## MCPA-MSA\_HB 338 Facial Recognition \_SUPPORT.pdf Uploaded by: Andrea Mansfield

Position: FAV



### Maryland Chiefs of Police Association Maryland Sheriffs' Association



### **MEMORANDUM**

TO: The Honorable Luke Clippinger, Chairman and

Members of the House Judiciary 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 13, 2024

**RE: HB 338 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 HB 338. 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 HB 338 as it strikes the correct balance.

As introduced, HB 338 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. HB 338 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).

HB 338 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. HB 338 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 three years ago.

For these reasons, MCPA and MSA SUPPORT HB 338 and respectfully request a FAVORABLE Committee report.

# HB 338 MOPD Fav.pdf Uploaded by: Andrew Northrup Position: FAV



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: HOUSE BILL 338** Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions

FROM: Maryland Office of the Public Defender

**POSITION: Favorable** 

DATE: 02/0/924

The Maryland Office of the Public Defender urges a favorable report on HB338.

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 House Bill 338 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 House Bill 338.

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

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

# HB0338\_Facial\_Recognition\_Technology\_MLC\_FAV.pdf Uploaded by: Cecilia Plante

Position: FAV



#### **TESTIMONY FOR HB0338**

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

Bill Sponsor: Delegate Moon

**Committee:** Judiciary

**Organization Submitting:** Maryland Legislative Coalition

Person Submitting: Cecilia Plante, co-chair

**Position: FAVORABLE** 

I am submitting this testimony in favor of HB0338 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.

**hb338.pdf**Uploaded by: Deborah Levi
Position: FAV



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: HB 338 Facial Recognition Technology Requirements, Procedures, and Prohibitions

FROM: Maryland Office of the Public Defender

**POSITION:** Favorable

DATE: 02/09/2024

The Maryland Office of the Public Defender respectfully requests that the Committee issue a favorable report on House Bill 338.

In 2023, an armed robbery case was dismissed in Baltimore City because the Office of the Public Defender established that facial recognition was used inappropriately, and certain discovery obligations were not adhered to. In that same year, a number of Black men were charged with misdemeanors and faced the threat of imprisonment on nothing more than an unsupported facial recognition report. Ultimately, all of those cases were also dismissed, but not without significant agony imposed on each of our clients. We have seen similar discovery violations with similar results in an attempted murder, rape, and gun possession case. The reality is that this technology has developed too rapidly and law enforcement is using it too recklessly, or without proper education, and society is not any safer as a result.

The Office of the Public Defender requested data from around the State regarding the use of facial recognition technology and from that data we have learned that this technology is used in at least three major metropolitan jurisdictions, with differing requirements and discovery obligations in each of those jurisdictions. Additionally, courts are challenged to decipher best practices and proper procedures related to facial recognition technology. While some of our clients' cases have been dismissed as a result of the improper use of facial recognition technology or the government's failure to produce the appropriate discovery, it is our belief that even more clients have been prejudiced by the lack of uniform procedures and requirements. To ensure fairness and a more just system, we

urge a favorable report on HB 338, as it is a very important starting point towards regulating the use of facial recognition technology.

For these reasons, the Maryland Office of the Public Defender urges this Committee to issue a favorable report on House Bill 338

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

Authored by: Deborah Katz Levi, Director of Special Litigation, Baltimore City,

(667)406-2348; Deborah.Levi@Maryland.Gov;

# HB 338 Facial Recognition Technology SIA 02.13.24. Uploaded by: Jacob Parker

Position: FAV



February 13, 2024

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

### Re: Written Testimony of SIA in Support of HB 338, Regarding Law Enforcement Use of Facial Recognition Technology

Dear Chair Clippinger, Vice-Chair Bartlett and Members of the House Judiciary Committee:

On behalf of the Security Industry Association (SIA) I am writing to express our support for HB 338 in its current form. SIA is a nonprofit trade association in Silver Spring, MD that represents more than 1,400 companies providing a broad range of security products and services in the U.S and throughout Maryland. Our members include the leading providers of facial recognition software tools available to U.S. law enforcement.

