

SB0762 Sen Sydnor Testimony for Facial Recognition

Uploaded by: Charles E. Sydnor III

Position: FAV

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

Judicial Proceedings Committee

Joint Committees

Children, Youth, and Families

Ending Homelessness



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

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

**Testimony Regarding SB 762:
Criminal Procedure – Facial Recognition Technology –
Requirements, Procedures, and Prohibitions
Before the Judicial Proceedings Committee
March 10, 2022**

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

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

By the time you read this sentence, 20,000 images will be uploaded to social media.¹ There is an ocean of pictures out there and facial recognition technology enables users to find face template matches rapidly.² In this ocean of data, what is there to stop law enforcement from going on a fishing expedition? While facial recognition can and will help enforce justice, we need to balance safety concerns against the very real threat that law enforcement will cast a net whenever they need a catch. SB 762 sets forth standards that will provide some level of accountability and control over when the facial recognition net is cast.

Undoubtedly there are benefits to use of facial recognition: preventing and addressing unlawful entry at ports,³ as well as monitoring high-security events, such as the Super Bowl.⁴ In the local

¹ Facial Recognition Technology: Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees. www.gao.gov Retrieved September 5, 2021.

² Matthew Doktor, *Facial Recognition and the Fourth Amendment in the Wake of Carpenter v. United States*, 89 U. CIN. L. REV. 552, 552 (2021).

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

³ *Id.* at 14.

⁴ *Id.*

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

Last year this committee passed SB 587 to establish a Task Force on Facial Recognition Privacy Protection. That bill ultimately did not make its way thru the legislative process, but I reached out to everyone who we had included in that legislation and asked them to work with me and Delegate Moon on legislation for this session. Our workgroup consisted of 14-members which included of law enforcement, the Department of Public Safety and Corrections, the Maryland States Attorney Association, the Office of the Public Defender, trade group representative and a vendor, an academic researchers, and civil rights advocates. We met virtually to discuss issues connected with the use of facial recognition technology. Invited contributors consisted of everyone from ordinary citizens with concerns, and a researcher from Australia. For more than five months our workgroup met over 10 times with the objective of adopting a foundational set of statewide requirements for law enforcement agencies using FRT, and to address the key public concerns about the technology, while preserving the public safety benefits of the technology. Those discussions resulted in SB 762.

SB 762 sets guardrails for the usage of FRT systems by law enforcement. SB 762 provides that FRT can be used as an investigative tool,⁹ and limits the types of crimes that can be investigated using FRT.¹⁰ To limit falsely identifying someone, SB 762 also limits the databases that can be used by law enforcement agencies to those government databases which were disclosed during the workgroup meetings to motor vehicle identification images and mugshot photos maintained by local, state or federal law enforcement agencies.

For the greater part of the time our workgroup met, we worked under the assumption that the Department of Public Safety and Correctional Services had the only FRT system in use in Maryland. Therefore, SB 762 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

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.

application programming interface of the vendor; requires the vendor to enable testing of its software for accuracy and mitigation for any performance differences as they apply across various population groups.

As suggested by some of our participants, SB 762 establishes training programs that will be developed and administered in order to provide for proficiency testing for law enforcement personnel who uses FRT. Additionally, each agency must maintain appropriate records regarding its use of FRT, and will annually report its uses to the Governor's Office of Crime Prevention, Youth & Victims Services.

In conclusion, I recognize that facial recognition technology is a complex investigative tool whose value is growing as the practical applications expand. We need to take this strong initial step towards developing and maintaining standards and guidance for the uses of this useful and innovative technology. FRT offers real benefits to our communities and to the law enforcement agencies who utilize it. Transparency, accountability and civil protections against human bias characteristics need to be developed and maintained now and evolve appropriately as the utilization evolves in its practical applications. For these reasons I urge the Committee to vote in favor of SB 762.

SB 762 Facial Recognition Support .pdf

Uploaded by: John Giannetti

Position: FAV

Maryland Criminal Defense Attorneys' Association



Md Senate – Judicial Proceedings Committee

March 10, 2022

Hearing on SB 762

Criminal Procedure – Facial Recognition Technology

MCDAA POSITION: SUPPORT

Brief bill explanation: This bill establishes significant new criminal law and criminal procedures regarding the use of facial recognition technology.

MCDAA's position: The use of facial recognition technology by law enforcement agencies must be carefully guided by the legislative bodies in our country. Significant civil liberties and privacy of Marylanders will be compromised without a careful examination of the use of this new technology. We generally endorse the aims and purposes of this legislation.

This legislation aims to limit the use of the technology to specific purposes: In connection with issuance of a warrant or at a preliminary hearing, and the results of the technology may not be used by the finder of fact 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 and limits its use in real-time evaluation of images or recordings. We believe these are appropriate and needed limitations.

For additional information or questions regarding this legislation, please contact MCDAA Government Relations Contact John Giannetti 410.300.6393, JohnGiannetti.mcdaa@gmail.com

MOPD favorable with Amendments sb0762 oral.pdf

Uploaded by: Andrew Northrup

Position: FWA



PAUL DeWOLFE
PUBLIC DEFENDER

KEITH LOTRIDGE
DEPUTY PUBLIC DEFENDER

MELISSA ROTHSTEIN
DIRECTOR OF POLICY AND DEVELOPMENT

KRYSTAL WILLIAMS
DIRECTOR OF GOVERNMENT RELATIONS DIVISION

ELIZABETH HILLIARD
ASSISTANT DIRECTOR OF GOVERNMENT RELATIONS DIVISION

POSITION ON PROPOSED LEGISLATION

BILL: SB0762 - Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions

FROM: Maryland Office of the Public Defender

POSITION: Favorable with Amendments

DATE: 3/9/2022

Thank you Mr. Chairman, good afternoon. My name is Andrew Northrup and I am an attorney in the Forensics Division of the OPD. The Maryland Office of the Public Defender's position on this bill is Favorable with amendments.

We want to thank Senator Sydnor and vice-chair Moon for their persistence and determination in grappling with this issue. This bill is an important first step in regulating the use of Facial Recognition Technology, which is currently unregulated and being used in casework. The restriction of its use to the most serious crimes, the need of additional independent evidence to establish probable cause, and the transparency requirements will help to foster a more measured and responsible use of the technology.

However, after discussing the bill with other I am concerned about the ways that certain provisions may be interpreted. To that end, we have offered and tendered amendments to add clarity and foster transparency.

First, it is imperative that a defendant is provided the results and supporting data whenever this technology is used. This bill states that the state shall disclose 'in accordance with the Maryland Rules regarding discovery.' In order to make clear that Facial Recognition Technology is addressed by these rules, it is our suggestion that a sentence be added to the end of the definition of Facial Recognition Technology clarifying that Facial Recognition Technology is considered electronic surveillance or pretrial identification for purposes of the rule.

Second, there appears to be agreement among all parties that the results generated from this technology should be used as an investigative lead and not introduced at trial under any circumstances. While there is language to this effect at the end of Section 2-503, it is our position that similar language should be added to the end of Section 2-502.

In addition to posting the name and version of the Facial Recognition Software approved for use, DPSCS, should also post any developmental and internal validation studies conducted on that software so that communities can fully evaluate and understand the technology.

It is important to recognize that this technology is new, and the standards for its use are still being developed. As our understanding in this area of science grows and standards are implemented, this legislation will almost certainly need to be revisited to incorporate these developments.

Nevertheless, this bill is an important first step to regulate this area of technology with a high potential of misuse. We have tendered amendments that we believe address the concerns that we have set forth above.

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

**Submitted By: Maryland Office of the Public Defender, Government Relations Division.
Authored By: Andrew Northrup, Forensics Division, (312) 804-9343,
andrew.northrup@maryland.gov.**

POGO_Maryland Face Recognition Testimony.pdf

Uploaded by: Jake Laperruque

Position: FWA



**Written Testimony of Jake Laperruque,
Senior Policy Counsel, The Constitution Project at the Project On Government Oversight,
Regarding SB 762, An Act Concerning Criminal Procedure – Facial Recognition
Technology – Requirements, Procedures, and Prohibitions**

Position: Favorable with Amendments

Members of the Judicial Proceedings Committee, I am submitting this written testimony on behalf of The Constitution Project at the Project On Government Oversight regarding SB 762, An Act Concerning Criminal Procedure – Facial Recognition Technology – Requirements, Procedures, and Prohibitions. We applaud the bill’s effort to limit government use of face surveillance and emerging biometric surveillance technologies in a manner consistent with civil rights, civil liberties, equity, and racial justice. However, the bill also lacks certain measures that are essential to effectively safeguarding the public from face recognition surveillance. We ask the committee to augment the important policies in the current bill with additional safeguards that will ensure it fully protects civil rights and civil liberties.

Founded in 1981, the Project On Government Oversight (POGO) is a nonpartisan independent watchdog that investigates and exposes waste, corruption, abuse of power, and when the government fails to serve the public or silences those who report wrongdoing. We champion reforms to achieve a more effective, ethical, and accountable federal government that safeguards constitutional principles. The Constitution Project at POGO centers its work on issues such as guarding against improper and overbroad surveillance, including unchecked face recognition. In 2019, The Constitution Project convened a task force of expert stakeholders including academics, tech experts, civil rights and civil liberties advocates, and law enforcement officials to examine the impact of face recognition surveillance.¹ Our group concluded that any law enforcement use of face recognition should be subject to strong limits, and it provided a set of policy recommendations to support legislatures in the creation of reasonable but necessary limits.

In order to effectively address the range of risks face recognition poses to civil rights and civil liberties, legislation must include a variety of safeguards. It is essential the law only allow police to use face recognition technology to investigate serious crimes by searching images to identify a suspect, with appropriate judicial authorization, and include clear due process protection for how the tech is used and disclosed. The law should not permit law enforcement to use face recognition for generalized surveillance, or for selective enforcement of low-level offenses that could harm marginalized and over-policed communities.

¹ Task Force on Facial Recognition Surveillance, Project On Government Oversight, *Facing the Future of Surveillance* (March 4, 2019), <https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/>.

In particular, we believe that legislation limiting face recognition should center on at least five key policy priorities:

1. Requiring that face recognition searches are based on probable cause.
2. Limiting use of face recognition to the investigation of serious crimes.
3. Prohibiting face recognition from being used as the sole basis for arrests.
4. Requiring notice to defendants whenever face recognition is used.
5. Prohibiting face recognition from being used for untargeted surveillance.

SB 762 would enact strong rules that accomplish three of these goals. It sets policies in furtherance of a fourth, but we believe it requires technical amendments to ensure effective compliance. In one key area, the bill lacks any effective safeguards. Thus, while we think the bill would offer significant improvements, it requires amendments in order to serve as a comprehensive response to the dangers posed by face recognition.

Require All Face Recognition Searches Be Based on Probable Cause

Requiring that law enforcement demonstrate probable cause that an unknown person in question has committed a crime before they use face recognition to identify that individual is a critical safeguard for preventing abuse. The primary police use for face recognition is to scan photographs of individuals taken during commission of a crime; demonstrating probable cause in such scenarios should not be an onerous burden for supporting legitimate law enforcement goals.

This requirement is essential to stopping face recognition from being used to catalog and target individuals engaged in constitutionally protected activities such as protesting, participating in political rallies, or attending religious services. The danger of this surveillance technology being misused in such a manner is not theoretical: Police have used face recognition on multiple occasions in recent years to identify peaceful civil rights protesters.² Without a probable cause requirement, police could also use face recognition as a dragnet surveillance tool, scanning, identifying, and cataloging individuals' activities on a mass scale.

Unfortunately, SB 762 does not include a requirement that face recognition searches be based on probable cause, or set any type of judicial authorization to guard against abuse. This is a significant omission that needlessly endangers the public.

