB 192.pdf
Uploaded by: Keith Walmsley
Position: FAV

Testimony in Support of SB 192: Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions

February 8, 2023

Chairman Smith and distinguished members of the Judicial Proceedings committee, we are writing to offer our support for SB 192 which focuses on law enforcement use of facial recognition technology. We wish to thank Senator Sydnor for his sustained attention to this important issue.

Microsoft believes that facial recognition can provide benefits to society, including by securing devices, assisting people who are blind or with low vision access to more immersive social experiences, and advancing public safety.

However, we also recognize that without clear guardrails that have the force of law, facial recognition technology creates potential risks, including in relation to potential bias and risk of unfair performance, potential new intrusions into people's privacy, and possible encroachment on democratic freedoms and human rights.

Microsoft is clear-eyed about these potential risks. We have enacted internal safeguards, including implementing Facial Recognition Principles[1] and developing our Face API Transparency Note, providing information to customers around appropriate and responsible use of our systems[2]. In addition to enacting these safeguards, Microsoft continues to believe frameworks must be developed that guide responsible use. This need is particularly acute for government and law enforcement use of facial recognition given the consequential nature of the decisions made by these organizations.

We support the way in which the bill lays out provisions for transparency and accountability around how law enforcement use facial recognition and encourage you to continue to advance this important legislation.

Thank you for your consideration, we urge a favorable report.

Sincerely,

Owen Larter
Director, Responsible AI Public Policy
Microsoft Corporation

[1] Microsoft, *Six Principles for Developing and Deploying Facial Recognition Technology*, https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2018/12/MSFT-Principles-on-Facial-Recognition.pdf.
[2] Microsoft AI, *Transparency Note: Azure Cognitive Services: Face API* (2019), https://azure.microsoft.com/mediahandler/files/resourcefiles/transparency-note-azure-cognitive-services-face-api/Face%20API%20Transparency%20Note%20(March%202019).pdf.

MCPA-MSA_SB 192 Facial Recognition _Oppose.pdf
Uploaded by: Andrea Mansfield
Position: UNF

Maryland Chiefs of Police Association
Maryland Sheriffs' Association

MEMORANDUM

TO: The Honorable William C. Smith, Jr., Chairman and
Members of the Senate Judicial Proceedings Committee

FROM: Darren Popkin, Executive Director, MCPA-MSA Joint Legislative Committee
Andrea Mansfield, Representative, MCPA-MSA Joint Legislative Committee
Natasha Mehu, Representative, MCPA-MSA Joint Legislative Committee

DATE: February 8, 2023

RE: **SB 192 Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions**

POSITION: **OPPOSE**

The Maryland Chiefs of Police Association (MCPA) and the Maryland Sheriffs' Association (MSA) OPPOSE SB 192.

The MCPA and MSA fully support strict guardrails and audit protocols to mitigate the risk of impartial and biased law enforcement and misuse of the technology. However, as currently drafted, SB 192 contains several provisions that would unacceptably impact public safety in Maryland as well as hamper effective implementation of the requirements.

1. **SB 192 limits the types of crimes to be investigated to crimes of violence, human trafficking, and those presenting a substantial and ongoing threat to public safety or national security. (Page 3, lines 7-15)**

The successful use of facial recognition technology in Maryland has aided in the identification of people whose images have been recorded on-camera committing robberies, burglaries, car jacking's, assaults, rapes, sexual assaults, shootings, homicides, kidnappings, hate crimes, human trafficking, sexual exploitation, threats of mass violence and other serious crimes. The technology has also been used to identify missing persons, deceased persons, incapacitated persons who can't identify themselves and to mitigate an imminent threat to health or public safety (e.g., to thwart an active terrorism scheme or plot). Striking this limitation will assist law enforcement with solving the other types of crimes listed as well as aid vulnerable populations.

