MCPA-MSA_SB 182 Facial Recognition _SUPPORT.pdf

Uploaded by: Andrea Mansfield

Position: FAV

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 7, 2023

RE: **SB 182 Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions**

POSITION: **SUPPORT**

The Maryland Chiefs of Police Association (MCPA) and the Maryland Sheriffs’ Association (MSA) SUPPORT SB 182. This bill establishes reasonable safeguards and audit protocols for the use of facial recognition technology.

Facial recognition technology is a valuable time savings investigatory tool for law enforcement. Understanding the concerns with its use, MCPA and MSA have proactively worked with the bill sponsor over the past two sessions to put reasonable safeguards in place for government use of the technology to ensure there is no intrusion on constitutionally protected activities. MCPA and MSA are pleased to support SB 182 as it strikes the correct balance.

As introduced, SB 182 is identical to the amended version of the bill from last year that was agreed upon in conference committee, but unfortunately did not achieve final passage in the final minutes of the Session. The bill in this form represents a compromise and is broadly supported. SB 182 authorizes the use of facial recognition technology for 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 can also be 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).

SB 182 will also allow matches to take place with multiple databases to 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.

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.

Lastly, 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. SB 182 authorizes the use of multiple technologies to leverage 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.

For these reasons, MCPA and MSA SUPPORT SB 182 and respectfully request a FAVORABLE Committee report.

SB 182 MOPD Fav.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: SENATE BILL 182 Criminal Procedure - Facial Recognition Technology - Requirements, P and Prohibitions

FROM: Maryland Office of the Public Defender

POSITION: Favorable

DATE: 02/06/24

The Maryland Office of the Public Defender urges a favorable report on SB182.

Since this bill was first introduced two years ago, the need to regulate this technology has become clear and more urgent. We know that faulty facial recognition identifications can, and do, occur. In fact, faulty facial recognition identifications have occurred here in Maryland. We view this bill as an initial step in the correct direction to establish critical guidelines in an area that is currently completely unregulated. We hope that once Senate Bill 182 is passed, we can focus on broad and comprehensive protections against the invasions of privacy that are inherent with constantly advancing technology.

By limiting the circumstances when this technology can be used, and by requiring independent evidence to corroborate any match, this bill strives to limit the possibility of an individual being wrongly charged based upon the results of facial recognition. A wrongful charge can completely derail an individual's life. Moreover, the discovery and disclosure provisions will help to ensure that this surveillance technology operates in a transparent manner.

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. We hope that as these standards are developed, that they are incorporated into the model statewide policy that is part of this bill. 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 report on Senate Bill 182.

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

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

SB0182_Facial_Recognition_Technology_MLC_FAV.pdf

Uploaded by: Cecilia Plante

Position: FAV

MARYLAND
LEGISLATIVE
COALITION

TESTIMONY FOR SB0182

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 SB0182 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 society 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.

FINAL Testimony SB182 .pdf

Uploaded by: Charles E. Sydnor III

Position: FAV

Charles E. Sydnor III, Esq.
Legislative District 44
Baltimore County

Deputy Majority Whip

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 182:
Criminal Procedure – Facial Recognition Technology –
Requirements, Procedures, and Prohibitions
Before the Judicial Proceedings Committee
February 7, 2024

Good afternoon, Chair Smith, members of the Judicial Proceedings Committee,

Today I offer Senate Bill 182 ("SB 182") in response to the growing, unregulated use of Facial Recognition Technology ("FRT") and reintroduces legislation which was voted out of this committee and this body unanimously; it unfortunately was unable to pass before on Sine Die. SB 182 establishes guidelines surrounding law enforcement's use of FRT, limits the databases law enforcement may use while utilizing FRT, and establishes training for law enforcement agencies (or officers) who employ FRT.

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.). Today facial recognition systems are also utilized throughout the world 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 FRT; 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

[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).

matches rapidly.[2] In this ocean of data, what is there to stop law enforcement from exceeding their reach, invading an individual's privacy, and embarking on a fishing expedition? While facial recognition can and help enforce justice, we must balance safety concerns against the very real threat that law enforcement will cast a net whenever they need a catch. SB 182 sets forth standards that will provide some level of accountability and control when law enforcement casts the facial recognition net.