#### **Ensuring Responsible, Effective and Non-Discriminatory Use**

If enacted, we believe HB 338/SB 182 would be the strongest measure in the country for regulating the use of facial recognition technology by state and local law enforcement agencies, in a way that both addresses public concerns and preserves proven capabilities. We commend the sponsors for their openness to working with stakeholders with subject matter expertise across law enforcement, industry and civil society in drafting the measure, as an accurate understanding of the technology and its place within existing investigative procedures is essential to policymaking in this area.

There is growing consensus among law enforcement professionals on the necessity of facial recognition as an available tool in investigations, as well as appropriate procedures surrounding its use. For well 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, solve cold cases and help citizens in need. There are many specific successes documented by Maryland law enforcement agencies using the technology demonstrating the clear benefit to public safety. The technology has also been an indispensable tool in fighting child sexual exploitation and human trafficking in Maryland. There are several organizations that provide the technology as part of investigator tools 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 from trafficking.

<sup>&</sup>lt;sup>1</sup> https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology/

<sup>&</sup>lt;sup>2</sup> https://www.thorn.org/spotlight/

At the same time, some public concerns have surfaced over whether the photo-matching technology is accurate, and how it might be used in the absence of uniform rules. Many advanced technologies offer both tremendous benefits and the potential for misuse, and we support policies ensuring facial recognition is only used for appropriate purposes consistent with SIA's *Principles for the Responsible and Effective Use of Facial Recognition Technology*. Applicable to law enforcement, we believe establishing key foundational safeguards in statute, combined with more thorough requirements in agency procedural rules, is the most effective legislative approach to building greater public trust, while allowing agencies to harness advances in technology and procedures over time.

#### **Consensus on Core Rules**

At its core, the bill would do just that, by establishing a statewide policy that is the same across state, county and city law enforcement agencies, subject to key requirements and limitations. This will bolster confidence that Maryland law enforcement agencies are leveraging facial recognition software in a lawful, effective, accurate and non-discriminatory manner that benefits our residents and communities. 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.
- Full public transparency, documentation and periodic centralized reporting on agency use of the technology.

### **Explained: How Law Enforcement Agencies Use Facial Recognition Technology**

Facial recognition software is used daily across the U.S. to assist in identifying and capturing the most violent criminals in our country and bringing justice and closure for victims. Many investigators feel that this technology has become a game-changer for keeping our communities safe, pointing to instances where crimes would never have been solved or prevented without it. Use under appropriate policies and procedures has been endorsed by the nation's leading law enforcement professional associations.<sup>4</sup>

In U.S. law enforcement, the technology serves as a tool to assist investigators in generating leads regarding the identity of an unknown person of interest in an image (such as a potential witness, victim, suspect or associate) where needed in a specific ongoing case. This is a post-incident investigative tool to aid identification, not "surveillance," and in this application <u>facial recognition technology does not confirm an identity</u> or result in automated decisions. If a lead is developed, investigative techniques outside of facial comparison must be used to find and confirm information needed to positively identify a person, and if a suspect, establish probable cause to make an arrest or obtain a search warrant.

<sup>&</sup>lt;sup>3</sup> https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/

<sup>&</sup>lt;sup>4</sup> For example, see https://majorcitieschiefs.com/wp-content/uploads/2021/10/MCCA-FRT-in-Modern-Policing-Final.pdf.

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 (from a security camera or cell phone for example). Under traditional methods, police seek to identify a person of interest manually by looking through hundreds of mugshots with victims, canvassing areas with photos or searching a database using vague suspect descriptions or names that could easily be criminal aliases or fraudulent identities. Facial recognition technology automates and improves the first step of identifying potentially matching photos from a database.

Beyond simply improving an otherwise manual process, facial recognition also contributes to more accurate identification. As the importance of limiting human bias in police work as well as unnecessary interactions with citizens becomes increasingly clear, this software makes the process of generating and investigating leads faster and more accurate than relying only on human analysis alone. The National Institute of Science and Technology has found<sup>5</sup> that forensic examiners performed best when supported by facial recognition technology and the most accurate performance resulted when these efforts are combined. Proper use of this technology is critical to protecting the innocent, as eyewitness identifications in criminal investigations are notoriously prone to error. According to the Innocence Project,<sup>6</sup> mistaken eyewitness identifications have been the key factor in the vast majority of wrongful convictions in the U.S. later overturned.