532 Baltimore Boulevard, Suite 308 Westminster,
Maryland 21157
667-314-3216 / 667-314-3236

2. **Limiting databases to be matched only to driver's license and IDs by MVA's and databases of mug shots. (Page 4, lines 5-11)**

A further limitation in the bill is only allowing queries to the Maryland Motor Vehicle Administration or other state Department Motor Vehicle images and mug shots maintained by local, state or federal law enforcement agencies. Individuals committing crimes in Maryland may not have a mug shot or a driver's license. They could be from out of state, another the country, or too young to have one. This limitation also extends to the search for missing children, human trafficking victims, missing adults, etc. The limitation prohibits the technology from accessing this state or other state's sex offender websites, the Maryland and National Center for Missing and Exploited Persons images, wanted posters or other images posted by law enforcement or families. Striking these limitations will allow law enforcement investigators to use FRT to possibly identify individuals with no prior criminal history, do not have an ID card or driver's license, non-MD residents or minors, who are suspects or unidentified victims.

3. **Limits use to just one single facial recognition technology reviewed and approved by DPSCS. (Page 6, lines 24-25)**

Due to the complexity of investigating crimes such as human trafficking and child sexual exploitation, using more than one facial recognition system to conduct searches of databases beyond driver's license, identification cards and booking photos may be necessary. People who engage in criminal activity often travel from out of state to commit crimes. Limiting use to a single facial recognition technology would prevent law enforcement from leveraging other legally obtained photos such as photos from other states and open-source photos which could assist with the identification of human trafficking/sexual exploitation victims, and individuals traveling from far outside the area to commit crime, as we saw with the unrest at the U.S. Capitol on January 6 last year.

The MCPA and MSA is aware there may be an amendment offered to the bill to require the technology used by Maryland law enforcement to be made available to any third party for testing. MCPA and MSA do not support this amendment. The majority of facial recognition systems in use for law enforcement applications have algorithms which have been evaluated by the National Institute of Standards and Technology (NIST) for matching efficiency and accuracy, which includes an evaluation of the accuracy of the algorithm across demographics. Algorithms utilized for these systems are periodically updated as necessary based on subsequent NIST evaluations. The NIST Facial Recognition Vendor Test Program, located here in Gaithersburg, MD is already the world standard for independent, scientific evaluation of the technology.

Facial recognition is a valuable time savings investigatory tool and MCPA and MSA agree there should be safeguards in place for government use of the technology to ensure there is no intrusion on constitutionally protected activities. However, SB 192 as it stands limits the use of the technology, prevents human trafficking and juvenile victims from being identified and restricts law enforcement's ability to effectively investigate cases. Unless the limitations described above are addressed, MCPA and MSA must oppose SB 192 and respectfully request an UNFAVORABLE Committee report.

532 Baltimore Boulevard, Suite 308 Westminster,
Maryland 21157
667-314-3216 / 667-314-3236

Written Testimony Bekah Charleston (MD SB 192).doc
Uploaded by: Bekah Charleston
Position: UNF

WRITTEN TESTIMONY OF BEKAH CHARLESTON

Before the Maryland Senate Judicial Proceedings Committee

IN OPPOSITION to Senate Bill 192 – Facial Recognition Technology

February 8, 2023

I am Bekah Charleston, CEO and Co-Founder of Charleston Law Center, a non-profit organization committed to ending sex trafficking and exploitation by providing pro bono legal services to its victims. As a survivor of over a decade of sex trafficking, I strongly oppose Senate Bill 192 and would like to share my personal testimony to offer a unique perspective on this issue.

During my experience with sex trafficking, law enforcement failed to correctly identify me due to the false identity my trafficker had obtained for me. This made it appear as though I was of legal age and allowed my exploitation in sexually oriented businesses across the country. If facial recognition technology had been available at the time, I believe it could have intervened and put an end to the abuse I suffered. Facial recognition technology can be a valuable tool for investigators as it can help identify victims and traffickers through images, such as a victim's face appearing in ads for sex work or a trafficker being captured on video at a handoff location or committing a related crime.