Without a warrant requirement, face recognition could facilitate fishing expeditions and nefarious uses such as identifying protesters at a large gathering. While the bill does include provisions against using face recognition based on features such as political beliefs, race, or sexual orientation, it sets a weak rule that police officers cannot conduct scans to identify individuals based "solely" on these factors.³

² Joanne Cavanaugh Simpson and Marc Freeman, "South Florida police quietly ran facial recognition scans to identify peaceful protesters. Is that legal?" *South Florida Sun Sentinel*, June 26, 2021, <https://www.sun-sentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sll5uuaqfbeda32rndlv3xwxi-htmlstory.html>; Kevin Rector and Alison Knezevich, "Social media companies rescind access to Geofeedia, which fed information to police during 2015 unrest," *Baltimore Sun*, October 11, 2016, <https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html>.

³ Sec. 2-503(B).

Such a standard would mean an officer could use face recognition to identify protesters en masse if an act of vandalism occurred nearby, or they could use the technology for disproportionate and highly invasive surveillance of marginalized communities. Face recognition could be deployed absent any suspicion of wrongdoing and with nefarious goals driving its use, so long as those nefarious goals were not the sole reason for doing so. Requiring a mere nexus to legitimate law enforcement goals is insufficient to prevent abuse, and it is not a standard the legislature should accept for such a powerful surveillance technology.

While SB 762 would institute some important rules that would be significant improvements over the status quo — which we discuss below — the bill cannot be viewed as a comprehensive or sufficient response to the dangers of face recognition without a warrant requirement. We strongly urge the committee to amend the legislation and add this critical safeguard.

Limit Use of Face Recognition to Investigating Serious Crimes

Another key pillar of effective safeguards on face recognition is limiting its use to the investigation of serious crimes. The concept of limiting use of powerful surveillance tools to top-tier investigations has clear precedent: It has been applied for over 50 years in similar surveillance contexts such as wiretapping.⁴

Face recognition should not be used to stockpile suspects for investigation of minor offenses.

In many places, police already use face recognition to investigate minor offenses such as shoplifting less than \$15 of goods or stealing a pack of beer.⁵ These low-profile cases often receive little scrutiny, so it is more likely that erroneous uses of face recognition — which can stem from a variety of causes such as algorithmic bias, poor image quality, lax software settings, or even pseudo-scientific techniques⁶ — will go unnoticed. For minor offences, it's also more likely that potentially exculpatory evidence will not be sought out. This is especially concerning because face recognition can be notoriously inaccurate, especially for women and people of color.⁷

⁴ 18 U.S.C. § 2510 et seq.

⁵ Drew Harwell, “Oregon became a testing ground for Amazon’s facial-recognition policing. But what if Rekognition gets it wrong?” *Washington Post*, April 30, 2019, <https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/>; Ebony Bowden, “How cops used a photo of Woody Harrelson to catch a beer thief,” *New York Post*, May 16, 2019, <https://nypost.com/2019/05/16/how-cops-used-a-photo-of-woody-harrelson-to-catch-a-beer-thief/>.

⁶ Police sometimes use face recognition in unreliable ways, such as to conduct scans on sketches, computer-edited images, or even celebrity lookalikes. Clare Garvie, “Garbage In, Garbage Out: Face Recognition on Flawed Data,” Georgetown Law Center on Privacy & Technology, May 16, 2019, <https://www.flawedfacedata.com/>.

⁷ Patrick Grother, Mei Ngan, Kayee Hanaoka, National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR 8280 (December 19, 2019), 2, <https://doi.org/10.6028/NIST.IR.8280>; Joy Buolamwini and Timnit Gebru, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,” *Proceedings of Machine Learning Research*, vol. 81 (2018), <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>; Joy Buolamwini and Inioluwa Deborah Raji, “Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products,” AIES ’19: *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society* (2019), <https://www.media.mit.edu/publications/actionable-auditing-investigating-the-impact-of-publicly-naming-biased-performance-results-of-commercial-ai-products/>; Jacob Snow, “Amazon’s Face Recognition Falsely Matched 28 Members of Congress With Mugshots,” American Civil Liberties Union, July 26, 2018, <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>; Brendan Klare et al., “Face Recognition Performance: Role of Demographic Information,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6 (December 2012), <http://openbiometrics.org/publications/klare2012demographics.pdf>.

A serious crime limit for face recognition would also prevent the misuse of discretionary powers, including selective targeting of marginalized communities and dissidents. For example, in 2015, as demonstrators protested the death of Freddie Gray in police custody, Baltimore police used face recognition to target protesters, scanning the crowd with the technology to find and arrest anyone who had an outstanding warrant for any offense.⁸ Without a serious crime limit, face recognition could be used in this manner on a broad scale, weaponized for selective enforcement of bench warrants for minor offenses and targeted at marginalized communities, political dissidents, and other vulnerable individuals. This can already be seen in autocratic regimes such as China, which uses face recognition for social control, deploying the technology to catalog minor offenses and then to engage in public shaming.⁹

By restricting use of the technology to investigating violent crimes, SB 762 makes a meaningful contribution to mitigating these risks while still permitting limited use for investigating offenses, such as homicides, that are genuine public safety priorities.¹⁰

Prohibit Face Recognition from Being Used as the Sole Basis for an Arrest

In addition to the measures above designed to prevent abuse and excess surveillance, effective safeguards on face recognition must also include policies that prevent excess reliance on the technology, which can be prone to error. There are already numerous documented instances when a face recognition misidentification led to a wrongful arrest.¹¹ While a probable cause warrant to run scans provides significant value, it does not prevent the harms that can arise when law enforcement excessively relies on the results of searches.

Factors that reduce image quality, such as bad lighting, indirect angles, distance, poor cameras, and low image resolution, all make misidentifications more likely. Lax system settings, such as employing a lower confidence threshold to trigger matches¹² or having broad sets of matches appear in search results, increase the potential that law enforcement will receive erroneous matches as well. Even as face recognition software improves in quality — and even if algorithmic bias dissipates — there will always be situation-based limits to how effective the

⁸ Kevin Rector and Alison Knezevich, “Social media companies rescind access to Geofeedia, which fed information to police during 2015 unrest,” *Baltimore Sun*, October 11, 2016, <https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html>.

⁹ Alfred Ng, “How China uses facial recognition to control human behavior,” *CNet*, August 11, 2020, <https://www.cnet.com/news/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/>; Dave Davies, “Facial Recognition And Beyond: Journalist Ventures Inside China’s ‘Surveillance State,’” *NPR*, January 5, 2021, <https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta>.

¹⁰ Sec. 2-503(A)(1)(I).

¹¹ Kashmir Hill, “Wrongfully Accused By An Algorithm,” *New York Times*, June 24, 2020, <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>; K. Holt, “Facial recognition linked to a second wrongful arrest by Detroit police,” *Engadget*, July 10, 2020, <https://www.engadget.com/facial-recognition-false-match-wrongful-arrest-224053761.html>; Kashmir Hill, “Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match,” *New York Times*, December 29, 2020, <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>.

¹² Confidence thresholds are a metric built into face recognition systems that acts as a scale for comparing which photos are more or less likely to be a match within that system. When face recognition systems are set to return results at lower confidence thresholds, it leads to matches that are more likely to be misidentifications. Jake Laperruque, “About-Face: Examining Amazon’s Shifting Story on Facial Recognition Accuracy,” Project On Government Oversight, April 10, 2019, <https://www.pogo.org/analysis/2019/04/about-face-examining-amazon-shifting-story-on-facial-recognition-accuracy/>.

technology is. And there will always be a danger in giving too much credence to matches that could misidentify innocent individuals.

SB 762 sets forth a clear requirement that “results generated by facial recognition technology may not serve as the sole basis to establish probable cause or the positive identification of an individual.”¹³ Such a rule would prevent face recognition matches from being the sole basis of an arrest, as well as guard against overreliance on matches leading to other invasive police actions, such as searches of private property. This is a key safeguard to preventing harm from overreliance on face recognition misidentifications, and a reform that has already been enacted as a rule in multiple states.¹⁴ We applaud the bill for including this important measure.

Require Defendants Be Given Notice When Face Recognition Is Used

Like any other complex forensic tool, face recognition’s effectiveness can depend on technical factors and manner of use. That is why it is critical that defendants are notified and given the opportunity to examine face recognition technology whenever it is used in an investigation.

Defendants have a vested interest in reviewing a variety of factors — such as algorithm quality, the software settings police used, and whether any other potential matches were discovered or investigated — that could provide exculpatory or mitigating evidence. Guaranteeing access to this information is not only critical for due process rights but also acts as an important safeguard to deter corner cutting and sloppy use of face recognition during investigations.

Despite the importance of disclosure, it rarely occurs.¹⁵ In some jurisdictions, law enforcement uses facial recognition thousands of times per month, and defendants almost never receive notice of its use in investigations.¹⁶ Yet even as law enforcement relies on the technology for investigations, they obscure it from examination in court by defendants and judges.¹⁷

SB 762 requires that the government disclose whenever face recognition has been used in the course of an investigation.¹⁸ This requirement would protect due process rights and strongly incentivize law enforcement to adhere to the highest standards in their use of face recognition.

Prohibit Face Recognition from Being Used for Untargeted Surveillance

One especially dangerous form of face recognition is in its use not to identify a designated person in an image, but rather to conduct untargeted scans of all individuals on video streams.

¹³ Sec. 2-502(B)(1)(I).

¹⁴ Maine and Washington have both enacted laws prohibiting face recognition from being the sole basis for establishing probable cause for searches and arrests, and state lawmakers in Hawaii have introduced legislation including this policy. L.D. 1585, 130th Leg. (Me. 2021); S.B. 6280, 66th Leg. (Wash. 2020); H.B. 1226, 31st Leg. (Haw. 2021).

¹⁵ Aaron Mak, “Facing Facts,” *Slate*, January 25, 2019, <https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html>.

¹⁶ Jennifer Valentino-DeVries, “How the Police Use Facial Recognition, and Where It Falls Short,” *New York Times*, January 12, 2020, <https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html>.

¹⁷ Face recognition “can play a significant role in investigations, though, without the judicial scrutiny applied to more proven forensic technologies.” Jennifer Valentino-DeVries, “How the Police Use Facial Recognition, and Where It Falls Short,” *New York Times*, January 12, 2020, <https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html>.

¹⁸ Sec. 2-504.

According to early testing, untargeted face recognition is notoriously inaccurate: In pilot programs in the United Kingdom, South Wales Police had a 91% error rate, and London Metropolitan Police had a 98% error rate.¹⁹ In the United States, the technology has not received any type of comparable tests or vetting.

Yet even if untargeted face recognition improves in accuracy, it would still present a serious threat to civil rights and civil liberties. This type of surveillance system could effortlessly monitor and catalogue individuals' movements, interactions, and activities on a mass scale.

SB 762 prohibits law enforcement from using face recognition “for the purpose of live or real-time identification of an image or a recording.”²⁰ This is a valuable rule that would help preempt the danger of untargeted face recognition being deployed for general public surveillance.

However, we believe that to ensure the spirit as well as the letter of this provision is followed, minor adjustments to the text should be made. While the goal of the bill appears to be preventing untargeted surveillance, because the text centers on “real-time identification,” law enforcement might argue it is permitted to conduct mass crowd scanning of video after events occurred, or even in a near real-time format subject to a small tape delay.

This type of activity would still involve the mass risk of error that comes with untargeted face recognition, as well as the risk of mass identification of crowds at sensitive events and locations, such as a protest, political rally, or religious ceremony. We urge the committee to amend this provision to make clear that it prohibits using face recognition for any form of untargeted surveillance and crowd-scanning, even when performed on a video feed that is not live.