Undoubtedly there are benefits to using FRT: preventing and addressing unlawful entry at ports,[3] and monitoring high-security events, such as the Super Bowl,[4] to name a few. 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. The LA Times reported, "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] Given Maryland's movement towards adoption of police body cameras, we must consider how FRT's 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]

Previously, this committee passed SB 587 establishing a Task Force on Facial Recognition Privacy Protection; however, the bill ultimately did not make its way through the legislative process. I reached out to everyone included in SB 587 and asked them to work with Delegate Moon and I on legislation for this session. Our workgroup consisted of 14-members which including members of law enforcement, the Department of Public Safety and Corrections, the Maryland States Attorney Association, the Office of the Public Defender, a trade group representative, a vendor, an academic researcher, and civil rights advocates. We met virtually to discuss issues connected with the use of FRT. Invited contributors ranged from ordinary citizens with concerns, and a researcher from Australia. For more than five months we met over 10 times—our objective, adopting a foundational set of statewide requirements for law enforcement agencies using FRT, and addressing key public concerns about the technology, while preserving the public safety benefits of the technology. These discussions resulted in SB 182. SB 182 sets guardrails for the law enforcement's usage of FRT systems. SB 182 provides that FRT can be used as an investigative tool,[9] and limits the types of crimes that can be investigated using FRT.[10]

[2] Ari B. Rubin, *A Facial Challenge: Facial Recognition Technology and the Carpenter Doctrine*, 27 RICH. J.L. & TECH. 1, 6 (2021).
[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.

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 182 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 participants, SB 182 establishes training programs that will be developed and administered to provide for proficiency testing for law enforcement personnel who use FRT. Additionally, each agency must maintain appropriate records regarding the use of FRTs, and annually report FRT uses to the Governor's Office of Crime Prevention and Policy.

In conclusion, I recognize that facial recognition technology is a complex investigative tool whose value is growing as the practical applications expand. We must take a strong initial step towards developing and maintaining standards and guidance for the uses of this beneficial 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. These protections must evolve appropriately as FRT utilization evolves in its practical applications.

For these reasons I respectfully urge the Committee to vote in favor of SB 182.

Testimony in favor of SB182.pdf

Uploaded by: Jerry Kickenson

Position: FAV

Testimony in favor with amendments of SB182
Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions
To: Hon. William Smith, Jr., Chair, Hon. Jeff Waldstreicher, Vice-chair and members of the Senate Judicial Proceedings Committee
From: Jerry Kickenson
Date: February 6, 2024

I am writing in **favor of Senate Bill 182**, Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions

Facial recognition technology can be a useful law enforcement tool, but many studies have demonstrated that the technology is also subject to bias and errors that can cause great harm, both to mistakenly identified residents and by misdirecting an investigation:

- When Artificial Intelligence Gets It Wrong (https://innocenceproject.org/when-artificial-intelligence-gets-it-wrong/#:~:text=The%20use%20of%20such%20biased,match%20%E2%80%94%20all%20six%20were%20Black)
- The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest (https://heinonline.org/HOL/LandingPage?handle=hein.journals/waslee79&div=21&id=&page=)
- The Bias in the Machine: Facial Recognition Technology and Racial Disparities (https://mit-serc.pubpub.org/pub/bias-in-machine/release/1?readingCollection=34db8026)
- Facing Injustice: How Face Recognition Technology May Increase the Incidence of Misidentifications and Wrongful Convictions (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4101826)

This bill will create useful constraints on the use of facial recognition technology in law enforcement, and most importantly require a state wide policy on its use that can prevent bias and errors.

I respectfully urge you to reach a **favorable** report for SB182.

Respectfully yours,
Jerry Kickenson
1701 Ladd Street
Silver Spring, MD 20902

Facial recognition - use for CP and HT - senate te

Uploaded by: Lisae C Jordan

Position: FAV

MCASA
Maryland Coalition Against Sexual Assault

Working to end sexual violence in Maryland

P.O. Box 8782
Silver Spring, MD 20907
Phone: 301-565-2277
Fax: 301-565-3619

For more information contact:
Lisae C. Jordan, Esquire
443-995-5544
www.mcasa.org

Testimony Supporting Senate Bill 182
Lisae C. Jordan, Executive Director & Counsel
February 1, 2024

The Maryland Coalition Against Sexual Assault (MCASA) is a non-profit membership organization that includes the State's seventeen rape crisis centers, law enforcement, mental health and health care providers, attorneys, educators, survivors of sexual violence and other concerned individuals. MCASA includes the Sexual Assault Legal Institute (SALI), a statewide legal services provider for survivors of sexual assault. MCASA represents the unified voice and combined energy of all of its members working to eliminate sexual violence. We urge the Judicial Proceedings Committee to report favorably on Senate Bill 182.