Unfortunately, Senate Bill 192 severely limits the ability to identify and rescue victims by restricting facial recognition searches to only driver's license databases and mugshots. This narrow scope of searches ignores the reality that trafficking victims, particularly minors, may not have any official records or may be using false identities, like in my case. This would prevent investigators from finding and rescuing victims and limit the ability to detect patterns in trafficking activities. Moreover, the prohibition on queries involving photos of minors puts children who are exploited at greater risk by reducing or eliminating chances of identifying them. The use of facial recognition technology in a broader range of databases, such as social media and online classified ads, could be crucial in identifying victims and detecting patterns in trafficking activities. High-performing facial recognition technology, trained on robust data sets, can also aid law enforcement in conducting more trauma-informed investigations, as it reduces the dependence on victim corroboration.

Every day that I was not identified was another day of abuse and violence, and I believe the same is true for countless other victims of sexual violence. The technology can help law enforcement quickly identify victims, so they can be rescued and begin their journey toward healing. Additionally, it can help identify and hold perpetrators accountable, preventing them from finding new victims for their abuse.

Victims of sexual violence deserve to be identified and rescued, and facial recognition technology has the potential to make this a reality. As a survivor, I understand the complex, compounded trauma faced by these victims and the importance of their identification in the pursuit of justice and healing.

I urge you to reconsider the limitations outlined in Senate Bill 192 and to find a solution that prioritizes not only the safety and well-being of trafficking victims, but also the public safety in general. The use of facial recognition technology can be a valuable tool in the fight against trafficking and other crimes, and it is crucial that we do not limit its potential to protect and serve all members of our community. Thank you for your time and consideration of this important issue.

SB192_DPSCS_Opposition.pdf
Uploaded by: Catherine Kahl
Position: UNF

Department of Public Safety and Correctional Services

Office of Government & Legislative Affairs

45 Calvert Street, Suite 7A, Annapolis, MD 21401
(443) 240-8696 • www.dpscs.maryland.gov

BILL: **SENATE BILL 192**

POSITION: **OPPOSITION**

EXPLANATION: This bill establishes requirements and procedures relating to the use of facial recognition by law enforcement agencies. Further, the bill requires the Department to adopt and publish a statewide model policy, develop and administer a training program and proficiency testing, and review and approve a single facial recognition technology for use by law enforcement agencies.

COMMENTS:

- The Department of Public Safety and Correctional Services operates the State's prisons that house individuals sentenced to serve 18 months or longer. The Department also oversees the Division of Parole and Probation, which supervises individuals who are on parole or probation in the community, and runs the Baltimore City Pretrial Complex that houses individuals awaiting trial.

- The Department houses the Police Training and Standards Commission, an independent commission that functions in the Department.

- Although the Department is the repository for the Criminal Justice Information System that houses criminal history record information, facial recognition technology and CJIS are independent of each other.

- The Department is not a "law enforcement agency" as defined in Public Safety Article § 2-101 and is not an end user of facial recognition technology. The approximately 150 law enforcement agencies in the State that use this service are independent of the Department.

- Section 2-506 of the bill will require the Department to:
    - Adopt and publish a model statewide policy regarding the use of facial recognition.

    - Develop and administer a training program as well as proficiency testing as it pertains to the use of facial recognition technology in the courts and criminal investigations - including training and testing on cultural diversity and implicit bias.
    - Review and approve a single facial recognition technology for use by law enforcement agencies in the State.

- Training and proficiency testing regarding the use of facial recognition technology should be provided by the technology's vendors who (1) are the subject matter experts on the use of their technology and (2) would be the ones to determine proficiency standards.

- **The Department is concerned with the language in Section 2-506 requiring review and approval of a single facial recognition technology as it is not in a position to determine the best and sole facial recognition technology for the approximately 150 law enforcement agencies in the State;** especially as the Department is not aware of the technology maintained by each of the enforcement agencies in the State, nor is it aware of the compatibility of each agency's information technology system with existing facial recognition technology.

- Additionally, the bill states a law enforcement agency may not use or contract for the use of facial recognition technology for use in criminal investigations unless the technology is currently approved for use by the Department. As stated previously, the Department does not have knowledge of the technological capabilities of various law enforcement agencies nor is the Department able to determine what is the best resource for EACH agency when conducting criminal investigations.