Thank you for the opportunity to submit testimony on this important legislation. We encourage you to issue a favorable report on the bill with the proposed amendments in order to protect Maryland residents from unchecked face surveillance. We need strong safeguards to ensure that this technology does not infringe on civil rights and civil liberties, and this legislation offers an effective path for achieving that important goal.

¹⁹ Big Brother Watch, *Face Off: The Lawless Growth of Facial Recognition in UK Policing* (May 2018), 3-4, <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf>.

²⁰ Sec. 2-503(A)(I)(V).

SB0762_kk_fwa.pdf

Uploaded by: Katie Kinsey

Position: FWA

To: The Honorable William C. Smith, Jr.; Members of the Senate Judicial Proceedings Committee

From: Katie Kinsey, Staff Attorney, The Policing Project at NYU School of Law

Date: March 10, 2022

Re: SB0762 – Criminal Procedure – Facial Recognition Technology – Requirements, Procedures, and Prohibitions

Position: FAVORABLE WITH AMENDMENTS

Chairman Smith, Vice Chair Waldstreicher and members of the Judicial Proceedings Committee: thank you for the opportunity to submit testimony on this Bill, which seeks to regulate law enforcement use of facial recognition technology (FRT). My name is Katie Kinsey, and I am a staff attorney at the Policing Project at New York University School of Law, an organization dedicated to partnering with communities, policymakers, police, and technology companies across the country to bring democratic accountability to policing. By democratic accountability we mean that the public has a voice in setting transparent, ethical, and effective policing policies **before** the police act. This hearing is a great example of democratic accountability in action, and I am grateful to participate.

In my testimony, I would like to make three overarching points:

1. Although we do not know whether the benefits of FRT outweigh its costs, we are certain that the unregulated status quo in Maryland around FRT use is unacceptable. There is an urgent need for the type of comprehensive, nuanced legislation before this Committee.
2. The public deserves to know whether FRT works as it actually is used by law enforcement. To ensure this, the Bill should be amended to require operational testing.
3. This Bill also should be amended to centralize FRT review in a single state agency, with use authorized only for a limited period of time during which its impact on public safety should be evaluated.

I. There is an urgent need to regulate law enforcement use of FRT

Since the inception of Maryland’s facial recognition program in 2011, law enforcement’s use here—as in most of the country—has been almost entirely unregulated. Police have acquired and used this technology in secretive ways, without adequate guardrails. In Maryland, this has included using FRT to target

individuals exercising their First Amendment rights.¹ Unsurprisingly, this non-transparent approach has bred public mistrust, especially in Black communities and marginalized communities, which already feel the brunt of many unfortunate policing practices. In short, unregulated law enforcement use of FRT is a recipe for harm – and it is undemocratic.

Although we have some suggestions for strengthening this Bill, I want to state clearly that I believe it contains meaningful safeguards designed to mitigate some of the greatest risks to citizens’ civil liberties and civil rights, and to racial justice. In particular, the crime restrictions set forth in section 2-503 should help ensure that FRT use does not exacerbate this country’s epidemic of overcriminalization. And section 2-504’s requirement that FRT use be disclosed to the accused in discovery will help protect these individual’s due process rights. Marylanders will be safer if you pass this Bill.

II. Legislation should require and facilitate operational testing

FRT is a powerful and expensive tool that raises serious risks for civil rights, civil liberties, and racial justice concerns. The public deserves to know whether it actually works.

And to know whether FRT works in practice requires testing it for accuracy and bias in actual uses contexts – i.e., assessing FRT as actually deployed with a human-in-the-loop, on the quality of images actually searched, the size of database searched and so on. This type of assessment is called “operational testing.”

As currently drafted, this Bill does not require any accuracy or bias testing. We would suggest amending section 2-506 to address the need for testing in two ways: (1) require that the Department of Public Safety (DPS) only approve a vendor that has demonstrated high accuracy across demographic groups on the National Institute of Standards and Technology’s (NIST) independent, expert testing of facial recognition algorithms; and (2) create a task force to develop an operational testing protocol to ensure the approved FRT system works in practice.

NIST’s testing is the gold standard for assessing facial recognition *algorithms*; as such, its evaluations can serve an important gatekeeping function when vetting vendors.² You should add a NIST testing requirement to this Bill.

But NIST doesn’t conduct operational testing. To start, NIST does not evaluate the humans-in-the-loop part of FRT use, so its tests don’t tell us about actual system performance. In addition, most of the images NIST tests (86%) are “excellent” portrait quality photos and not the low-quality surveillance camera images that law enforcement typically uses for FRT searches.³ This discrepancy matters because image quality has a

¹ Jameson Spivack, Maryland’s face recognition system is one of the most invasive in the nation, Baltimore Sun (Mar. 9, 2020), <https://www.baltimoresun.com/opinion/op-ed/bs-ed-op-0310-face-recognition-20200309-hg6jfkfav2fdz3ccs55bvqjtnmu-story.html>.

² See, e.g., Kate Kaye, This little-known facial-recognition accuracy tests has big influence, iapp (Jan. 7, 2019), <https://iapp.org/news/a/this-little-known-facial-recognition-accuracy-test-has-big-influence>.

³ Patrick Grother et al., Face Recognition Vendor Test (FRVT) Part 2: Identification, NIST (Feb. 23, 2022), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf at 7, 19; see e.g., IJIS Institute & IACP, Law Enforcement Facial Recognition Use Case Catalog (Mar. 2019), https://www.theiacp.org/sites/default/files/2019-10/IJIS_IACP%20WP_LEITTF_Facial%20Recognition%20UseCasesRpt_20190322.pdf.

huge impact on accuracy. As NIST itself has explained, “While publicly available test data from NIST and elsewhere can inform owners, it will usually be informative to *specifically measure accuracy of the operational algorithm on the operational image data.*”⁴

This means that truly meaningful evaluation requires operational testing. And this is where it gets trickier. Currently, there are neither standards nor an agreed-upon method for operational testing. There are some resources to work from, such as the NIST-backed Facial Identification Scientific Working Group’s operational testing protocol.⁵

Luckily, this body is uniquely positioned to address this issue by commissioning a group of diverse subject matter experts—including computer science academics, technologists, and public defenders—to develop an operational testing protocol. Once this operational protocol is developed, DPS—which the Bill already charges with sole authority to select an FRT vendor—should incorporate this protocol in its vetting process.

III. Centralize FRT review and only authorize use for a limited duration to assess impact

At the Policing Project, our evaluation of any policing technology starts with a basic question: will the public benefit from the use of this tool? If a technology has identifiable, concrete benefits then we can begin to address costs and ways to mitigate them before it is used.

Current law enforcement use of FRT has inverted this analytical process – applying a deploy first, assess benefit later (if ever) approach. What is needed instead is a full accounting of how FRT is being used, and an evaluation of the technology’s impact on public safety. This evaluation should include a real commitment to stop use if the public safety benefits do not outweigh the costs, or the most serious costs – such as those to racial justice interests – cannot be mitigated. Fortunately, section 2-510 of this Bill already takes huge strides in the right direction by requiring comprehensive data collection and reporting requirements on agencies’ FRT use.

We urge one addition to the data collection mandated by section 2-510: add a requirement for agencies to track and report investigative outcomes from any leads generated from FRT – e.g., the number of arrests and convictions that FRT leads contributed to, by crime type.

We also urge that you amend this Bill to take two additional steps. (1) Centralize FRT use in a single state agency, such as DPS. Centralizing FRT in a single agency rather than permitting individual agencies to conduct searches would facilitate a consistent training standard, consolidate expertise, and concentrate the data collection process rather than placing the burden on individual agencies. (2) Authorize use under the terms of this Bill for a limited trial period during which impact is assessed. The careful, transparent data collection envisioned by section 2-510 will enable an assessment of benefits and costs. And this assessment will allow you to see which safeguards are working, which require modification, or whether the program should be scrapped entirely because benefits do not outweigh the costs, or the most serious costs – such as those to racial justice interests – cannot be mitigated.

⁴ Patrick Grother et al., Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NIST (Dec. 2019), <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf> at 3 (emphasis added).

⁵ Understanding and Testing for Face Recognition Systems Operational Assurance, FISWG, https://fiswg.org/fiswg_understanding_&_testing_for_frs_operatnl_assur_v1.0_2020.12.11.pdf.

Thank you again for the opportunity to testify today. The Bill you are considering is extremely consequential. We would be happy to provide any other information that could be useful.

Microsoft Testimony - SB 762.pdf

Uploaded by: Owen Larter

Position: FWA

SB 762 - Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions

FAVORABLE WITH AMENDMENT

Chairman Smith and members of the Judicial Proceedings Committee, Microsoft appreciates the opportunity to provide testimony in favor of SB 762. We would like to thank Senator Sydnor and Delegate Moon for their leadership on this important issue of ensuring that facial recognition technology is used responsibly and believe this bill is an important step forward in giving people protection under the law. Through this bill, Maryland has the opportunity to set itself apart as only the second state in the United States to establish specific guardrails to ensure that the use of facial recognition technology by law enforcement is rights-respecting, transparent, and accountable.

Facial recognition can provide many benefits to society, including helping secure devices and assisting people who are blind or with low vision access more immersive social experiences. In the public safety context, it can be used to help find victims of trafficking, or as part of the criminal investigation process.

However, without clear guardrails that have the force of law, facial recognition technology can also pose potential risks to individuals and society. There are three important types of potential risks around facial recognition technology:

- A risk of bias and unfair performance, including across different demographic groups;
- the potential for new intrusions on people's privacy; and
- possible threats to democratic freedoms and human rights.

Microsoft is clear-eyed about the risks posed by facial recognition technology. Since 2018, we have engaged in an expansive program of work to design and enact effective safeguards to help secure its responsible use. This has included the internal adoption and implementation of Facial Recognition Principles¹ and the development of our Face API Transparency Note.² The Transparency Note helps customers make informed decisions about how best to responsibly deploy our facial recognition service. It communicates, in understandable language aimed at non-technical audiences, how Face API works and factors that will affect system accuracy. It also emphasizes the need to think about the whole system during deployment, including the importance of having a human in the loop.

In addition to these safeguards, Microsoft continues to believe that there is an urgent need for regulation. This need is particularly acute in the law enforcement context, given the consequential nature of the decisions that police take.

¹ Microsoft, *Six Principles for Developing and Deploying Facial Recognition Technology*, <https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2018/12/MSFT-Principles-on-Facial-Recognition.pdf>.

² Microsoft AI, *Transparency Note: Azure Cognitive Services: Face API (2019)*, [https://azure.microsoft.com/mediahandler/files/resourcefiles/transparency-note-azure-cognitive-services-face-api/Face%20API%20Transparency%20Note%20\(March%202019\).pdf](https://azure.microsoft.com/mediahandler/files/resourcefiles/transparency-note-azure-cognitive-services-face-api/Face%20API%20Transparency%20Note%20(March%202019).pdf).

Microsoft strongly believes that facial recognition should not be deployed by police without specific civil liberties protections and safeguards in relation to transparency and accountability, testing, and human review. Microsoft believes this bill introduces some important safeguards, including:

- **Robust civil liberty protections**, such as restricting the use of facial recognition to establishing probable cause or positive identification in relation to only the most serious crimes, and only in conjunction with other independently obtained evidence. The prohibitions on real-time identification and the use of facial recognition on an individual suspected of being a juvenile provide further important protections, as does the prohibition on using the technology on the basis of an individual's engagement in lawful activity or their race, color, religious beliefs, sexual orientation, gender, disability or status as being homeless.
- **Transparency and accountability requirements**, such as the need for an agency to adopt a model policy on facial recognition use and a use and data management policy. It will be important that these policies are developed in a way that ensures police can identify and address risks around a system and keep data secure. The need to complete an annual audit to determine compliance with the law and use policies is also important, as is the restriction of facial recognition searches to high quality images in drivers' license and mugshot databases, which will deliver better quality results and transparency around the databases police are searching.
- **Important requirements around human review** of facial recognition output and the training and testing of the reviewer.

