Sydnor Testimony Fav SB0587 Facial Recognition.pd
Uploaded by: Clark, Eugene
Position: FAV

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

Judicial Proceedings Committee

Joint Committees

Children, Youth, and Families

Cybersecurity, Information Technology, and Biotechnology

Ending Homelessness

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

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

Testimony for SB 587
Facial Recognition – Privacy Protection Act
Before the Judicial Proceedings Committee
On March 2, 2021

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

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 ("FRT") 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. Senate Bill 587 will implement necessary accountability and control over when the facial recognition net is cast.

Ari B. Rubin explains how FRT acts as an automated police lineup:[3]

> A criminal investigator or FRT analyst begins the process with an input, called a "probe photo." The probe photo might come from anywhere: a police booking shot, the person's social media presence, or a blurry freeze-frame from a video surveillance camera. The technology then automatically compares a computer analysis of the photo against analyses of a database of other photos—FBI mug shots, government photo libraries (such as drivers' records), or commercial photo libraries (sometimes lifted from public websites)—and returns possible matches. In the criminal-justice context, authorities can then use other investigative tools and corroborative evidence to narrow the list of possible suspects to confirm a single, most-probable match with corroborative evidence.[4]

Undoubtedly there are benefits to use of facial recognition: preventing and addressing unlawful entry at ports.[5] Monitoring high-security events, such as the Super Bowl.[6] In the local law

[1] 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 4
[4] *Id.* at 5.
[5] *Id.* at 14.
[6] *Id.*

enforcement context, police can use FRT to identify a suspect incident to arrest;[7] or may use FRT to determine an unknown person's identity based on a photo of him or her at a crime scene.[8]

However, Facial Recognition Technology has also been used maliciously. The New York Times reported in 2019 that government officials in Tumxuk (China) collected blood samples from hundreds of Uighurs as they are trying to find a way to use a DNA sample to create an image of a person's face. Regarding China's efforts, experts say, "it may even be possible for the Communist government to feed images produced from a DNA sample into the mass surveillance and facial recognition systems that it is building, tightening its grip on society by improving its ability to track dissidents and protesters as well as criminals."[9] It was also recently 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.[10] 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.[11]

SB 587 attempts to address some of these concerns by building guardrails around the usage of these systems by requiring law enforcement accountability. The bill requires accountability reports for the uses of facial recognition services ("FRS"). In addition, annual reports will be required to keep the community informed of the impacts of FRS on citizens' civil rights.

The bill requires quality assurance testing by FRS vendors. Moreover, the use of FRS technology must be subject to meaningful human review, and FRS vendors will be required to enable independent inspection. Additionally, under the bill, law enforcement users of FRS will undergo mandatory periodic training to ensure FRS best practices are used uniformly. To address concerns highlighted in the stories I mentioned above, the use of FRS on the basis of political or religious expression will be prohibited, and its use on the basis of race will be restricted. Any proposed use of FRS for ongoing surveillance must be monitored by a court, and any such authorization may not continue indefinitely without good cause.

Finally, and crucially, prosecution's use of FRS must be disclosed in criminal proceedings. This will be crucial for putting defense counsel on notice of law enforcement strategies, but also for informing the public as to how police intend to use FRS to engage in prosecution. With that, I ask for this committee to bring the law into the 21 century and help regulate the use by our government of FRT and move favorably on SB 587.

---

[7] *Id.* at 19.
[8] *Id.* at 20.
[9] China Uses DNA to Map Faces, With Help From the West - The New York Times (nytimes.com)
[10] Dahua facial recognition touts 'real-time Uighur warnings' - Los Angeles Times (latimes.com)
[11] *Id*. at 16.

MD SB 587 - Oral Testimony - Microsoft.pdf
Uploaded by: Tolani, Pooja
Position: FAV

Hearing on

MD SB587

FACIAL RECOGNITION PRIVACY PROTECTION ACT

Oral Testimony of Pooja Tolani

Associate Corporate Counsel, US Government Affairs

Microsoft

Chairman Smith and members of the Judicial Proceedings committee my name is Pooja Tolani, I'm an Associate Corporate Counsel at Microsoft, thank you for the opportunity to be here.

We would like to thank you and Senator Sydnor for your leadership and your efforts to restrict the government's use of Facial Recognition technology.