#### 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. We urge the Committee to approve HB 338 and 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

iparker@securityindustry.o

rg

<sup>&</sup>lt;sup>5</sup> https://www.nist.gov/news-events/news/2018/05/nist-study-shows-face-recognition-experts-perform-better-ai-partner

<sup>&</sup>lt;sup>6</sup> https://innocenceproject.org/eyewitness-misidentification/

## **NPAP\_HB 338 Favorable Testimony.pdf**Uploaded by: Keisha James

Position: FAV



**FAVORABLE - HB 338** – Criminal Procedure – Facial Recognition Technology – Requirements, Procedures, and Prohibitions

**Written Testimony** of National Lawyers Guild-National Police Accountability Project, Keisha James, Staff Attorney

Judiciary Committee - February 13, 2024

Dear Chair Clippinger, Vice Chair Bartlett, and Judiciary Committee Members,

Thank you for the opportunity to provide comment on this important issue. The National Lawyers Guild National Police Accountability Project ("NPAP") is a nonprofit organization dedicated to holding law enforcement and corrections officers accountable to constitutional and professional standards. We urge a favorable report on HB 338, a bill that will limit how law enforcement agencies can use the results generated by facial recognition technology.

The government's use of facial recognition technology raises a number of serious concerns: the breadth of people impacted by the technology, the misuse of the technology for widespread surveillance, the inaccuracy of facial recognition systems, and racial biases in both police practices and facial recognition algorithms. These concerns directly implicate our free speech and freedom of association rights under the First Amendment, our right to be free from

<sup>&</sup>lt;sup>1</sup> Alex Pasternack, *Police Body Cameras Will Do More Than Just Record You*, Fast Company (Mar. 3, 2017), available at <a href="https://www.fastcompany.com/3061935/police-body-cameras-livestreaming-face-recognition-and-ai">https://www.fastcompany.com/3061935/police-body-cameras-livestreaming-face-recognition-and-ai</a> (researchers estimate that the faces of 117 million people in the U.S. have already been captured and stored in searchable federal, state, or local databases).

<sup>2</sup> Id

<sup>&</sup>lt;sup>3</sup> Jennifer Lynch, Face Off: Law Enforcement Use of Face Recognition Technology, Electronic Frontier Foundation, at 6-7 (April 20, 2020), available at <a href="https://www.eff.org/wp/law-enforcement-use-face-recognition">https://www.eff.org/wp/law-enforcement-use-face-recognition</a> ("Face recognition systems vary in their ability to identify people, and no system is 100 percent accurate under all conditions....Technical issues endemic to all face recognition systems mean false positives will continue to be a common problem for the foreseeable future.").

<sup>&</sup>lt;sup>4</sup> *Id.* at 9-10 ("The false-positive risks...will likely disproportionately impact African Americans and other people of color. Research...found that face recognition misidentified African Americans and ethnic minorities, young people, and women at higher rates than whites, older people, and men, respectively. Due to years of well-documented racially-biased police practices, all criminal databases—including mugshot databases—include a disproportionate number of African Americans, Latinos, and immigrants.") (internal citations omitted); *see also* Pasternack, *supra*, n.1 ("The faces of certain races and ethnic groups have proved difficult for some facial recognition algorithms, raising the risk of false positives that reinscribe existing biases in the criminal justice system.").

<sup>&</sup>lt;sup>5</sup> Lynch at 8, *supra*, n.3 ("Face recognition and the accumulation of easily identifiable photographs implicate free speech and freedom of association rights and values under the First Amendment, especially because face-



unreasonable searches and seizures under the Fourth Amendment,<sup>6</sup> and our due process rights.<sup>7</sup>

There are also issues presented by plans for future use of facial recognition technology in policing, including departments buying body-worn cameras from manufacturers that provide face recognition in their cameras and allow for remote access to cameras<sup>8</sup> and generating images of a person based on a police sketch or a DNA sample.<sup>9</sup>

Without meaningful limitations on its use, law enforcement agencies will continue to use facial recognition technology in increasingly invasive and inaccurate ways. By adopting HB 338, Maryland would be taking a step in the right direction to limit the impact of this harmful technology.

HB 338 will prohibit the use of facial recognition for live or real-time identification (a problem that will become increasingly prevalent as more companies integrate facial recognition features into their cameras). The bill will prevent the results of facial recognition technology from being used in criminal and delinquency proceedings and require the results to be supported by independent evidence when being used to establish probable cause. Further, law enforcement officers and employees will only be permitted to use facial recognition technology to investigate certain serious crimes.

identifying photographs of crowds or political protests can be captured in public, online, and through public and semipublic social media sites without individuals' knowledge.")