We do, however, think the bill can be strengthened, most notably by requiring two types of testing of facial recognition systems. First, the bill should require that vendors offering facial recognition services enable legitimate and reasonable third-party testing of their services. This is critical given the wide variation in accuracy across vendor offerings³. Third party testing is therefore needed to ensure law enforcement can identify high performing systems that can be trusted by the public to perform accurately, including across different demographic groups.

Second, the bill should require agencies deploying facial recognition to subject those systems to operational testing prior to deployment in the environment in which they will be used. This is because environmental factors like lighting and camera positioning have a material impact on accuracy. Requiring that systems are tested and that any gaps in performance are addressed is therefore vital in ensuring police are using technology in a way that builds public trust.

Microsoft believes this bill represents important progress. We recognize that it is the product of an ongoing conversation between lawmakers, civil society and law enforcement which we have welcomed the opportunity to contribute to. We look forward to continuing to contribute to this effort, now and in the future, with a view to building out safeguards for the responsible use of facial recognition that are robust and durable over the long term.

³ National Institute of Standards & Technology, Face Recognition Vendor Test (FRVT) (2022) 5, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

MCPA-MSA_SB 762 Facial Recognition _Oppose.pdf

Uploaded by: Andrea Mansfield

Position: UNF



Maryland Chiefs of Police Association Maryland Sheriffs' Association



MEMORANDUM

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

FROM: Chief of Staff David Morris, Co-Chair, MCPA, Joint Legislative Committee
Sheriff Darren Popkin, Co-Chair, MSA, Joint Legislative Committee
Andrea Mansfield, Representative, MCPA-MSA Joint Legislative Committee

DATE: March 10, 2022

RE: **SB 762 – Criminal Procedure - Facial Recognition Technology -
Requirements, Procedures, and Prohibitions**

POSITION: **OPPOSE**

Since July 2021, the Maryland Sheriffs' Association (MSA) and the Maryland Chiefs of Police Association (MCPA) were pleased to participate with other stakeholders in a facial recognition working group formed by Senator Sydnor and Delegate Moon, at their request. Although there has been some productive dialogue over the last six months, the group has been unable to reach a consensus regarding a mutually agreeable bill. This has resulted in the production of a bill which restricts law enforcement's legitimate use of the technology, and we feel it is imperative that changes be made to SB 762. If changes are not made to this bill, public safety and crime victims could be adversely affected. Therefore, the MSA and the MCPA **OPPOSE SB 762** in its current form.

Maryland law enforcement has successfully used facial recognition technology for many years. We recognize that there are misunderstandings surrounding facial recognition technology and its uses. There are many false narratives fueled by Hollywood portrayals which vastly misrepresent how law enforcement agencies legitimately use facial recognition. For example, facial recognition in Maryland is not used as ongoing government surveillance and it's not connected real time to live CCTV, Drone, Aviation or Body Worn Camera video. In reality, the facial recognition is primarily used in criminal investigations following an incident and under a process that requires a great deal of manual, human analysis, and an image of a sufficient quality to make a possible match.

The MCPA and MSA support the intention of the bill to establish safeguards for government use of the technology and we agree there should be use restrictions to ensure there is no intrusion on constitutionally protected activities. The successful use of facial recognition technology in Maryland has aided in the identification of people whose images have been recorded

on-camera committing robberies, burglaries, car jacking's, assaults, rapes, sexual assaults, shootings, homicides, kidnappings, hate crimes, human trafficking, sexual exploitation, threats of mass violence and other serious crimes. The technology has also been used to identify missing persons, deceased persons, incapacitated persons who can't identify themselves and to mitigate an imminent threat to health or public safety (e.g., to thwart an active terrorism scheme or plot).

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

Facial recognition is not an absolute science. It is not quantifiable like DNA, so while any potential match results will greatly contribute to the investigation, it will provide a tentative investigative lead only. When used in combination with human analysis and additional investigation, we have seen facial recognition technology is a proven valuable tool in solving crimes and increasing public safety.

We do not support SB 762 mandating the use of a single facial recognition technology, which would limit photo sources to certain images which will have a clear and immediate negative impact on public safety. Due to the complexity of investigating crimes such as human trafficking and child sexual exploitation, there are some law enforcement agencies in the state using more than one facial recognition system, searching databases beyond driver's license, identification cards and booking photos. People who engage in this and other criminal activity often travel from out of state to commit crimes. Limiting use to a single facial recognition technology would prevent law enforcement from leveraging other legally obtained photos such as photos from other states and open-source photos which could assist with the identification of human trafficking/sexual exploitation victims, and individuals traveling from far outside the area to commit crime, as we saw with the unrest at the U.S. Capitol on January 6 last year.

We support ensuring that facial recognition alone does not constitute probable cause. However, it may generate investigative leads through a combination of biometric comparisons and human analysis. Investigators have to do the work, not the technology. The technology is used when there is already an investigation underway. We support that an arrest should not be made until the assigned investigator establishes, with other corroborating evidence, that the person identified by the photo match is the perpetrator in an alleged crime.

Facial recognition is a valuable time saving tool. Under traditional methods, law enforcement sought to identify an unknown person of interest during an investigation by manually looking through hundreds of mugshots with victims, canvassing areas with photos or searching a database using limited information. When time was crucial, the Anne Arundel County Police developed a tentative identification of the Capital Gazette shooter by using facial recognition technology to generate a lead. He was successfully identified, and later charged and convicted based on other evidence. Let us not forget, when the need arose to expeditiously make tentative

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

identification of persons involved in the unrest at the U.S. Capitol, the technology generated many investigative leads which when corroborated by additional investigative information led to the arrests and convictions of individuals who attacked our democracy.

The MCPA and MSA fully support strict guardrails and audit protocols to mitigate the risk of impartial and biased law enforcement and misuse of the technology, without eroding current investigative capabilities that have proven their worth. For example, we support the development of a model statewide use policy and ensuring relevant training in the use of the technology, as well as providing complete transparency through public reporting by agencies using the technology.

However, as currently drafted, SB 762 contains several provisions that would unacceptably impact public safety in Maryland as well as hamper effective implementation of the requirements. We are unable to support the bill without key revisions. With the changes, SB 762 would be the strongest measure in the country for regulating the use of facial recognition technology used by law enforcement agencies, while addressing public concerns and preserving proven capabilities.

We applaud Senator Sydnor for his willingness to listen to participants in the facial recognition working group and we remain open to further discussion. However, SB 762 as it stands limits the use of the technology, prevents human trafficking and juvenile victims from being identified and restricts law enforcement's ability to effectively investigate cases.

For aforementioned reasons, the MCPA and MSA **OPPOSE SB 762** and urge an **UNFAVORABLE** Committee report.

MARYLAND SUCCESS STORIES

(Shared by Maryland law enforcement agencies utilizing facial recognition technology)

VICTIM IDENTIFICATION

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

RESPONDING TO HEALTH EMERGENCIES

- Local law enforcement responded to a **health emergency involving an individual at the College Park Airport**, with no shirt, shoes or mask, stating that they wanted to "fly to outer space/the stars" but the subject left the area before units arrived. An officer was able to locate the subject after subsequent calls from concerned citizens nearby; however, they had no identification and could not communicate coherently. An image was taken of the subject and queried, producing a potential matching female identity. At first, officers on the scene believed it was not a match because the individual was male. Upon further investigations the lead proved correct, as the transgender man's identity was confirmed by his father, who had been contacted in another state. The man had reportedly not been the same since taking LSD the previous week. He was reunited with a family member and then taken to a local hospital for evaluation.
- **An unknown person in Annapolis, MD was posting plans to commit suicide on open sources.** Reports were made to the police by concerned persons who saw this post. Due to what was written, police believed a suicide was eminent and attempted to identify this person using a still image from open sources. This image was used with facial recognition technology and generated a lead through a driver's license photo. Through further investigation, the suicidal person was identified and the police and a crisis team were sent to the person's address. Police were able to locate the suicidal person and they were provided with assistance.

SOLVING SEX CRIMES

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

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

- **In 2021, an unknown subject went to the front door of a residence and began sexually stimulating himself in front of a security camera.** The use of facial recognition by Montgomery County Police Department provided an investigative lead – a person that had conducted the same behavior in front of a 72-year-old female neighbor two years prior. Upon further investigation, the case resulted in a confession by the suspect and criminal charges related to the indecent exposure.
- **In 2021, an unconscious subject was reported in Montgomery County.** Responding officers found a disoriented pregnant female subject who was unable to recall anything from the past two days. Eventually, the female victim was able to recall potentially being drugged, and later, an unknown suspect forcing oral and vaginal sex. Facial recognition was used to generate a lead from a photo of the suspect available from security cameras nearby. This case is still ongoing as of this writing, so no further information can be provided.

SOLVING VIOLENT CRIME

- **Local law enforcement investigated a violent assault on public transportation in Baltimore.** Images of the suspect and the incident were obtained through security camera footage from the coach. Information was disseminated to law enforcement partners seeking assistance with the case. A comparison was made with a law enforcement database, and an investigative lead was developed and provided to the investigating agency. Upon further investigation it led to the arrest of the assailant who was identified by the victim.
- **In Annapolis, MD the “Capitol Gazette Killer” Jarrod Ramos** was angered by a story the *Capital Gazette* ran about him in 2011 and brought a lawsuit against the paper for defamation, which a judge later dismissed. In 2018, **Ramos entered the newspaper’s headquarters in Annapolis, Maryland with a shotgun and killed five employees, leaving two others critically injured.** Anne Arundel County Police faced a perfect storm of problems when they took the suspected gunman into custody: the man had no identification, he wouldn’t speak to investigators, and a fingerprint database was not immediately returning any matches. Detectives obtained an image of Ramos and used facial recognition which generated a lead in the case. Through further investigation, detectives were able to positively identify Ramos and search warrants were conducted at this residence. He plead guilty in the case and was sentenced to five consecutive life sentences.
- **In 2015, two suspects armed with guns walked into a Towson liquor store and announced a robbery,** taking aim at a 68-year-old clerk. The clerk, fearing for his life, pulled out a gun and shot one of the people robbing the store, who was later pronounced dead at the scene. The second person involved in the robbery got away. The police then went to work to identify the second suspect. Through social media, detectives were able to find an image of a person of interest who was a friend of the other person involved in the robbery. The police entered this photograph into facial recognition which returned a tentative lead. Through further investigation the second person involved in the

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

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

FIGHTING ORGANIZED CRIME AND GANG VIOLENCE

- **Local law enforcement in Maryland requested assistance with a firearms trafficking investigation, providing an image of a suspect.** The image was run against a law enforcement database and a potential lead was developed. Upon further investigation, detectives positively identified the suspect and executed a search warrant that resulted in the seizure of drugs, guns and ammunition.
- **A retailer reached out to law enforcement with information about an organized theft crew that had been targeting stores throughout Virginia, D.C. and Maryland.** An image provided showed a male with unique tattoos on his neck and left hand. Facial recognition was used to generate a lead in the case. Upon further investigation, the individual was subsequently identified and charged.
- **Throughout 2019 and 2020, local law enforcement conducted a homicide/gang investigation involving a violent group responsible for multiple homicides, drug distribution, kidnapping, and robbery in Anne Arundel County.** Digital images of persons of interest were obtained and with the assistance of facial recognition, law enforcement was able to generate leads regarding three individuals involved. Through further investigation, individuals were positively identified and probable cause was established to obtain a wiretap warrant. Though subsequent monitoring of communications, law enforcement was able to prevent at least three shootings, as well as interrupt a kidnapping. As a result of the investigation over a dozen people were indicted and successfully prosecuted, multiple firearms were recovered including an assault rifle, drugs and a significant amount of U.S. currency were also seized.