Senate Bill 182 -- Facial Recognition Technology
Use in Child Pornography, Sexual Assault, Stalking, and Human Trafficking Cases
SB182 would impose limits on the use of facial recognition technology. MCASA appreciates the careful drafting to continue to allow use of this technology in cases involving child pornography, sexual assault (under the crimes of violence provisions), stalking and human trafficking cases.

The Maryland Coalition Against Sexual Assault urges the
Judicial Proceedings Committee to
report favorably on Senate Bill 182

SB 182 - Facial Recognition.pdf

Uploaded by: Scott Shellenberger

Position: FAV

Bill Number: SB 182
Scott D. Shellenberger, State's Attorney for Baltimore County
Support

WRITTEN TESTIMONY OF SCOTT D. SHELLENBERGER, STATE'S ATTORNEY FOR BALTIMORE COUNTY, IN SUPPORT OF SENATE BILL 182 FACIAL RECOGNITION

I write in support of Senate Bill 182 that represents a compromise that has been long in the making. Senate Bill 182 strikes a balance between those who want to use Facial Recognition Technology to solve crimes and those who want to protect the privacy of citizens. Senate Bill 182 represents a long discussed compromise of this issue.

In Summary Senate Bill 182:

- prevents the results generated by facial recognition technology from being introduced in a criminal trial or delinquency proceeding;
- permits the results of Facial Recognition to establish probable cause;
- does not permit the results to be the "sole basis" for probable cause;
- requires the addition of independent evidence.
- limits the use of the technology to violent and serious crimes;
- prevents the technologies use if the activity is under the protection of the Constitution etc.
- is not used to analyze a sketch;
- results may not be disclosed prior to a witness identification procedure;
- analysis may not be done in live or real time.
- limits the database of photos to MVA records and mug shots;
- the results must be verified by a specially trained individual;
- requires disclosure during discovery that the technology was used;
- requires yearly public disclosure of certain information.

Senate Bill 182 strikes an important balance between law enforcement interests and those who have privacy concerns.

I urge a favorable report.

SB 183 Testimony_Unfavorable_LDF_2-6-2024.pdf

Uploaded by: Kristina Roth

Position: UNF

LDF Legal Defense Fund

Advancing racial
justice since1940

February 6, 2024

Via Electronic Delivery

William C. Smith, Jr., Chair
Jeff D. Waldstreicher, Vice Chair
Senate Judicial Proceedings Committee
Miller Senate Office Building, 2 East Wing
11 Bladen St.
Annapolis, MD 21401 - 1991

RE: Senate Bill 182 - Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions – Unfavorable

Dear Chairperson Smith and Vice Chairperson Waldstreicher:

On behalf of the NAACP Legal Defense and Educational Fund, Inc. ("LDF"),[1] we submit this written testimony regarding Senate Bill 182 ("SB 182") and House Bill 338 ("HB 338"), Criminal Procedure – Facial Recognition Technology – Requirements, Procedures, and Prohibitions, which aim to establish "requirements, procedures, and prohibitions relating to the use of facial recognition technology by a law enforcement agency." Although facial recognition technology ("FRT") is promoted as a tool to increase efficiency in policing, this technology is ineffective, and exacerbates and replicates racial bias and discrimination by law enforcement[2] and in the criminal legal system.[3] Systemic and implicit bias can taint FRT at every stage of its life cycle—from the data used to train the technology, as well as through the practices of how FRT is commissioned, developed, and deployed.[4] Therefore, legislators must examine and contend with the use of FRT by law enforcement in the larger context of pre-existing racial bias and discrimination in law enforcement practices and the criminal legal system. For the reasons provided below, LDF submits this testimony in opposition to SB 182 and HB 338.

[1] Founded by Thurgood Marshall in 1940, LDF is the nation's oldest civil rights law organization. Since its founding, LDF has relied on the United States Constitution and federal and state civil rights laws to pursue equality and justice for Black Americans and other marginalized communities. LDF's mission has always been transformative: to achieve racial justice, equality, and an inclusive society. As part of that work, LDF has forged longstanding partnerships with impacted communities, organizers, researchers, and attorneys to challenge and reform unlawful and discriminatory policing practices across the country, including law enforcement's use of technology and algorithmic systems in a racially discriminatory manner. These technologies, coupled with their use by law enforcement agencies, directly threaten the lives, liberty, rights, and dignity of Black people and other marginalized communities.