<sup>&</sup>lt;sup>6</sup> Pasternack, *supra*, n. 1 ("[C]onstant video footage from body-worn cameras could enhance the ability of the police to monitor anyone who passes in front of a camera lens 'without the individual basis for suspicion constitutionally required to justify a police search.' In essence, simply walking past a police officer could legally become an encounter.").

<sup>&</sup>lt;sup>7</sup> Lynch at 10, *supra*, n. 3 ("False positives can alter the traditional presumption of innocence in criminal cases by placing more of a burden on suspects and defendants to show they are not who the system identifies them to be. This is true even if a face recognition system offers several results for a search instead of one; each of the people identified could be brought in for questioning, even if there is nothing else linking them to the crime.").

 $<sup>^8</sup>$  Lynch at 21-22, supra, n. 3;  $see\ also$  Pasternack, supra, n. 1.

<sup>&</sup>lt;sup>9</sup> Lynch at 22-23, *supra*, n. 3.



The bill also accounts for law enforcement transparency, accountability, and oversight, as recommended by subject matter experts. <sup>10</sup> Law enforcement agencies with service contracts for facial recognition technology will be required to complete an annual audit to ensure compliance with the bill's requirements and produce an annual report with information about their use of the technology.

Maryland will not be alone in considering and imposing important limitations on the use of facial recognition technology. Cities across California, Louisiana, Maine, Massachusetts, Minnesota, Oregon, Pennsylvania, Washington, and Wisconsin have considered or enacted legislation limiting or banning the use of facial recognition technology. Last year, after Baltimore's moratorium on facial recognition expired, Baltimore's City Council considered legislation that would limit the types of crimes face recognition could be used to investigate, prohibit it from being used at protests, and establish specialized training and oversight requirements for its use. 12

We urge you to make a favorable report on HB 338. Thank you, again, for the opportunity to provide comment on this important issue.

Keisha James

National Police Accountability Project

keisha.npap@nlg.org

<sup>&</sup>lt;sup>10</sup> Lynch at 27, *supra*, n. 3 ("All database transactions—including face recognition input, access to and searches of the system, data transmission, etc.—should be logged and recorded in a way that ensures accountability. Privacy and security impact assessments, including independent certification of device design and accuracy, should be conducted regularly."); Lynch at 28, *supra*, n. 3 ("Government entities that collect or use face recognition must be subject to meaningful oversight from an independent entity. Individuals whose data are compromised by the government or the private sector should have strong and meaningful avenues to hold them accountable.").

 <sup>11</sup> See, e.g., Electronic Frontier Foundation, Bans, bills, and moratoria, available at <a href="https://www.eff.org/aboutface/bans-bills-and-moratoria#main-content">https://www.eff.org/aboutface/bans-bills-and-moratoria#main-content</a> (a non-comprehensive list of legislation).
 12 See, e.g., David Collins, Baltimore City seeks to regulate facial recognition technology, WBAL-TV 11 (Nov. 15, 2023), available at <a href="https://www.wbaltv.com/article/baltimore-city-facial-recognition-technology-bill-considered/45851909">https://www.wbaltv.com/article/baltimore-city-facial-recognition-technology-bill-considered/45851909</a>; Christian Olaniran and Paul Gessler, Baltimore City seeks to regulate facial recognition technology, WJZ News (Nov. 15, 2023), available at <a href="https://www.cbsnews.com/baltimore/news/baltimore-city-council-to-hold-first-public-hearing-on-facial-recognition-bill/">https://www.cbsnews.com/baltimore/news/baltimore-city-council-to-hold-first-public-hearing-on-facial-recognition-bill/</a>.

# **HB 338 - Facial Recognition.pdf**Uploaded by: Scott Shellenberger Position: FAV

**Bill Number: HB 338** 

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 HOUSE BILL 338 FACIAL RECOGNITION

I write in support of House Bill 338 that represents a compromise that has been long in the making. House Bill 338 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. House Bill 338 represents a long discussed compromise of this issue.

### In Summary House Bill 338:

- 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.