PREVENTING IDENTITY THEFT

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

SOLVING FIREARMS TRAFICKING

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

SOLVING BURGLARIES

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

SOLVING DAMAGE TO MULTIPLE POLICE VEHICLES

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

ADDITIONAL NOTE - TOOLS TO ANALYZE OPEN-SOURCE INFORMATION ARE CRITICAL TO PREVENTING MASS VIOLENCE AND DOMESTIC TERRORISM

EL Paso, TX Walmart Shooting – A 21-year-old man was arrested at the scene of a shooting in El Paso, near the US-Mexico border. He is believed to have posted an online document calling the attack a response to "the Hispanic invasion of Texas". The El Paso gunman opened fire on a crowded Walmart with an assault-style rifle and surrendered after being confronted by police officers outside the store. Twenty-six people were injured in the shooting.

Parkland, FL School Shooting: On social media, Nikolas Cruz expressed his desire to perpetrate violence. Before he committed one of the worst mass shootings in US history at a Parkland, Florida, high school, Cruz wrote threatening social media posts. He made racist comments and said he would shoot people with his AR-15, singling out police and “anti-fascist protesters” as deserving of his vengeance. He stated his aspiration to become a “professional school shooter.” Prior to the school shooting, Cruz posted an online video talking about his plans.

Attack on Tree of Life Congregation in Pittsburgh, PA: Eleven people were killed and six others including four police officers were injured when a gunman opened fire during a baby-naming ceremony at the Tree of Life Congregation, a Synagogue in Pittsburgh. The shooter, Robert Bowers surrendered to the police. Bowers was linked to an account on social media that shared anti-Semitic messages. Before the killing in three short sentences, Bowers social media post revealed volumes about his hateful worldview and his motivation to kill.

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

Planning Political Violence: Cesar Sayoc, was arrested in connection with 13 explosive devices sent to prominent Democrats and he used sites like Twitter to share ultra-right-wing conspiracy theories about many of the people he targeted. That includes George Soros, a prominent Jewish philanthropist. The first device discovered was located at Soros' home.

Violent Racism: In 2014 Elliot Rodger a 22-year-old who killed seven in Isla Vista, California, uploaded a sprawling YouTube manifesto filled with hatred of young women and interracial couples. In this video, he discussed a day of retribution before committing the attacks. His parents found the open-source post but it was too late.

SB762.DPSCS.OPPOSE.pdf

Uploaded by: Catherine Kahl

Position: UNF



Department of Public Safety and Correctional Services

Office of Government and Legislative Affairs

45 Calvert Street, Suite 7A-C, Annapolis MD 21401
410-260-6070 • www.dpscs.state.md.us

STATE OF MARYLAND
LAWRENCE J. HOGAN, JR.
GOVERNOR

BOYD K. RUTHERFORD
LT. GOVERNOR

ROBERT L. GREEN
SECRETARY

RACHEL SESSA
CHIEF OF STAFF

SASHA
VAZQUEZ-GONZALEZ
ACTING DEPUTY
SECRETARY
ADMINISTRATION

WAYNE HILL
DEPUTY SECRETARY
OPERATIONS

CAROLYN J. SCRUGGS
ASSISTANT SECRETARY

GARY McLHINNEY
ASSISTANT SECRETARY

JENNIFER A. BESKID
DIRECTOR

BILL: SENATE BILL 762

POSITION: OPPOSE

EXPLANATION: This bill establishes requirements and procedures relating to the use of facial recognition. Further, the bill requires the Department to adopt and publish a statewide model policy and develop and administer a training program regarding the use of facial recognition.

COMMENTS:

- The Department of Public Safety and Correctional Services operates the State's prisons that house individuals sentenced to serve 18 months or longer. The Department also oversees the Division of Parole and Probation, which supervises individuals who are on parole or probation in the community. The Department also runs the Baltimore City Pretrial Complex that houses individuals awaiting trial.
- The Department houses the facial recognition program. The approximately 150 law enforcement agencies in the State use this tool to aid in the investigation of unknown individuals. It is up to each law enforcement agency to determine the circumstances of its use.
- Section 2-506 of the bill will require the Department to:
 - Adopt and publish a model statewide policy regarding the use of facial recognition.
 - Develop and administer a training program as well as proficiency testing as it pertains to the use of facial recognition technology in the courts and criminal investigations - including training and testing on cultural diversity and implicit bias.
 - **Review and approve a single facial recognition technology for use by law enforcement agencies in the State.**
- **The Department is concerned with the language in Section 2-506 as it is not in a position to determine the best and sole facial recognition technology for the approximately 150 law enforcement agencies in the State; especially as the Department is not aware of the**

technology maintained by each agency and its compatibility with existing facial recognition technology.

- Additionally, the bill states a law enforcement agency may not use or contract for the use of facial recognition technology for use in criminal investigations unless the technology is currently approved for use by the Department. As stated previously, the Department does not have knowledge of the technological capabilities of various law enforcement agencies nor is the Department able to determine what is the best resource for EACH agency when conducting criminal investigations.
- The Department of Public Safety and Correctional Services is NOT a law enforcement agency. As such, the Department should not drive policy on how law enforcement agencies use facial recognition, including approving what technology is used.
- The Department understands amendments to the bill may be forthcoming that would address the Department's concerns and could be supported.

CONCLUSION: For these reasons, the Department of Public Safety and Correctional Services respectfully requests the Committee vote **UNFAVORABLE** on Senate Bill 762.

SIA Concerns - MD SB 762 Facial Recongition Techno

Uploaded by: Jacob Parker

Position: UNF



March 10, 2022

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

Written Testimony of SIA in Opposition to HB 762, Regarding Facial Recognition Technology

Dear Chairman Smith and Members of the Senate Judicial Proceedings Committee:

On behalf of the Security Industry Association (SIA) I am writing to express our concerns with Senate Bill 762, as currently written. SIA is a nonprofit trade association in Silver Spring, MD that represents companies providing a broad range of security products and services in the U.S and throughout Maryland, including more than 30 companies headquartered in our state. Among many other companies, our members include the leading providers of facial recognition software available in the U.S.

Support for Ensure Responsible, Ethical and Non-Discriminatory Use

We believe all technology products must only be used for purposes that are lawful, ethical, and non-discriminatory. Since many advanced technologies offer both tremendous benefits and the potential for misuse, we support policies ensuring facial recognition it is only used for appropriate purposes and in acceptable ways. Public concerns about facial recognition technology have centered around law enforcement and fears the technology might be used inaccurately or inappropriately, or in ways that raise privacy and civil liberties concerns. We believe establishing foundational safeguards in statute, combined with more detailed requirements in agency procedural rules, is the most effective approach to ensuring effective and accountable use of this technology by law enforcement. We support such policies consistent with *SIA's Principles for the Responsible and Effective Use of Facial Recognition Technology*,¹ and many comprehensive use policies put in place by leading agencies in Maryland and around the country.

SB 762 Should Establish Rules, Not Eliminate Current Capabilities

While the intention of the bill is to establish safeguards for law enforcement use of the technology, several provisions will also have the effect of eliminating current investigative tools being leveraged successfully by Maryland law enforcement. These are critical at a time of rising crime throughout the state, where shootings for example, have increased nearly 40% over the past year.

As written, the bill would deny investigators one method – but not others – of analyzing information that is already available to them. It's limitation to queries against mugshot or driver's license photos using "a single facial recognition technology," would only serve to hamper and delay investigations versus provide any public benefit. Investigators routinely query open-source information and records held by other agencies to help identify victims, witnesses or suspects that may have no prior criminal history or are from outside Maryland, especially when other methods result in dead ends. Related to this, the total prohibition on queries involving photos of minors will eliminate internet and dark web search tools essential to investigating human trafficking and child sexual exploitation. Additionally, while well

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

intentioned to limit “surveillance” use of the technology, the total prohibition on “live or real-time” use does not allow an exception for emergency situations when protecting lives demands being able to quickly identify a person of interest, such as during a terrorist attack. These harmful prohibitions simply must be addressed to avoid a significant negative impact on public safety in Maryland.

Support for Core Limitations and Transparency, Accountability Requirements

Facial recognition technology has been successfully utilized by Maryland law enforcement for over a decade, without a single instance of misidentification, misuse or false arrest. In fact, there are many documented success stories where the technology has been leveraged to help solve violent crime as well as assist citizens in need across our state, several of which have been shared with the Committee by Maryland law enforcement organizations. At the same time, there is a clear need for rules and other mechanisms that help address public concerns by helping ensure these technology tools are being leveraged in a lawful, effective, accurate and non-discriminatory manner that benefits our residents and communities. We support the core provisions of the bill that address primary public concerns as well as impose stringent transparency and accountability requirements on agencies using the technology, which:

- Prohibit law enforcement from using facial recognition match results as the sole basis to make an arrest, establish probable cause or make a positive identification.
- Ensure use of facial recognition technology in an investigation is discoverable in court proceedings.
- Exclude facial recognition results from use as evidence against a defendant.
- Prohibit use on images of individuals engaged in constitutionally protected activities, or based on their race, color, religious beliefs, sexual orientation, gender, disability and national origin.
- Require a statewide standard for agency policies on use of the technology.
- Require annual reporting and periodic audits from agencies using the technology that provide public transparency regarding how the technology is being used and the extent.

Third-Party Testing

Additionally, we understand that an amendment may be offered to the bill that would require providers of technology used by Maryland law enforcement to make the same technology available to any third party for testing. Not only would this make it difficult, if not impossible for law enforcement to be able to obtain and use needed technology, it is completely unnecessary as the accuracy of facial recognition technologies used in today’s law enforcement applications is evaluated by the U.S. government’s National Institute of Standards and Technology (NIST).

For over 20 years, the NIST Face Recognition Vendor Test Program, located here in Gaithersburg, MD, remains the world standard for objective, third party scientific evaluation, which provides an “apples to apples” comparison of the performance of facial recognition technologies. Despite claims that might be made to the contrary, the range of tests periodically conducted under the NIST program include those with relevance to law enforcement applications (notably the “Investigation Performance” tests), against images of varying quality (including mugshots, webcam, and “wild” images) and demographics, and using data sets similar to or larger in size than what would be available to law enforcement agencies (up to 12 million images). This federal program is used to validate technologies for U.S. government applications where highly accurate performance is critical to our national and homeland security.

Developers of facial recognition for law enforcement participate in the NIST program but do not make their technology publicly available, to ensure it is only used for intended purposes and does not fall into the wrong hands. For this reason, the requirement to provide an application programming interface (API) for third-party testing would specifically benefit specific vendors that already offer cloud-based “general purpose” software to the public. The result will be disruption for agencies using platforms that do not use cloud-based matching software – including Maryland’s current criminal records database. For these reasons, if a third-party testing requirement is added to the bill, we strongly urge that it specify participation in the NIST Face Recognition Vendor Test Program would satisfy this requirement.