[2] Alfred Ng, *'Wholly ineffective and pretty obviously racist': Inside New Orleans' struggle with facial-recognition policing*, Politico (Oct. 31, 2023), https://www.politico.com/news/2023/10/31/new-orleans-police-facial-recognition-00121427 ("Records obtained and analyzed by POLITICO show that computer facial recognition in New Orleans has low effectiveness, is rarely associated with arrests and is disproportionately used on Black people . . . . Although it has not led to any false arrests, which have happened in other cities, the story of police facial identification in New Orleans appears to confirm what civil rights advocates have argued for years, as police departments and federal agencies nationwide increasingly adopt high-tech identification techniques: that it amplifies, rather than corrects, the underlying human biases of the authorities that use them.").

[3] Khari Johnson, *The Hidden Role of Facial Recognition Tech in Many Arrests*, Wired (Mar. 7, 2022), https://www.wired.com/story/hidden-role-facial-recognition-tech-arrests/.

[4] Reva Schwartz et al., *Towards a Standard for Identifying and Managing Bias in Artificial* Intelligence, National Institute of Standards and Technology 10 (Mar. 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.

I. Evidence Shows Facial Recognition Technology is Error-Prone and Its Use by Law Enforcement Results in Discriminatory Policing.

Facial recognition systems are inaccurate, and these errors exacerbate preexisting racial biases in police practices. The technology is error-prone for people with darker skin and for features associated with Black people, Asian people, women, and transgender or nonbinary people.[5] A report by the National Institute of Standards and Technology found that Black and Asian people may be between ten to one hundred times more likely to be misidentified by facial recognition systems than white men, depending on the algorithm used.[6] Additionally, for one-to-many matching,[7] the research team saw higher rates of false positives for Black women.[8] As noted by the team, "differentials in false positives in one-to-many matching are particularly important because the consequences could include false accusations."[9] Finally, even if the technology became accurate across demographic groups, law enforcement's use of FRTs would still worsen the disparate and targeted policing, surveillance, and criminalization of Black and Brown communities because of the systemic racial bias that continues to plague police practices.[10]

[5] Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, WIRED (July 22, 2019), https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/; Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018), https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28; Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proceedings Mach. Learning Rsch. 1 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; *Facial Recognition: Analyzing Gender and Intersectionality in Machine Learning*, Gendered Innovations, https://genderedinnovations.stanford.edu/case-studies/facial.html#tabs-2 (last visited Jan. 18, 2024).

[6] See Patrick Grother et al., Nat'l Inst. of Standards & Tech., U.S. Dep't of Com., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, Interagency Internal Report 8280 2 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf (evaluating 189 software algorithms from 99 developers on their ability to correctly identify individuals in (1) one-to-one matching and (2) one-to-many matching, two of the most common uses of facial recognition technology); see also *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, Nat'l Inst. of Standards & Tech. (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software#:~:text=According%20to%20a%20new%20study,recognition%20algorithms%20exhibit%20demographic%20differentials.

[7] A "one-to-many" matching system is when software takes an "unknown face and compares it to a large database of known faces to determine the unknown person's identity." William Crumpler, *How Accurate Are Facial Recognition Systems – and Why Does It Matter?*, Ctr. for Strategic & Int'l Stud. (Apr. 14, 2020), https://www.csis.org/blogs/strategic-technologies-blog/how-accurate-are-facial-recognition-systems-and-why-does-it.

[8] Grother et al., *supra* note 6, at 63; *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, *supra* note 6.

[9] *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, *supra* note 6; NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, FACIAL RECOGNITION TECHNOLOGY: CURRENT CAPABILITIES, FUTURE PROSPECTS, AND GOVERNANCE 40 (2024), https://doi.org/10.17226/27397 ("The consequences of false positives vary by application. As a false positive involves two people, either or both can be affected. In a one-to-one access control task, a false positive could lead to loss of privacy or theft, for example. In a pharmacy, an employee would not be able to refute the assertion that they dispensed drugs to a fraudster. In a benefits-fraud detection setting, a false positive might lead to a wrongly delayed or rejected application. In a public-area surveillance application, a false positive could result in interview and arrest.").