House Bill 338 strikes an important balance between law enforcement interests and those who have privacy concerns.

I urge a favorable report.

## **2-9-2024 CJSJ Sign-on Testimony - HB 338 - Unfavor** Uploaded by: Kristina Roth

Position: UNF



February 9, 2024

Luke Clippinger, Chair Sandy Bartlett, Vice Chair House Judiciary Committee House Office Building 6 Bladen St., Room 101 Annapolis, MD 21401

### RE: House Bill 338 - Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions – Unfavorable

As part of the undersigned group, we write to voice our strong opposition to HB 338/SB 182, which establishes requirements, procedures, and prohibitions relating to the use of facial recognition technology ("FRT") by law enforcement. Research shows that FRT algorithms are biased, and the technology is particularly error-prone for people with darker skin, women, young people, and transgender and nonbinary people. Moreover, law enforcement use of FRT can cause harm to wrongfully accused individuals. As such, we fundamentally believe that the guardrails this bill sets to limit the use of FRT by law enforcement are insufficient and use of FRT by law enforcement will disproportionately harm Black and other marginalized Marylanders.

In addition to the numerous studies evaluating accuracy and bias in FRT, there have been several documented examples of real-world harm caused by law enforcement use of FRT: of the six known cases of FRT misidentification, all of them have been Black people. Most recently, Porcha Woodruff—who was 8-months pregnant at the time she was confronted by police in Detroit—was wrongfully arrested and held in jail for 11 hours after being implicated as a suspect due to misidentification by FRT. While in the holding cell, Ms. Woodruff experienced contractions and spasms, had a possible panic attack, and became dehydrated. She later shared that "she was embarrassed to be arrested in front of her neighbors and that her daughters were traumatized."

The exceptions in HB 338 are too broad to effectively limit the use of FRT by law enforcement. Specifically, HB 338 includes several loopholes or vaguely written exceptions which would broaden the scope for law enforcement use of FRT. Additionally, HB 338 lacks adequate measures for creating transparency when it comes to law enforcement's use of FRT. Without strong measures that require documentation

and publication of law enforcement's use of FRT, Marylanders will remain in the dark regarding law enforcement use of FRT and this can further complicate efforts by community members who are advocating for more transparency regarding policing practices in Maryland. We are concerned that the bill will fail to adequately limit law enforcement use of FRT and that law enforcement use of FRT will contribute to racially disparate policing, increased surveillance of marginalized communities, and wrongful arrests.

Due to the threats that use of FRT by law enforcement pose, the use of FRT must be (1) narrow and explicitly limited, (2) consistent and independently assessed for accuracy and bias, and (3) made known to Marylanders through published access to annual reports and the results of audits.

Since HB 338 does not provide adequate provisions for any of these measures, we do not believe this bill offers Marylanders protection from the proven harms of FRT use by law enforcement.

Although law enforcement already use FRT in Maryland, which is disconcerting given the lack of information made publicly available about the technology's use, we believe that HB 338 lacks the safeguards necessary to protect Marylanders' rights. For these reasons, we respectfully submit this testimony in opposition to HB 338.

The Campaign for Justice Safety and Jobs

**Baltimore Action Legal Team** 

Citizens Policing Project

Common Cause Maryland

**Making Changes** 

**Public Justice Center** 

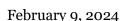
Showing Up for Racial Justice (SURJ) Baltimore

The Shriver Center at UMBC

The Talking Drum Incorporated

# HB 338 Testimony\_Unfavorable\_LDF\_2-9-2024.pdf Uploaded by: Kristina Roth

Position: UNF





### **Via Electronic Delivery**

Luke Clippinger, Chair J. Sandy Bartlett, Vice Chair House Judiciary Committee House Office Building 6 Bladen St. Annapolis, MD 21401 - 1991

**RE:** House Bill 338 - Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions – Unfavorable

Dear Chairperson Clippinger and Vice Chairperson Bartlett:

On behalf of the NAACP Legal Defense and Educational Fund, Inc. ("LDF"),¹ we submit this written testimony regarding House Bill 338 ("HB 338") and Senate Bill 182 ("SB 182"), 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 enforcement² 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 HB 338 and SB 182.

<sup>&</sup>lt;sup>1</sup> 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.

<sup>&</sup>lt;sup>2</sup> 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.").