Microsoft has called for new laws to regulate facial recognition technology since July 2018, well before lawmakers across the country began introducing proposals to govern the technology. The company believes that facial recognition offers tremendous benefits for security, public safety, and society, we also think it's important for lawmakers to ensure that the technology will not be used to undermine civil liberties, discriminate against members of protected classes, or otherwise harm marginalized communities.

For those reasons, in June of 2020, Microsoft announced that we would not sell facial recognition technology to police departments until there are laws regulating it.

Microsoft strongly supports your efforts to address this important issue including imposing safeguards like accountability, transparency, training, testing, and public reporting, as well as restrictions on use. However, we believe it is most important to listen to and work with law enforcement and civil society regarding regulation of such technologies. We look forward to hearing the perspectives of those groups and are willing to help in any way we can, including efforts to help foster a dialogue between those important groups.

Thank you for your time.

OPD SB0587 Written Testimony.pdf
Uploaded by: Northrup, Andrew
Position: FWA

MARYLAND OFFICE OF THE PUBLIC DEFENDER- FORENSICS DIVISION
TESTIMONY IN SUPPORT OF SENATE BILL587 WITH AMENDMENTS

The Office of the Public Defender supports Senate Bill 587 with amendments.

The use of facial recognition programs by the government raises all sorts of privacy concerns as this is yet another technology that allows us to be more easily surveilled. This is even more concerning when the accuracy and efficacy of the facial recognition programs used to identify individuals is uncertain.

Senator Sydnor deserves a lot of credit for taking this difficult subject head on, and this bill is an important first step in creating guard rails. However, because this area of technology is in its nascency, the many of the standards, guidelines and proficiency assessments to ensure its proper use, simply have not been developed. These considerations are reflected in our proposed amendments, which have been given to the bill's sponsor.

Facial recognition searches are very similar in operation to fingerprint searches. An image is captured, it is prepared to be searched in the database, and the algorithm selects a list of the top candidates. Those candidates are reviewed by the machine operator, who determines if one of the candidates is a match.

As one can see, there are several variables that can affect the search:

(1) the quality of the initial image;

(2) how that image is prepared to be entered into the database; (i.e. lightened, darkened, rotated, etc.), which presumably is addressed by training of the individual operator;

(3) the quality of the algorithm that selects the prospective candidates.;

(4) the ability of the operator to select the proper match (assuming it is there) from the list of candidates.

As shown, the facial recognition algorithm is only one component of the analysis. The training of the individual operators is also very important as is the quality of the initial image. Currently, standards for each of these areas are still being developed. Until proficiency standards are set for

the algorithms used, and the humans who operate the machines, we have to be very circumspect in the use of this technology.

To address these concerns, we have suggested the following amendments.

First, we propose limiting the use of this technology to developing investigative leads, and not to allow its use for probable cause purposes or as evidence in court. As previously stated, the standards are not in place to ensure its reliable use.

Second, that a board be set up to review the use of Facial Recognition technology and make policy recommendations as the contours of this technology area come more into focus.

Third, that in addition to the use of the technology in an investigation being disclosed to criminal defendants, the original facial image collected, the image as uploaded, and the candidate list of any search during the investigation should be disclosed as well.

Ideally, the use of this technology would be put on hold until these issues were ironed out. However, since that is not possible, this bill could be a good first step to providing guard rails to the use of this technology.

MCPA-MSA_SB 587 Facial Recognition _Oppose.pdf
Uploaded by: Mansfield, Andrea
Position: UNF

Maryland Chiefs of Police Association

Maryland Sheriffs' Association

MEMORANDUM

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

FROM: Chief 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 2, 2021

RE: **SB 587 Facial Recognition Privacy Protection Act**

POSITION: **OPPOSE**

The Maryland Sheriffs' Association (MSA) and the Maryland Chiefs of Police Association (MCPA) **OPPOSE SB 587.** This bill would prohibit the use of facial recognition systems by law enforcement agencies until the agency, which uses the System, creates and submit a bi-annual report related to the development, procurement or use of facial recognition. This legislation also requires each governmental unit to perform testing of facial recognition services prior to their use, as well as many prohibitions on the use of facial recognition.

Currently, the Facial Recognition System managed by the Department of Public Safety and Correctional Services (DPSCS), is used by 90% of law enforcement agencies in Maryland.

The DPSCS system has been in use for years. SB 587 would prohibit the continued use of the system until each agency who used the system to complete an "Accountability Report". Requiring every unit using that platform to create and submit the same report would be duplicative. Instead of one report by the DPSCS, there could potentially be in excess of fifty reports.