[10] *See* Kade Crockford, *How Is Face Recognition Surveillance Technology Racist?*, ACLU (June 16 2020), https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist; NATIONAL ACADEMIES OF SCIENCES, *supra* note 9, at 59-60 ("FRT provides law enforcement with a powerful new tool for identifying individuals more rapidly, at a distance, and at greater scale and thus, depending on where and how it is used, has the potential to reinforce patterns or perceptions of elevated scrutiny by law enforcement and national security agencies, especially in marginalized communities. Put bluntly, some communities may be more surveilled

In the law enforcement context, these errors result in significant harm and can lead to false arrests, wrongful incarceration, and detrimental, lifelong consequences. To date, six people are known to have been falsely accused of a crime due to law enforcement's use of facial recognition systems. All six are Black people.[11] Errors leading to additional false arrests likely exist but are difficult to ascertain because law enforcement's use of facial recognition is usually not disclosed.[12] Moreover, the vast majority of people accused of crimes agrees to plea deals rather than risk lengthy sentences, preventing scrutiny of officers' investigative methods leading to their arrests.[13]

II. While Prohibition is Preferable, Maryland Must, at a Minimum, Advance Strong and Defined Safeguards for Limited Law Enforcement Use of Facial Recognition Technology in SB 182.

Law enforcement's use of FRT will likely exacerbate racial biases by law enforcement and in the criminal legal system and as such, should be prohibited. However, if the Maryland legislature seeks to regulate law enforcement use of FRT, it is critical that any legislation ensures that use of the technology does not perpetuate discriminatory policing, violate the constitutional and statutory rights of Maryland residents; nor further obscure policing practices.

1. Law Enforcement's Use of Facial Recognition Technology Must Be Subject to Clear Limitations.

The limits and parameters for law enforcement's use of FRT must be clear to thwart unlawful or discriminatory use of the technology. SB 182 prohibits the use of FRT except in limited circumstances. However, the bill's exception that permits use of FRT by law enforcement to investigate "a criminal act involving circumstances presenting a substantial and ongoing threat to public safety or national security"[14] is vague and does not create an enforceable limit. Law enforcement agencies may interpret "substantial" to include crimes not involving violence and presenting an "ongoing threat to public safety" merely if a suspect has not been identified, located, or apprehended. "Substantial" should be interpreted to mean credible threats of serious or fatal violence to multiple persons. "Ongoing" must also be defined narrowly to exclude vague descriptions often used to justify law enforcement surveillance practices in Black and Brown communities.[15]

than others, and increased scrutiny can lead to neighborhoods being designated as high-crime areas, a feedback loop that can further justify use of FRT or other technologies that disproportionately affect marginalized communities. Moreover, the use of FRT has raised concerns in some communities—including Black, Hispanic, and Muslim communities—reflecting in part differential intensity of past interactions with law enforcement and other government authorities.").

[11] Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, N.Y. Times (Aug. 6, 2023), https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html#:~:text=Handcuffed%20in%20front%20of%20her,to%20be%20searched%20for%20evidence.

[12] Jake Laperruque, *Limiting Face Recognition Surveillance: Progress and Paths Forward*, Ctr. for Democracy & Tech. (Aug. 23, 2022), https://cdt.org/insights/limiting-face-recognition-surveillance-progress-and-paths-forward/#:~:text=Currently%20two%20states%20%E2%80%94%20Colorado%20and,recognition%20was%20used%20in%20investigations (noting only 2 states "require the government to disclose the use of face recognition to defendants before a trial").

[13] *See* Lindsey Devers, Bureau of Just. Assistance, U.S. Dep't of Just., *Plea and Charge Bargaining* 3 (2011), https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/pleabargainingresearchsummary.pdf (90-95 percent of cases result in plea bargaining).

[14] S.B. 182, 446th Sess. sec. 2-503 (A)(1)(I)(11), https://mgaleg.maryland.gov/2024RS/bills/sb/sb0182F.pdf.

[15] *See* Kade Crockford, *How Is Face Recognition Surveillance Technology Racist?*, ACLU (June 16 2020), https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist.

Additionally, SB 182 prohibits the use of FRT on an image or a recording of an individual that engages in activity protected by the United States Constitution, Maryland Constitution, and Maryland Declaration of Rights, which includes protests and demonstrations that are protected under the First Amendment. However, the exception to this prohibition would permit the use of FRT where there is reasonable suspicion to believe that an individual has "committed, is in the process of committing, or is about to commit a crime"[16] and, thus, does not limit the use of FRT to a category of limited crimes. As a result, FRT could be used on protestors who "loiter" or refuse to obey an officer, without committing any other offense. Recent research examining nearly 2000 protests in 2020 found that law enforcement arrived more often and with a a greater demonstration of force at racial justice protests compared to other protests.[17] Additionally, law enforcement were more likely to make arrests at racial justice protests.[18] These findings remained true even after controlling for differences in protestor behaviors, crowd size, time of day, use of force policies, and other factors. To prevent the disparate use of facial recognition on protestors challenging racial discrimination, law enforcement use of FRT should not be permitted on protestors, even where a crime has been committed, due to the broad nature of the criminal code.