- As stated previously, the Department is not an end user of this technology and therefore, should not be charged with training and proficiency testing or review and approval of an unknown product for other entities that do use these products on a regular basis. Nor should the Department review and approve a single technology that impacts approximately 150 independent law enforcement agencies. These requirements should solely lie with the subject matter experts who provide the technology and the law enforcement agencies who utilize these services.

- Facial recognition technology is an investigatory tool used by law enforcement agencies and, as such, should reside with them.

CONCLUSION: For these reasons, the Department of Public Safety and Correctional Services respectfully requests the Committee vote **UNFAVORABLE** on Senate Bill 192.

LEYDEN--Legislative Testimony--SB 192--2-7-23.pdf
Uploaded by: Edward Leyden
Position: UNF

AISHA N. BRAVEBOY
STATE'S ATTORNEY

JASON B. ABBOTT
PRINCIPAL DEPUTY STATE'S ATTORNEY

State's Attorney for Prince George's County
14735 Main Street, Suite M3403
Upper Marlboro, Maryland 20772
301-952-3500

February 9, 2023

Testimony in **Opposition** of

SB 192 – Criminal Procedure – Facial Recognition Technology – Requirements, Procedure, and Prohibitions

---

Dear Chairman Smith, Vice Chairman Waldstreicher, and Members of the Committee:

I am writing to show my opposition to Senate Bill (HB) 192 on behalf of State's Attorney Aisha Braveboy and to urge an unfavorable report. I am an Assistant State's Attorney in the Special Prosecutions Unit in the State's Attorney's Office for Prince George's County.

As a member of the Special Prosecutions Unit, I prosecute, in addition to vehicular homicides and particular murders, financial and property crimes (including arsons and terroristic threats). As a result, I am all too familiar with the very real assistance that evolving facial recognition technologies provide in rapidly identifying subjects for investigation and in helping to dissuade chronic offenders from even entering vulnerable venues, such as banks, hospitals, and casinos.

To be clear, the civil liberty concerns encapsulated in this proposed bill are certainly well-considered and weighty. It must also be borne in mind, however, that the bulk of the individuals that facial technologies have brought to the prosecutorial attention of this office had voluntarily entered the commercial premises where allegedly they committed their crimes – hence, the expectation of privacy such individuals could have reasonably entertained while within such premises was minimal.

In a real, practical sense, facial recognition technologies simply provide the kind of advanced institutional memory that a savvy and experienced premises security officer would command in being able to recognize those individuals who have earlier come into an establishment bent on committing crimes and causing trouble. It is, thus, vital to meeting evolving challenges that law enforcement be availed of these irreplaceable technologies.

For the foregoing reasons, I respectfully urge an unfavorable report, and ultimately rejection, on SB 192.

Sincerely,

/s/

Edward J. Leyden
Assistant State's Attorney – Special Prosecutions Unit
State's Attorney's Office for Prince George's County

LEYDEN--Legislative Testimony--SB 192--2-7-23.pdf
Uploaded by: Edward Leyden
Position: UNF

AISHA N. BRAVEBOY
STATE'S ATTORNEY

JASON B. ABBOTT
PRINCIPAL DEPUTY STATE'S ATTORNEY

State's Attorney for Prince George's County
14735 Main Street, Suite M3403
Upper Marlboro, Maryland 20772
301-952-3500

February 8, 2023

Testimony in **Opposition** of

SB 192 – Criminal Procedure – Facial Recognition Technology – Requirements, Procedure, and Prohibitions

---

Dear Chairman Smith, Vice Chairman Waldstreicher, and Members of the Committee:

I am writing to show my opposition to Senate Bill (HB) 192 on behalf of State's Attorney Aisha Braveboy and to urge an unfavorable report. I am an Assistant State's Attorney in the Special Prosecutions Unit in the State's Attorney's Office for Prince George's County.

As a member of the Special Prosecutions Unit, I prosecute, in addition to vehicular homicides and particular murders, financial and property crimes (including arsons and terroristic threats). As a result, I am all too familiar with the very real assistance that evolving facial recognition technologies provide in rapidly identifying subjects for investigation and in helping to dissuade chronic offenders from even entering vulnerable venues, such as banks, hospitals, and casinos.