The Accuracy of Facial Recognition

Calls for restricting use of the technology have often stemmed from misconceptions regarding its performance. While there is evidence that some, especially older versions of facial recognition technology have struggled to perform consistently across various demographic factors, the oft-repeated claim that it is *inherently* less accurate in matching photos of Black and female subjects simply does not reflect the current state of the science. In fact, the evidence *most* cited in the media is either irrelevant, obsolete, non-scientific or misrepresented.² An analysis of NIST test data from 2021 shows that each of the top 150 algorithms are over 99% accurate across Black male, white male, Black female and white female demographics, remarkable uniformity at high accuracy levels. For the top 20 algorithms, accuracy of the highest performing demographic versus the lowest varies only between 99.7% and 99.8%. For 17 of these algorithms, accuracy for white female, Black male and Black female are nearly identical at 99.8%, while they are least accurate for the white male demographic at 99.7%.³

The Case for Law Enforcement Use of Facial Recognition

In U.S law enforcement, facial recognition is used for a comparison search of records when the identity of the subject in an image is unknown, typically at the beginning stages of an investigation. It is used as a post-incident investigative tool to aid identification – not “surveillance.” The purpose is to generate or follow leads only and not to make a positive identification. Investigators compare “probe” images (such as photos lawfully obtained from a crime scene, no different from latent prints) against images in an established database for possible matches. However, unlike fingerprint and DNA matching, any potential facial recognition match result is not considered evidence. If an analyst using the software determines an image from a database likely matches a submitted image, investigators should use other means outside of facial comparison to provide confirming evidence needed to establish probable cause.

If the technology is not available, investigators will search arrest records by physical traits such as race and gender, as well as arrest history and other info, to narrow down search fields and possible identities before a visual examination of the photos in the records. However, as the importance of limiting human bias in police work becomes increasingly clear, biometric technology makes identification processes faster and more accurate than relying only on human analysis, subject descriptions, broadcasting suspect lookouts, public announcements or soliciting anonymous tips. Leading research⁴ tells us facial recognition is better at matching photos than humans can unassisted and that the highest accuracy results are achieved when combining technology and trained personnel.

Facial recognition has also been an indispensable tool for years in investigations of child sexual exploitation and human trafficking. There are several organizations that provide the technology to law enforcement investigators in Maryland as part of tools developed for searching online information to make identifications in these cases. For example, the Thorn organization’s Spotlight tool is credited with helping rescue more than 17,000 children⁵ from trafficking over the last four years. According to the National Child Projection Task Force,⁶ facial recognition technology is key to its mission of bringing exploited children to safety and sexual predators to justice, as it assists investigations around the country.

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

³ *ibid.*

⁴ <https://www.nist.gov/news-events/news/2018/05/nist-study-shows-face-recognition-experts-perform-better-ai-partner>

⁵ <https://www.thorn.org/spotlight/>

⁶ <https://baltimore.legistar.com/View.ashx?M=F&ID=9438739&GUID=911C7E85-D97A-4325-A008-77AE42D1098E>

Conclusion

On behalf of SIA and its members, we share the goal of ensuring responsible use of advanced technologies and would support policies ensuring that facial recognition is only used for appropriate purposes and in non-discriminatory ways. However, for the reasons above, we urge the Committee not to approve SB 762 in its current form, and instead first work to correct the issues identified above. We stand ready to provide any additional information or expertise needed as you consider these issues.

Respectfully,



Jake Parker

Senior Director, Government Relations

Security Industry Association

Silver Spring, MD

jparker@securityindustry.org

SB762UNFAVORABLEFacialRecognition3:10Sydnor.pdf

Uploaded by: Linda Diefenbach

Position: UNF

SB 762 UNFAVORABLE!

No Facial Recognition technology EVER!
From the bill: (B) (1) "FACIAL RECOGNITION TECHNOLOGY"

Linda Diefenbach
6742 Deer Spring Ln.
Middletown, MD

SB0762_IDSL_Testimony.pdf

Uploaded by: Yevgeniy Sirotin

Position: INFO

The Identity and Data Sciences Laboratory (IDSL)

at the Maryland Test Facility
1221 Caraway Ct. Suite 1070
Upper Marlboro, MD 20774

RE: Senate Bill 762 - Informational Only

March 8, 2022

On behalf of the Identity and Data Sciences Laboratory (IDSL) we are pleased to submit written informational testimony regarding Senate Bill 762 / House Bill 1046. We were also able to review and would like to comment regarding the amendment to be offered in the Judicial Proceedings Committee by Senator Sydnor. The IDSL is an independent research organization within Science Applications International Corporation (SAIC), specializing in independent test and evaluation of commercial biometric systems, including face recognition systems.

Since 2014, we have tested dozens of commercial biometric technologies in various government use-cases¹. Our research shows that, when commercial face recognition systems are used to establish the identity of individuals, they can make errors, sometimes conflicting with notions of 'fairness' or 'equitability'. While top performing systems can work well across demographic groups, our experience suggests that vendor-reported efficacy claims may not always align with real-world performance. There is also significant variation in performance across vendors.

Face recognition systems are complex and international standards define several types of biometric testing including technology testing, scenario testing, and operational testing. The different tiers of testing are needed because, in addition to the matching algorithm, performance of these systems depends on implementation details. These include gallery size, quality of the face photos used for matching, the demographics of the individuals in the photos, as well as the training of human reviewers of system results.

Maryland houses significant expertise in testing biometric systems. For example, the National Institute of Standards and Technology (NIST) in Gaithersburg runs the Face Recognition Vendor Test (FRVT) which performs technology testing of algorithms in isolation. The IDSL in Upper Marlboro has performed a variety of tests on behalf of the Department of Homeland Security Science and Technology Directorate (DHS S&T), but specializes in scenario testing, which tests full systems in a simulated environment. Both NIST and the IDSL have successfully integrated commercial systems into test infrastructure by asking vendors to implement a standardized API [**AMENDMENT NO. 2 (B) (1)**], to measure performance. No one type of testing is sufficient in isolation, however, our experience suggests the following approach [**2-506 (A) (3)**]: (1) Pick initial vendors based on NIST algorithm testing; (2) test vendor performance with scenario testing using operationally relevant images, galleries, and demographics (e.g., probes and reference galleries that reflect the sizes and demographics of those in Maryland's intended operational use); and (3) use test results to select a final vendor. Additionally, face recognition algorithms are updated frequently; once, purchased

¹ The IDSL staffs DHS S&T's Maryland Test Facility (MdTF). <https://mdtf.org>

those selecting the algorithm should validate if the specific version tested matches the version being purchased.

Testing of biometric systems requires a significant quantity of data. Test data may be gathered from new volunteers in a scenario test (typically hundreds of volunteers are needed for a statistically significant evaluation), or use previously acquired photos linked with ground truth self-reported demographic information and independently measured skin tone [**AMENDMENT NO. 2 (A) (1)**]. Web-scraped data are generally inappropriate as they are not linked with ground-truth demographic information. Ideally, data for testing should be acquired with informed consent as well as privacy protections. There are few appropriately labeled, responsibly collected, datasets of sufficient size to test modern face recognition systems along the subpopulations delineated in the amendment [**AMENDMENT NO. 2 (A)(1)**].

For these reasons, test datasets must remain sequestered. If technology developers have access to test datasets, they may use them in the creation of their algorithms. This will lead to good performance on tests for trivial reasons, like knowing the questions and answers on a test ahead of time. For this reason, sharing test data with technology developers is not considered good practice [**AMENDMENT NO. 2 (B) (3)**]. If test data is shared, subsequent testing would require all new data. If new operational data cannot be shared [**AMENDMENT NO. 2 (D)**], then these new data would have to be collected specially, which may carry significant costs.

Though international standards for testing biometric systems have existed since 2006, there is currently no standard methodology for testing biometric systems for fairness. Our group has examined these issues in great technical detail. Indeed, two of the authors of this letter (J.J.H. and Y.B.S.) are co-editors of a draft international standard on measuring demographic differentials in biometric system performance. There are many fairness metrics proposed for evaluating biometric systems, most of which include mathematical differences and ratios. Picking the right metric is extremely important to understand the result. For example, one can obtain large ratios of error rates observed between two groups (e.g., 10-100 times) even though differences between error rates are vanishingly small. More important still, there is no standard statistical criteria for determining what constitutes unfair difference in system performance. This criterion for what constitutes a “material” difference cannot come from a statistical or mathematical formula, it must be developed by policy [**AMENDMENT NO. 2 (B) (2)**].

Testing face recognition systems is needed to select appropriate commercial technologies and to ensure they work well within a specific use-case. We have provided similar information to a recent RFI from the White House Office of Science and Technology Policy (OSTP; attached). We hope this testimony will inform further development of this important legislation.

Very Respectfully,

On behalf of the Identity and Data Sciences Laboratory

Jerry L. Tipton, Executive Director, jtipton@idslabs.org

Yevgeniy B. Sirotin, PhD, Technical Director, ysirotin@idslabs.org

John J. Howard, PhD, Lead Data Scientist, jhoward@idslabs.org

ATTACHMENT:

**IDSL Response to the White House Office of Science and Technology Policy RFI
Document No: 2021-21975**

1.0 About the Identity and Data Sciences Laboratory (IDSL)

The Identity and Data Sciences Laboratory (IDSL) is an independent research organization within SAIC, a technology integrator for the US government. The IDSL is comprised of scientists, engineers, IT specialists, and program managers with demonstrated expertise in the test and evaluation of AI systems.

Since inception, the IDSL has carried out authoritative analyses and reporting on the performance of biometric identity systems, including face recognition systems. Much of our work has been in support of the Department of Homeland Security Science and Technology Directorate (DHS S&T). The IDSL operates the Maryland Test Facility (MdTF) in support of research conducted on behalf of the DHS S&T Biometric and Identity Technology Center (BI-TC). Starting with our work on the Air Entry-Exit Re-engineering (AEER) project we have tested well over 200 commercial biometric technologies in varied use-cases. Our technology evaluations have been provided to inform government agencies (DHS S&T, CBP, TSA, USCIS, OBIM, DOD, DOJ, and others) as well as published in peer-reviewed scientific journals². Our expert staff are regularly invited to present our findings at conferences within the US and internationally. IDSL applied research addresses topics including biometric system performance, demographic group fairness, and human-algorithm teaming. We are using this insight to inform the development of international standards, including technical editorship of ISO/IEC 19795-10 on quantifying biometric system performance variation across demographic groups.

Given this relevant background, we are pleased to respond to the White House Office of Science and Technology Policy (OSTP) request for information (RFI) titled “Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies”. In the sections below, we provide responses to topic areas outlined within the RFI.

2.0 Responses to RFI Topic Areas

2.1 Descriptions of use of biometric information for recognition and inference

As defined by OSTP, the definition of biometric technology to include both individual recognition and cognitive/emotional state inference encompasses a wide range of disparate technology. Because of foundational differences in these two kinds of computer applications, care is often taken to separate the two in the scientific community. For example, there are internationally adopted standards that define the term “biometrics” as “automated recognition of individuals” based on their behavioral and biological characteristics” (emphasis ours)³. This definition has also previously been adopted by agencies in the U.S. Government⁴. By this definition, biometric recognition involves a comparison between two biometric samples to determine whether they are of the same individual.

² MdTF Publications. <https://mdtf.org/Research/Publications>.

³ ISO/IEC 2382-37:2017 Information technology — Vocabulary — Part 37: “Biometrics Recognition” term 37.01.03. <https://www.iso.org/standard/66693.html>

⁴ DHS OBIM defines a biometric as “a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition”. <https://www.dhs.gov/biometrics>



Biometric recognition has well defined scientific underpinnings, metrics, and international standards that have been in existence for nearly 20 years⁵. Indeed, biometric systems may be one of the most well tested current applications of artificial intelligence (AI)⁶. For nearly a decade, biometric systems have been deployed in a variety of scenarios including to facilitate identity determination at international borders and airport checkpoints, for individual identification in both public and commercial settings including the identification of missing persons and those involved in human trafficking, and for access to personal electronic devices.