Similarly, SB 182 prohibits law enforcement from using FRT to identify individuals based on personal interests. However, the prohibition has an exception: it permits the use of facial recognition technology by law enforcement to identify an individual based on personal interest if it is "related to legitimate duties or objectives of the law enforcement agency"[19]—a carveout that is otherwise undefined and not narrowly tailored. Finally, SB 182 clarifies that law enforcement use of FRT is not restricted for certain enumerated purposes but creates an exception that renders those enumerated purposes unnecessary by allowing law enforcement to use FRT to "conduct[] otherwise legitimate activity unrelated to a criminal investigation."[20]

All of these exceptions should be narrowly delineated or eliminated altogether. Regulating the use of FRT by law enforcement requires narrow and clear enforceable limits. Maryland must enumerate with precision law enforcement's use of FRT to avoid abuse and misuse of the technology and curb its risk of creating disproportionate harm on Black and other marginalized communities.

2. <u>All Facial Recognition Technology Used by Law Enforcement Must Be Assessed for Accuracy and Fairness by the National Institute of Standards and Technology.</u>

As noted above, facial recognition technology is error-prone, and these errors exacerbate preexisting racial biases in policing.[21] The National Institute of Standards and Technology ("NIST") Face Recognition Vendor Testing Program ("FRVT") provides "independent evaluations of both prototype and commercially available facial recognition algorithms."[22] NIST publishes their independent evaluations of facial recognition systems, and this information is used to assist the federal government in deploying FRT.[23] The evaluations conducted by NIST measure the core algorithmic capability of FRT and reported accuracy and performance of the

[16] S.B. 182, 446th Sess. sec. 2-503(A)(1)(II)(1), https://mgaleg.maryland.gov/2024RS/bills/sb/sb0182F.pdf.
[17] SANDHYA KAJEEPETA AND DANIEL K.N. JOHNSON, POLICE AND PROTESTS: THE INEQUITY OF POLICE RESPONSES TO RACIAL JUSTICE DEMONSTRATIONS 7 (2023), https://tminstituteldf.org/wp-content/uploads/2023/10/Police-and-Protests_PDF-3.pdf.
[18] *Id.* At 8.
[19] S.B. 182, 446th Sess. sec. 2-503(B)(1), https://mgaleg.maryland.gov/2024RS/bills/sb/sb0182F.pdf.
[20] S.B. 182, 446th Sess. sec. 2-507(5), https://mgaleg.maryland.gov/2024RS/bills/sb/sb0182F.pdf.
[21] *See supra* Part I.
[22] Dr. Charles H. Romine, *Facial Recognition Technology*, NIST (Feb. 6, 2020), https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0.
[23] *Id.*

algorithm with regard to certain characteristics, including, race, sex, and age.[24] Legislators should require prior NIST testing of FRT used or contracted by Maryland's law enforcement agencies. The technology must meet minimum accuracy standards across demographics and receive an accuracy score of 98% or higher[25] for true positive across all demographic groups. Because the risks stemming from false positives are dire, including false arrests, detention, and lifelong consequences, any FRT used by law enforcement must demonstrate a high accuracy rate.

III. Law Enforcement's Use of Facial Recognition Technology Remains Largely Obscure, and Maryland's Efforts to Create Transparency Must Allow for Independent Oversight and Auditing in SB 182.

1. SB 182 Should Promote Transparency by Releasing Results of Audits and Providing Comprehensive Annual Reports.

The inability of communities to access data that an algorithm uses—or an explanation of an algorithmic system's decision regarding an individual—in a law enforcement context poses significant risks to the life and liberty of people subjected to the technologies. For example, law enforcement's unfettered use of FRT, which incorporates publicly available, photo datasets that expose people to government identification and tracking[26] without their knowledge and largely without independent oversight,[27] raises grave concerns about the potential infringement of individuals' rights. Yet, there is very little data collected and made publicly available about the activities of individual law enforcement officers or agencies, including their use of FRT, that would permit public oversight. The public does not know the demographic characteristics of persons searched, the justification for each search, what technology was used, how the search was conducted, or the outcomes of searches.[28] Subsequently, people are provided with little or no information regarding the role a facial recognition system played in law enforcement's