<sup>&</sup>lt;sup>3</sup> 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/.

<sup>&</sup>lt;sup>4</sup> 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.<sup>5</sup> 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.<sup>6</sup> Additionally, for one-to-many matching,<sup>7</sup> the research team saw higher rates of false positives for Black women.<sup>8</sup> As noted by the team, "differentials in false positives in one-to-many matching are particularly important because the consequences could include false accusations." 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.<sup>10</sup>

<sup>&</sup>lt;sup>5</sup> 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). <sup>6</sup> 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/newsevents/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognitionsoftware#:~:text=According%20to%20a%20new%20study,recognition%20algorithms%20exhibit%20demographic% 20differentials.

<sup>&</sup>lt;sup>7</sup> 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

 $<sup>^8</sup>$  Grother et al., supra note 6, at 63; NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software, supra note 6.

<sup>&</sup>lt;sup>9</sup> 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.").

<sup>&</sup>lt;sup>10</sup> 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 HB 338.

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. <u>Law Enforcement's Use of Facial Recognition Technology Must Be Subject to</u> 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. HB 338 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" 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

3

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.").

 $<sup>^{11}</sup>$  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.

<sup>&</sup>lt;sup>12</sup> 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").

<sup>&</sup>lt;sup>13</sup> 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).

<sup>&</sup>lt;sup>14</sup> H.B. 338, 446th Sess. sec. 2-503 (A)(1)(I)(11), https://mgaleg.maryland.gov/2024RS/bills/hb/hb0338F.pdf. <sup>15</sup> 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, HB 338 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" 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 greater demonstration of force at racial justice protests compared to other protests. Additionally, law enforcement were more likely to make arrests at racial justice protests. 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, HB 338 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" —a carveout that is otherwise undefined and not narrowly tailored. Finally, HB 338 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." <sup>20</sup>

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</u> for Accuracy and Fairness by the National Institute of Standards and Technology.

As noted above, facial recognition technology is error-prone, and these errors exacerbate preexisting racial biases in policing.<sup>21</sup> 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." <sup>22</sup> NIST publishes their independent evaluations of facial recognition systems, and this information is used to assist the federal government in deploying FRT.<sup>23</sup> The evaluations conducted by NIST measure the core algorithmic capability of FRT and reported accuracy and performance of the

<sup>&</sup>lt;sup>16</sup> H.B. 338, 446th Sess. sec. 2-503(A)(1)(II)(1), https://mgaleg.maryland.gov/2024RS/bills/hb/hb0338F.pdf.
<sup>17</sup> SANDHYA KAJEEPETA AND DANIEL K.N. JOHNSON, POLICE AND PROTESTS: THE INEQUITY OF POLICE RESPONSES TO RACIAL

 $<sup>{\</sup>tt JUSTICE\ DEMONSTRATIONS\ 7\ (2023), https://tminstituteldf.org/wp-content/uploads/2023/10/Police-and-Protests\_PDF-3.pdf.}$ 

<sup>&</sup>lt;sup>18</sup> *Id*. At 8.

<sup>&</sup>lt;sup>19</sup> H.B. 338, 446th Sess. sec. 2-503(B)(1), https://mgaleg.maryland.gov/2024RS/bills/hb/hb0338F.pdf.

<sup>&</sup>lt;sup>20</sup> H.B. 338, 446th Sess. sec. 2-507(5), https://mgaleg.maryland.gov/2024RS/bills/hb/hb0338F.pdf.

<sup>&</sup>lt;sup>21</sup> See supra Part I.

<sup>&</sup>lt;sup>22</sup> Dr. Charles H. Romine, *Facial Recognition Technology*, NIST (Feb. 6, 2020), https://www.nist.gov/speechtestimony/facial-recognition-technology-frt-0.
<sup>23</sup> *Id*.



algorithm with regard to certain characteristics, including, race, sex, and age.<sup>24</sup> 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<sup>25</sup> 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 HB 338.

1. <u>HB 338 Should Promote Transparency by Releasing Results of Audits and Providing Comprehensive Annual Reports.</u>

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<sup>26</sup> without their knowledge and largely without independent oversight,<sup>27</sup> 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.<sup>28</sup> Subsequently, people are provided with little or no information regarding the role a facial recognition system played in law enforcement's

<sup>&</sup>lt;sup>24</sup> Id

<sup>&</sup>lt;sup>25</sup> 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.