To be clear, the civil liberty concerns encapsulated in this proposed bill are certainly well-considered and weighty. It must also be borne in mind, however, that the bulk of the individuals that facial technologies have brought to the prosecutorial attention of this office had voluntarily entered the commercial premises where allegedly they committed their crimes – hence, the expectation of privacy such individuals could have reasonably entertained while within such premises was minimal.

In a real, practical sense, facial recognition technologies simply provide the kind of advanced institutional memory that a savvy and experienced premises security officer would command in being able to recognize those individuals who have earlier come into an establishment bent on committing crimes and causing trouble. It is, thus, vital to meeting evolving challenges that law enforcement be availed of these irreplaceable technologies.

For the foregoing reasons, I respectfully urge an unfavorable report, and ultimately rejection, on SB 192.

Sincerely,

/s/

Edward J. Leyden
Assistant State's Attorney – Special Prosecutions Unit
State's Attorney's Office for Prince George's County

SB 192 Facial Recognition Technology SIA - Oppose

Uploaded by: K. Alexander Wallace

Position: UNF

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/

SB 192 - Facial Recognition.pdf
Uploaded by: Scott Shellenberger
Position: UNF

Bill Number: SB 192
Scott D. Shellenberger, States Attorney for Baltimore County
Opposed

WRITTEN TESTIMONY OF SCOTT D. SHELLENBERGER,
STATE'S ATTORNEY FOR BALTIMORE COUNTY,
IN OPPOSITION OF SENATE BILL 192
FACIAL RECOGNITION PRIVACY PROTECTION ACT

Senate Bill 192 greatly hampers the ability of the police to use modern technology to locate possible suspects in crimes by using publicly accessible databases that have been used for years.

The best way to understand how this technology works is with an example of how it was used to solve an armed robbery in Towson.

On Monday, December 7, 2015 two suspects armed with guns walked into a Towson liquor store and announced a robbery.

Claude Mayo aimed his handgun at the 68 year old clerk. The clerk fearing for his life pulled out a gun and shot Mayo. Mayo was pronounced dead at the scene. Mayo had a previous conviction for armed robbery.

The second suspect got away.

The police then went to work to identify the second suspect. The police through social media were able to find a picture of a friend of Mayo's who they believed was the other armed robber. Generally matching the description the police entered this photograph into facial recognition software that scanned that picture and ran it through various databases.

The facial recognition technology was able to return to the detective approximately 702 photographs of possible matches. Some of those were duplicates.

It was then that the detective had to use old fashion police work, look through the pictures and find the one, or ones that most matched the second armed robber to the original picture. The facial recognition technology is just a starting point much like an anonymous tip that you have to investigate to include or exclude someone as a suspect.

Once they found the match they were able to compare it to a surveillance video of the two armed robbers found in the Towson area when the robbers were together just before the crime.

Hayes Sample was convicted of attempted robbery and was sentenced to twenty years in jail.

That is how law enforcement is using facial recognition technology to solve violent crimes.

For decades people have looked through books of mug shots. No one complained. For quite some time police have been able to access MVA photos. No one complained.

But now because we have a computer to do it faster suddenly it is a privacy violation. You still have to do the old fashioned police work to get the case in court. We are not using the software in court for the judge or jury it is only a way to locate suspects.

We still have to prove it was you in a courtroom.

This Bill makes me get a court order to access databases. It is like requiring a court order to look at mug shots.

What constitutional right are we protecting here? What privacy interest do you have when the MVA has been keeping your photo that you voluntarily submit for years?

Think of some of the things Senate Bill 192 would prevent. The use of this technology in airports like BWI. You subjecting your face to the public should not the police be able to use the best technology to find the next shoe bomber.

This bill makes me get a court order to help me find missing persons or identify the body we have found in the woods. What Constitutional right are we protecting there?

Senate Bill 192 is too restrictive and does not allow the police to do their job. It is merely a way to speed up the universe of those who may be suspects but the State must still prove its case.

I urge an unfavorable report.