In contrast, technology for inference of cognitive and/or emotional states based on a single sample are varied in their domain of application and poorly understood. The scientific basis for these technologies also varies dramatically (some basis for emotion recognition⁷ vs no basis for criminality⁸). Additionally, we are not aware of any international standards for the test and evaluation of these systems. Despite growing commercial deployment in areas such as hiring and exam monitoring, these technologies are rarely, if ever, vetted for validity by independent third parties.

As an entity specifically focused on AI system test and evaluation, the bulk of our responses to this RFI are centered on biometric technology as used for recognition since this is where our primary experience lies. Our position is that it may be timely to consider similar scrutiny to other AI systems in the public domain.

2.2 Procedures for and results of data-driven and scientific validation of biometric technologies

With support from the Department of Homeland Security Science and Technology Directorate, the IDSL conducts data-driven scientific evaluations of biometric technology in government use-cases. At a high level, there are three kinds of biometric evaluations as defined by ISO standards⁹ enumerated below. In Sections 2.2.1 – 2.2.3, we outline each evaluation type, including measurement setup, evaluation procedure, specific measures, outcomes and error rates.

Technology evaluations are typically centered on a specific component of a biometric system (e.g. a matching algorithm) and use previously acquired biometric datasets with large sample sizes. This type of testing is appropriate for measuring the limits of a technology's performance and for comparison of different technologies. This testing is not appropriate for answering questions about how a technology performs in a specific application.

⁵ ISO/IEC JTC 1/SC 37 Biometrics. <https://www.iso.org/committee/313770.html>

⁶ NIST: Biometrics. <https://www.nist.gov/programs-projects/biometrics>.

DHS S&T Biometric and Identity Technology Center (BI-TC). <https://www.dhs.gov/science-and-technology/BI-TC>.

The Maryland Test Facility. <https://mdtf.org>.

⁷ Barrett, Lisa Feldman, et al. "Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements." *Psychological science in the public interest* 20.1 (2019): 1-68.

⁸ Bowyer, Kevin W., et al. "The "Criminality From Face" Illusion." *IEEE TTS* 1.4 (2020): 175-183.

⁹ ISO IEC 19795-1: Information technology–biometric performance testing and reporting-part 1: Principles and framework. <https://www.iso.org/standard/73515.html>.



Figure 1. Maryland Test Facility test bay set up for a “Rally” scenario test.

Scenario evaluations center around a specific technology use-case (e.g. airplane boarding) and test a full multi-component biometric system (i.e. including any acquisition devices, databases, and algorithms) with test volunteers in a controlled environment. This type of testing gathers new biometric samples to answer questions about how a technology performs for a specific intended use (**FIGURE 1**).

Operational evaluations assess the performance of a technology in the fielded environment. This testing measures the performance of the system within a specific location and environment (e.g. a face recognition system installed in at a specific airport terminal). While most operationally relevant, reduced experimental control in operational evaluations makes it harder to identify the key factors influencing performance.

2.2.1 Technology evaluations

By far the most common category of biometric evaluation are what’s known as technology evaluations. Technology evaluations typically rely on large static test datasets and can be used to test performance limits and track the performance of algorithms over time, motivating innovation. Tests are typically executed on biometric algorithms in isolation, disentangling them from the larger workflows of full operational biometric systems (i.e. cameras, databases, administrative systems, etc.).

The IDSL regularly executes technology evaluations to report on both the state of the biometric industry and industry progress. To execute technology evaluations, the IDSL maintains a sophisticated data storage, processing and reporting infrastructure in house at the Maryland Test Facility. This computational testbed consists of over 25 distinct server systems, 100 virtualized software platforms for redundancy, and 20 TB of on-premise storage.

The protocols, measures, and outcomes for technology testing are defined in the international standard ISO/IEC 19795-2, which has been in place since 2007¹⁰. Typically, experimental setup in a technology test involves a large static dataset of biometric samples with ground truth. Biometric algorithms are used to create biometric templates, or mathematical models of the physiological sample. These templates can then be compared to calculate a similarity score. Once this process has been executed on many biometric sample

¹⁰ ISO/IEC 19795-2:2007 Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation. <https://www.iso.org/standard/41448.html>

pairs (face pairs, iris pairs, etc.) the generated scores are separated into two categories; those that came from biometric samples that should match (individual A's face image on day 1 and individual A's face on day 2) and those that should not (individual A's face and individual B's face). These pairs are called mated and non-mated pairs respectively. Using these pairs, two foundational error rates for a biometric algorithm can be calculated, namely the false non-match rate and the false match rate. Both these error rates measures are specific to a match or discrimination threshold. Its common in technology testing for these error rates to be calculated over a range of thresholds to produce summary statistics, such as detection error tradeoff curves.

The main benefits of technology evaluations of biometric systems lie in their reproducibility. This is advantageous because 1) the findings can be replicated by others and used to improve their systems (assuming data availability) and 2) the findings can be replicated longitudinally as algorithms or other system components improve. In this way technology evaluators can monitor and report on industry progress. We have previously used technology evaluations to identify a phenomenon named “demographic clustering”, by which face recognition algorithms tend to score different people of the same race, age, and gender as more similar than those who do not share demographic characteristics¹¹. We first pointed out this “homogeneity effect” in 2019 and subsequently replicated it with numerous algorithms and on other datasets¹².

Technology testing has important limitations. Much like comparing two formula 1 race cars on a test track, you are able to see what is achievable, but you are unlikely to see comparable performance driving your sedan around town. Technology testing will miss important aspects of operational system performance. For example, a technology evaluation may not discover a scenario in which a facial recognition camera systematically cannot find faces (and therefore take pictures) of individuals with darker skin, since these evaluations starting point is captured images. Furthermore, the static nature of the datasets used in technology evaluations means that they often do not represent changing circumstances in the real world. For example, when the COVID-19 pandemic led to large scale public masking requirements, the datasets used in typical face recognition technology evaluations no longer reflected the facial characteristics of individuals a face recognition system was likely to encounter in situations like an airport or border crossing.

In summary, technology evaluations of biometric technologies are well defined processes that provide important information, particularly to biometric system developers. However, they are not sufficient to anticipate the full range of issues a biometric system might experience once deployed in a robust, operational environment. They are one part of a larger, necessary testing regime to ensure the effectiveness and equitability of biometric systems.

¹¹ Howard, Sirotin, Tipton, Vemury. Quantifying the Extent to Which Race and Gender Features Determine Identity in Commercial Face Recognition Algorithms. DHS S&T Technical Paper Series. (2021). https://www.dhs.gov/sites/default/files/publications/21_0922_st_quantifying-commercial-face-recognition-gender-and-race_updated.pdf

¹² Grother, Ngan, Hanaoka. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. NISTIR 8280. <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.

2.2.2 Scenario evaluations

Scenario evaluations of biometric technologies simulate a full biometric application and its real-world deployment environment. Unlike technology evaluations, scenario evaluations measure error and success rates on full biometric systems (i.e., algorithms, acquisition devices like cameras, and any needed databases). Further scenario evaluations measure performance using new data collected from test volunteers. In every new evaluation, volunteers utilize biometric systems just as they would in a real-world deployment, allowing unique insights into the efficiency of the system (e.g. how long it takes to use) and on human perceptions of the system (e.g. how satisfied are the users).

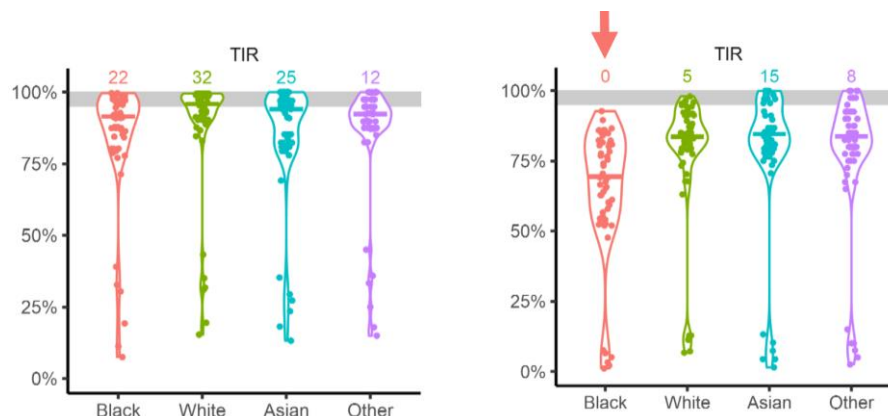


Figure 2. True Identification Rate (TIR) of face recognition systems without face masks (left) and with face masks (right) disaggregated by self-identified Race. Note greater reduction (arrow) due to masks for those self-identifying as Black.

To date, the IDSL has primarily focused on scenario evaluations of both staffed and automated biometric systems within the travel environment¹³. We curate and maintain an ethically collected structured dataset of over 137,000 face, fingerprint, and iris images of over 2,000 unique persons together with metadata on demographics and phenotypes (e.g. skin tone). For our scenario tests, we recruit volunteers from the local area stratified by race, gender, and age or other factors as needed for each evaluation. We have tested well over 200 face, fingerprint, and iris recognition systems with over 5,000 unique volunteer visits to the Maryland Test Facility. The IDSL uses dedicated data processing systems for computing standard measures of biometric performance and generating reports.

Using this scenario test model, scientists at the IDSL have identified important new insights into biometric performance. For example, in a widely cited 2018 study that explored the effect of camera on bias, we found evidence that differential performance in face recognition could largely be traced to differences in camera’s abilities to capture high quality photographs of individuals with difference skin tones¹⁴. This impact of camera had largely been ignored in discussions of “bias” in face recognition but plays a key role in creating a more equitable system. Additionally, using the scenario test model the IDSL was able in 2020 to collect the first

¹³ Howard, Blanchard, Sirotin, Hasselgren, Vemury. An Investigation of High-Throughput Biometric Systems: Results of the 2018 Department of Homeland Security Biometric Technology Rally. <https://mdtf.org/publications/rally-results.pdf>.

¹⁴ Cook, Howard, Sirotin, Tipton, Vemury. Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems. <https://mdtf.org/publications/demographic-effects-image-acquisition.pdf>

dataset of masked individuals since the onset of the COVID-19 pandemic. We were able to quantify the expected reduction in face recognition performance due to masked face occlusion and critically demonstrated that this performance reduction was not equivalent across demographic groups (individual with darker skin saw larger reductions in performance than those with lighter skin, **FIGURE 2**)¹⁵. This insight motivated improvements in masked face recognition performance across industry and helped created more equitable face recognition systems.

Lastly, we have found that scenario testing at the IDSL forecasts error cases in the operational environment. In particular, scenario testing predicts the use errors and differences in performance associated with demographic factors. On the other hand, results observed in technology tests depend critically on the type of data used for the evaluation. For instance, the performance of face recognition technologies in NIST’s FRVT tests depends critically on the type of dataset used¹⁶. In our own assessments, we find that the performance of system components is inter-dependent with algorithm results depending strongly on the acquisition camera used (**FIGURE 3**)¹⁷. We strongly believe that, like other forms of AI, biometric technologies must be proven in scenario tests in order to understand their likely performance within the operational environment.

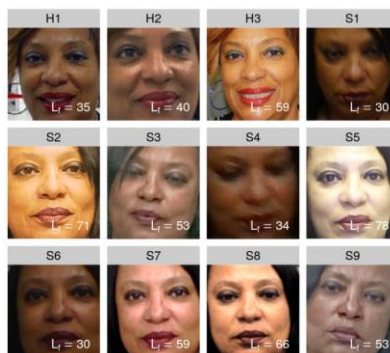


Figure 3. Images of a person gathered using different biometric cameras. Note the change in appearance and skin tone. Images S1-S9 were collected on the same day under consistent lighting conditions.