<sup>&</sup>lt;sup>26</sup> 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.

<sup>&</sup>lt;sup>27</sup> 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.").

<sup>&</sup>lt;sup>28</sup> 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.<sup>29</sup>

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 HB 338 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>HB 338 Should Provide Written Notice to Recipients of Drivers Licenses and</u> Identification Cards.

Additionally, the use of surveillance cameras, facial recognition software, and databases containing driver's license and state identification photos, as proposed in HB 338, exposes millions of people to a "perpetual line-up." 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. 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. In fact, a

<sup>&</sup>lt;sup>29</sup> 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-metwith-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.

<sup>30</sup> 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

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/.

<sup>&</sup>lt;sup>31</sup> 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.

<sup>&</sup>lt;sup>32</sup> 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-asclearview-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).



person's face could be used to create and train a facial recognition algorithm without that person having ever uploaded a photo or consented to its use.<sup>33</sup> 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.<sup>34</sup> 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.<sup>35</sup>

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.<sup>36</sup> 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, HB 338'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 HB 338 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 HB 338 and SB 182.

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

<sup>&</sup>lt;sup>33</sup> 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.

<sup>&</sup>lt;sup>34</sup> 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.

<sup>&</sup>lt;sup>35</sup> 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.").

# **HB338MTsiongasTestimony.pdf**Uploaded by: Magdalena Tsiongas Position: UNF

Luke Clippinger, Chair Sandy Bartlett, Vice Chair House Judiciary Committee House Office Building 6 Bladen St., Room 101 Annapolis, MD 21401

### RE: House Bill 338 - Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions – Unfavorable

I, Magdalena Tsiongas, write to voice my strong opposition to HB 338/SB 182, which establishes requirements, procedures, and prohibitions relating to the use of facial recognition technology ("FRT") by law enforcement. Research shows that FRT algorithms are biased and the technology is particularly error-prone for people with darker skin, women, young people, and transgender and nonbinary people. Moreover, law enforcement use of FRT can cause harm to wrongfully accused individuals. As such, we fundamentally believe that the guardrails this bill sets to limit the use of FRT by law enforcement are insufficient and use of FRT by law enforcement will disproportionately harm Black and other marginalized Marylanders.

In addition to the numerous studies evaluating accuracy and bias in FRT, there have been several documented examples of real-world harm caused by law enforcement use of FRT: of the six known cases of FRT misidentification, all of them have been Black people. Most recently, Porcha Woodruff—who was 8-months pregnant at the time she was confronted by police in Detroit—was wrongfully arrested and held in jail for 11 hours after being implicated as a suspect due to misidentification by FRT. While in the holding cell, Ms. Woodruff experienced contractions and spasms, had a possible panic attack, and became dehydrated. She later shared that "she was embarrassed to be arrested in front of her neighbors and that her daughters were traumatized."

The exceptions in HB 338 are too broad to effectively limit the use of FRT by law enforcement. Specifically, HB 338 includes several loopholes or vaguely written exceptions which would broaden the scope for law enforcement use of FRT. Additionally, HB 338 lacks adequate measures for creating transparency when it comes to law enforcement's use of FRT. Without strong measures that require documentation and publication of law enforcement's use of FRT, Marylanders will remain in the dark regarding law enforcement use of FRT and this can further complicate efforts by community members who are advocating for more transparency regarding policing practices in Maryland. We are concerned that the bill will fail to adequately limit law enforcement use of FRT and that law enforcement use of FRT will contribute to racially

disparate policing, increased surveillance of marginalized communities, and wrongful arrests.

Due to the threats that use of FRT by law enforcement pose, the use of FRT must be (1) narrow and explicitly limited, (2) consistent and independently assessed for accuracy and bias, and (3) made known to Marylanders through published access to annual reports and the results of audits.

Since HB 338 does not provide adequate provisions for any of these measures, we do not believe this bill offers Marylanders protection from the proven harms of FRT use by law enforcement.

Although law enforcement already use FRT in Maryland, which is disconcerting given the lack of information made publicly available about the technology's use, we believe this HB 338 lacks the safeguards necessary to protect Marylanders' rights. For these reasons, I respectfully submit this testimony in opposition to HB 338.