[24] *Id.*

[25] In the third series of reports on NIST's facial recognition vendor tests, NIST tested and documented accuracy variations across demographic groups. This evaluation did not capture demographic differentials that consist of "wild images" (i.e., has tested across demographics to determine accuracy image data from the internet or from video surveillance). The research, however, shows "a wide range in accuracy across algorithm developers, with the most accurate algorithms producing many fewer errors than lower-performing variants." More accurate algorithms produce fewer errors and are therefore expected to have smaller demographic differentials. Given the performance differentials across demographic groups, setting a minimum performance standard for accuracy across demographics provides a guardrail to ensure that inaccuracies in the technology do not contribute to racial disparities. *See* GAO, Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law, 36-37 GAO-20-522 (July 2020). Because law enforcement activity poses a high risk to people's fundamental rights, a high accuracy threshold across demographic differentials is warranted to prevent violations of these rights.

[26] *See* Ryan Mac, Caroline Haskins & Logan McDonald, *Clearview's Facial Recognition App Has Been Used By the Justice Department, ICE, Macy's, Walmart, and the NBA*, BuzzFeed News (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

[27] Clare Garvie, *Garbage In, Garbage Out: Face Recognition On Flawed Data*, Geo. Law Ctr. on Priv. & Tech. (May 16, 2019), https://www.flawedfacedata.com/ ("There are no rules when it comes to what images police can submit to face recognition algorithms to generate investigative leads.").

[28] *See id.* ("The NYPD made 2,878 arrests pursuant to face recognition searches in the first 5.5 years of using the technology [,] Florida law enforcement agencies . . . run on average 8,000 searches per month of the Pinellas County Sheriff's Office face recognition system, [but] [m]any other agencies do not keep close track of how many times their officers run face recognition searches and whether these searches result in an arrest.").

investigative or enforcement activity, the recourse to challenge its use, or the ability to contest abuses or errors.[29]

To promote transparency, data and other pertinent information related to law enforcement's use of facial recognition technology must be made available to the public annually and disaggregated by race and other protected categories. While SB 182 requires the preparation and publication of an annual report from law enforcement agencies contracting for the use of facial recognition technology, the bill does not include certain categories of information that would help inform Marylanders of the technology's effectiveness, usefulness, and accuracy. For example, the report should include the total number of false positives and false negatives; complaints of bias resulting from use of the technology; violations of the model statewide policy or use and data management policy; and a breakdown of all reported uses of facial recognition technology that includes the age, race, and sex in connection to the search. Additionally, all audit materials should be made available to members of the general public through a public records request.

2. <u>SB 182 Should Provide Written Notice to Recipients of Drivers Licenses and Identification Cards.</u>

Additionally, the use of surveillance cameras, facial recognition software, and databases containing driver's license and state identification photos, as proposed in SB 182, exposes millions of people to a "perpetual line-up."[30] The use of one's photo in these perpetual line-ups often occurs without the consent, or even awareness, of the individuals pictured, creating additional privacy implications.[31] At least one facial recognition technology company, Clearview AI, has contracted with law enforcement agencies across the country and mines public platforms and/or photo databases, such as social media platforms and security footage, for the datasets supporting its technology—all without the captured person's knowledge or consent.[32] In fact, a person's face

[29] *See* Lauren Feiner & Annie Palmer, *Rules Around Facial Recognition and Policing Remain Blurry*, CNBC (June 12, 2021), https://www.cnbc.com/2021/06/12/a-year-later-tech-companies-calls-to-regulate-facial-recognition-met-with-little-progress.html; *see also* Aaron Mak, *Facing Facts: A Case in Florida Demonstrates the Problems with Using Facial Recognition to Identify Suspects in Low-Stakes Crimes*, Slate (Jan. 25, 2019), https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html.