2.2.3 Operational evaluations

The final variety of biometric system evaluation is known as an operational evaluation. The protocols and procedures for this form of testing is defined in international standard ISO/IEC 19795-6, which was published in 2012¹⁸. Operational evaluations provide the most direct insight into how a biometric system is performing as deployed in a given implementation. However, despite their value, operational evaluations of biometric

¹⁵ Y. B. Sirotin and A. R. Vemury. “Demographic variation in the performance of biometric systems: Insights gained from large-scale scenario testing.” In Virtual Events Series – Demographic fairness in biometric systems. EAB, March 2021.

<https://mdtf.org/publications/EAB2021-Demographics.pdf>

¹⁶Grother, Patrick, et al., “Ongoing Face Recognition Vendor Test (FRVT) Part I: Verification.”

¹⁷Hasselgren, Jacob A., et al., “A scenario evaluation of high-throughput face biometric systems: select results from the 2019 Department of Homeland Security Biometric Technology Rally.” DHS S&T Technical Paper Series. (2020).

https://www.dhs.gov/sites/default/files/publications/2021_st-01_2019selectrallyresultstip20201104_revised_3046.pdf

¹⁸ ISO/IEC 19795-6:2012 Information technology — Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation. <https://www.iso.org/standard/50873.html>

systems can be challenging to resource and execute properly. Consequently, they are relatively rare compared to scenario and laboratory evaluations of biometric systems. The two main challenges when conducting operational evaluations of biometric systems are lack of experimental control and lack of ground truth information. For example, it can be arduous to collect accurate race, gender and age information from people in crowded operational environments, like airports or train stations. It can also be challenging attributing observed effects directly to specific causes because of many nuisance factors.

To perform operational evaluations, the IDSL team goes on location to observe and record the operational environment, the technology configuration, and first-hand observations of user interactions with the system. The IDSL can receive and process operational sample-based and transactional data to generate performance measures. We believe operational evaluations of biometric systems provide the most direct evidence of system performance in the field to inform system developers and system owners.

2.3 Security considerations associated with a particular biometric technology

Discussion topic 3 in OSTP's RFI deals with the security of biometric systems, particularly around spoofing and more traditional software system security (i.e. encryption, data access/audit, etc.). We anticipate many respondents will provide material on these two topics. However, we wanted to raise a security issue that OSTP might not yet be aware of that relates specifically to face recognition applications. Often when face recognition is used for security applications, the digital images that require identification can come from poor quality cameras and challenging environments. There is a strong incentive to improve the utility of such low-quality images for biometrics, especially when this may help solve a crime.

However, the performance of biometric systems with altered digital images, even if altered with the intent to enhance, is generally not well understood and has been suggested to lead to potential law enforcement errors¹⁹. Further, recent advances in AI have made it easier to perform such alterations without needing technical skill²⁰. This creates additional concerns regarding privacy whereby security equipment previously suitable only for detecting suspicious activity may now become useful for biometric surveillance.

To avoid errors and privacy implications that may be caused by image manipulation in security applications, it is important that biometric systems include specific descriptions of their intended context of use and that any performance information be clearly associated with this context of use.

2.4 Exhibited and potential harms of face recognition technology

The deployment of face recognition technologies undoubtedly carries with it potential harms, some of which have been realized as these technologies are increasingly used in the real world. First, in regards to the validity of the science, there is little doubt the human face contains characteristics that allow for individual recognition. Human beings innately perform such functions on a daily basis when we recognize friends,

¹⁹ Garvie, Clare, et al., "The perpetual line-up. Unregulated police face recognition in America". Georgetown Law Center on Privacy & Technology. (2016). <https://www.perpetuallineup.org/>

²⁰ Some examples: research from Google (<https://ai.googleblog.com/2021/07/high-fidelity-image-generation-using.html>) and of a tool easily available online (<https://github.com/TencentARC/GFPGAN>).

family, co-workers, etc. It stands to reason that computer processes could similarly carry out such tasks, a notion which has been repeatedly validated by over 20 years of government and industry testing.

However, just because a given technology works in the general case, does not mean it works equally well for all groups of people. Additionally, a technology that works well in the general case can also have idiosyncrasies that cause it to fail in predictable ways. Both of these conditions are true for face recognition. Many scientists, IDSL staff included, have documented error rates that can differ for individuals based on their demographics in face recognition. We coined the, now widely adopted, term “demographic differentials” to describe these effects in 2018²¹. While studying these phenomena is important, IDSL scientists have also pointed out that solving for this situation may not fully solve issues of “bias” in face recognition. In 2021, IDSL scientists highlighted an often overlooked but nearly universal characteristic of face recognition. Face recognition algorithms judge different individuals who share demographic characteristics (same race, gender age, etc.) as more alike than those that don’t. We used the term “broad homogeneity” to describe this effect and pointed out that no other major biometric modality does this, yet it has somehow become accepted in face recognition²².

We believe this clustering by demographics may be one source of potential harm in face recognition deployments when used for law enforcement. The fact that broad homogeneity exists means that identifications against galleries that are demographically skewed (majority male, for example) could have unequal false positive identification rates. Implementers of face recognition workflows should be aware of this effect and its consequences. Training may help avoid adverse impacts that stem from this phenomenon.

2.5 Exhibited and potential benefits of face recognition technology

The deployment of face recognition systems has undoubtedly benefitted the general public in many ways. One of the clearest examples is in the travel environment, where face recognition applications have sped airplane boarding and border crossing. Prior to the introduction of automated face recognition in these environments, identity verification tasks were performed by exclusively by humans. However, humans have well documented shortcomings when it comes to identifying unfamiliar faces. Humans also have limitations in terms of attention. This makes automated face recognition an attractive choice to both improve the effectiveness and efficiency in these environments.

2.6 Governance programs, practices, and procedures

All IDSL scenario test activities conducted at the Maryland Test Facility receive approval from an external Institutional Review Board (IRB) to ensure that ethical and data safeguards are met. Additionally, all data collected as part of our work with DHS S&T is maintained in accordance with a Privacy Threshold Analysis approved by the DHS Privacy Office. As part of standard practices required by the IRB, all human-subjects that participate are properly informed about the test and provide explicit consent to participate.

²¹ Howard, Sirotin, Vemury. The Effect of Broad and Specific Demographic Homogeneity on the Imposter Distributions and False Match Rates in Face Recognition Algorithm Performance. <https://mdtf.org/publications/broad-and-specific-homogeneity.pdf>

²² Ibid., 10

The IDSL conducts two forms of informed consent for all test events: group consent and individual consent. In the group consent, all human-subjects are informed of what data will be collected and how their data will be protected. In the individual consent, human-subjects are called into private interview rooms with doors and white noise to guarantee privacy to each human-subject while going over consent forms. Each human-subject is asked for explicit permission to reproduce any images collected during the test in publication materials; subjects that opt-out are not excluded from the test.

All data collected by the IDSL is associated with a unique subject-ID, separated from any personal information. This protection is to avoid personally identifiable information (PII) from being leaked or compromised. The IDSL's datasets are also sequestered to prohibit datasets from being taken advantage of by developers of AI/ML systems. Developers of AI/ML systems will leverage all available information in developing their system, but this can result in 'overfitting' (a phenomenon where you can do better on the data you know and paradoxically worse on new data) or even cheating²³. For this reason we limit access to our datasets and routinely gather new data to prevent such practices, even when unintentional.

We believe technology and scenario evaluations play a critical role in biometric system governance prior to system deployment by reducing the odds that non-performant or unfair systems are put into real-world applications. However, following system deployment, additional performance auditing steps are also necessary to ensure that real-world conditions have not adversely impacted the expected performance of a biometric system. Because post-deployment performance evaluations are likely to contain PII collected outside the lab context, the IDSL utilizes separate systems for processing data gathered as part of an operational evaluation. Operational data used for performance evaluations resides on Government systems granted Authority to Operate (ATO) and is used in accordance with any required Privacy Threshold Assessments. Steps and considerations when conducting post deployment, operational evaluations of biometric systems are discussed in Section 2.2.3.

3.0 The case for requiring independent testing of biometric systems

As real-world deployments of AI systems multiply, the public is becoming increasingly aware of the need to evaluate the performance of AI systems. Our research shows that, when these systems are used to establish the identity of individuals and make inferences about individuals, they can make errors, sometimes conflicting with notions of 'fairness' or 'equitability'. Our experience suggests that vendor-reported efficacy claims may not always align with real-world performance. Depending on the application, biometric system errors may carry significant costs or harms at both the individual and group level²⁴.

²³ Markoff, John. "Baidu team is barred from A.I. competition." The New York Times. (2015). <https://www.nytimes.com/2015/06/04/technology/computer-scientists-are-astir-after-baidu-team-is-barred-from-ai-competition.html> and Quach, K. (2020, June 18). How a kaggle grandmaster cheated in \$25,000 ai contest with hidden code – and was fired from Dream SV job. The Register - Biting the hand that feeds IT. Retrieved January 14, 2022, from https://www.theregister.com/2020/01/21/ai_kaggle_contest_cheat/

²⁴ Hill, Kashmir. "Wrongfully accused by an algorithm." The New York Times (2020). <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>



Despite technology developers racing to create and implement AI systems, few entities have the capability and focus, like the IDSL, to test the performance of these systems. The situation is comparable to the field of drug development prior to The Federal Food, Drug, and Cosmetic Act of 1938, which required new drugs to be shown safe and prohibited false therapeutic claims²⁵. AI systems may not have direct effects on human life, but their increasing ubiquity and scale also carry the potential for significant harms.

Some recent discussions have focused on AI audits as means to ensure that harms of AI systems are managed²⁶. While important, we believe that audits in the absence of independent third-party *performance testing* are insufficient to ensure that systems meet required benchmarks for performance and equitability.

The IDSL has a unique mission to evaluate biometric systems to better understand their likely performance in the field and to provide quantitative empirical evidence to inform analyses of these systems' potential harms, including harms to protected demographic groups. Currently, there is little incentive for companies to perform independent third-party tests of their biometric technology products. Conversely, companies have strong incentives to present optimistic performance claims in marketing that conflate results of technology testing performed during AI training and real-world performance.

Without robust regulations and requirements for rigorous scientific testing, like the kind carried out by the IDSL, few biometric system developers have the incentive to test their systems. Indeed, the US government currently shoulders much of the cost associated with testing these technologies. The costs of deploying untested systems will be realized in unexpected technology failures, including potentially unfair systems. These issues may be realized only after deployment, when changes or adjustments become more costly. Worse still is the possibility that such issues may simply go undetected, leading to increasing opportunity periods for harms to manifest. This will undermine public trust in biometric systems.

We believe that independent third-party scenario and operational testing with demographically diverse people should be a prerequisite to marketing biometric systems for any high-risk applications that carry potential for harms at the individual or the group level. We hope the information we have provided herein can inform the development of an AI bill of rights²⁷.

Durkin, Erin. "New York tenants fight as landlords embrace facial recognition cameras." The Guardian (2019). <https://www.theguardian.com/cities/2019/may/29/new-york-facial-recognition-cameras-apartment-complex>

²⁵ FDA. "Milestones in U.S. Food and Drug Law." <https://www.fda.gov/about-fda/fda-history/milestones-us-food-and-drug-law>

²⁶ The New York City Council - File #: Int 1894-2020 (nyc.gov) <https://legistar.council.nyc.gov/LegislationDetail.aspx>

²⁷ Lander, Eric and Nelson, Alondra. "ICYMI: WIRED (Opinion): Americans Need a Bill of Rights for an AI-Powered World." The Office of Science and Technology Policy. (2021). <https://www.whitehouse.gov/ostp/news-updates/2021/10/22/icymi-wired-opinion-americans-need-a-bill-of-rights-for-an-ai-powered-world/>