[30] Clare Garvie et al., *The Perpetual Line-Up*, Geo. Law Ctr. on Priv. & Tech. (Oct. 18, 2016), https://www.perpetuallineup.org/. There is also a high concentration of Black and Brown people in police-created gang databases. For example, the NYPD maintains a database of 42,000 "gang affiliates"—99 percent Black and Latinx—with no requirements to prove suspected gang affiliation. In fact, certain police departments use gang member identification as a productivity measure, incentivizing false reports. Alex Najibi, *Racial Discrimination in Face Recognition Technology*, Sci. in the News (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

[31] *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It,* N.Y. Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[32] Police in Miami arrested protestors by working with Clearview AI, which has built a database of 3 billion pictures by extracting faceprints of individuals without their consent from pictures posted online. Connie Fossi & Phil Prazan, *Miami Police Used Facial Recognition Technology in Protester's Arrest*, NBC MIAMI (Aug. 17, 2020), https://www.nbcmiami.com/investigations/miami-police-used-facial-recognition-technology-in-protesters-arrest/2278848/; *Despite Concerns, Law Enforcement Use of Facial Recognition Expands in South Florida*, NBC MIAMI (Jul. 8, 2020), https://www.nbcmiami.com/investigations/despite-concerns-law-enforcement-use-of-facial-recognition-expands-in-south-florida/2259663/. Clearview AI's app carries extra risks because law enforcement agencies are uploading sensitive photos to the servers of a company whose ability to protect its data is untested. Hill, *supra* note 31; *see also Facial Recognition Under Scrutiny as Clearview AI's Practices Ruled Illegal in Canada*, IFSEC Insider (Feb. 16, 2021), https://www.ifsecglobal.com/video-surveillance/facial-recognition-under-scrutiny-as-clearview-ais-practices-ruled-illegal-in-canada/ (ruling by Canadian government that Clearview AI's collection of biometric information from its citizens without their knowledge or consent is illegal).

could be used to create and train a facial recognition algorithm without that person having ever uploaded a photo or consented to its use.[33] When FRT is shared with law enforcement agencies, police may run hundreds of thousands of searches for an identification, using any photo, against a broad range of available databases, without those individuals whose facial images are in the database ever being informed of law enforcements' access to these photos or use of such searches.[34] If the technology identifies a match, their identifying biometric information is then available for use across multiple law enforcement agencies at the push of a button.[35]

Many people are unwillingly and unknowingly participating in a perpetual lineup simply because databases containing driver's license and state identification photos are used by law enforcement to run matches.[36] As such, legislators must mandate that the Maryland Motor Vehicle Administration provide written notice, in a conspicuous manner, to recipients of driver's license and state identification cards of this possibility.

* * *

In sum, short of prohibition, SB 182's aim to dramatically limit law enforcement use of FRT, establish parameters for when it may be used, and provide accountability mechanisms is a step in the right direction. However, additional parameters and accountability mechanisms must be included for SB 182 to achieve its purpose and adequately protect Marylanders from potential violations of their rights and liberties. For the above reasons, LDF submits this testimony in opposition to SB 182 and HB 338.

Thank you for your consideration of these issues. If you have questions, please do not hesitate to contact Puneet Cheema, pcheema@naacpldf.org and Avatara Smith-Carrington, acarrington@naacpldf.org.

Sincerely,

Avatara A. Smith-Carrington

Avatara Smith-Carrington, Fellow, Strategic Initiatives Department
Puneet Cheema, Manager, Justice in Public Safety Project

[33] *See* Joseph Goldstein & Ali Walker, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database.*, N.Y. Times (Aug. 1, 2019), https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html.

[34] Katie Canales, *Thousands of US Police Officers and Public Servants Have Reportedly Used Clearview's Controversial Facial Recognition Tech Without Approval*, Bus. Insider (Apr. 6, 2021), https://www.businessinsider.com/clearview-ai-facial-recognition-thousands-police-departments-2021-4; *see also* Press Release, Surveillance Tech. Oversight Project, S.T.O.P. Condemns NYPD for 22K Facial Recognition Searches (Oct. 23, 2020), https://www.stopspying.org/latest-news/2020/10/23/stop-condemns-nypd-for-22k-facial-recognition-searches.

[35] For example, the Chicago and Detroit Department camera systems allow officers to run facial recognition software against any captured images. Blair Paddock, *Chicago Police Using Controversial Facial Recognition Tool*, WTTW (Jan. 30, 2020), https://news.wttw.com/2020/01/30/chicago-police-using-controversial-facial-recognition-tool (In a statement, the Chicago Police Department said it is: "using a facial matching tool to sort through its mugshot database and public source information in the course of an investigation triggered by an incident or crime."); Bryce Huffman, *What We Know So Far About Detroit's Controversial Use of Facial Recognition*, Bridge Detroit (July 22, 2021), https://www.bridgedetroit.com/what-we-know-so-far-about-detroits-controversial-use-of-facial-recognition/ ("Detroit police use facial recognition technology to compare pictures of a suspect with a database of images culled from public records, social media and other sources.").

[36] *See supra* Sect.II.2.