The use of facial recognition is only a tool or a pointer system like other crime fighting tools. While MCPA and MSA agrees there should be restrictions on constitutional protected activities, there are many valid reasons for its use. A 'timely" notification to the person subject to the use of the technology could jeopardize ongoing criminal investigations. Evidentiary disclosure should be done by the State's Attorney. Also, the identification of the officer and unit making the application undermines the use of confidential sources on prolonged investigations and puts the officer who may be undercover at risk.

For these reasons, MCPA and MSA OPPOSE SB 587 and urge an UNFAVORABLE report.

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

SIA Concerns - MD SB 587 Regarding Facial Recongit

Uploaded by: Parker, Jake

Position: UNF

March 2, 2021

The Honorable Senator Smith
Chair, Judicial Proceedings Committee
2 East
Miller Senate Office Building
Annapolis, Maryland 21401

Written Testimony of SIA in Opposition to Senate Bill 587 Facial Recognition Privacy Protection Act

Dear Chairman Smith and Members of the Judicial Proceedings Committee:

On behalf of the Security Industry Association (SIA) I am writing to express our concerns with the proposed bill, which could negatively impact security applications of facial recognition and others that help protect public safety. SIA is a nonprofit trade association representing companies that provide a broad range of security products and services in the U.S and throughout Maryland, including 27 companies headquartered in our state. Our members include many of the leading developers of facial recognition software as well as companies offering products that incorporate this technology into a wide variety of government, commercial and consumer products.

Support for Ensure Responsible, Ethical Use
We believe all technology products must only be used for purposes that are lawful, ethical, and non-discriminatory. Since many advanced technologies 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.[1]

We support the intention of the bill to establish safeguards for government use of the technology. However, we believe its current structure as drafted will unnecessarily limited proven uses of the technology in ways that benefit Marylanders. Additionally, confusing terminology used throughout the bill will make it difficult for agencies to comply. Significant revisions would be required to address these issues.

Flawed Definition of Ongoing Surveillance
Public concerns about facial recognition technology have centered around law enforcement uses that might raise privacy and civil liberties concerns. However, the definition of "ongoing surveillance" appears to prohibit beneficial non-law enforcement uses in security systems used to protect state or local government facilities that may include areas open to the public, such as courthouses, and other public buildings. In these cases, security staff can be alerted to the presence of known individuals that are potentially dangerous, but the situation may not yet rise to the level of an emergency or where law enforcement should be involved. Additionally, much like how it is commonly used to unlock an electronic device, facial recognition enabled access control systems allow an authorized user to unlock a door or to access a secured area. In these instances, individuals could enter a premises multiple times or move throughout areas where their identity is connected to a particular place and time, potentially triggering the "ongoing surveillance" definition. Requiring a law enforcement purpose appears to take the technology off the table for these types of uses, which can

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

positively impact the day-to-day safety and security of government personnel and members of the public visiting buildings and other government facilities.

Third-Party Testing

The requirement to provide an application programming interface (API) for the third-party testing could provide an unfair advantage to larger companies using software as a service business model – which may make free or trial versions publicly available. This requirement would disrupt agencies using technology that is not cloud based – like the Maryland Image Repository Systems (MIRS). It would also disadvantage small U.S. developers of facial recognition designed for government use, most of which have not made their technology publicly available to ensure it is only used for specific purposes. These developers should have the alternative option of participating in the National Institute of Standards and Technology (NIST) Facial Recognition Vendor Test (FRVT) program to meet this requirement. FRVT is the global gold standard for scientific, independent evaluations of facial recognition algorithm performance, including comprehensive measurements of differences across demographic groups. This program run by the federal government is available to developers at no cost.

A Note on the Science Regarding Facial Recognition Accuracy

Additionally, you may have heard the oft-repeated claim in media reports about racial "bias" in the technology. What this really refers to is the performance of the software in successfully comparing and matching photos of the same person. While it is true some versions of the technology have struggled to provide consistent performance across racial and other demographic factors, the claim that all facial recognition technology is less accurate across the board in matching photos of black and female subjects does not accurately reflect the current state of the science.

The National Institute of Standards and Technology (NIST), the leading scientific authority worldwide on the accuracy of facial recognition algorithms, found in its Demographic Effects report in 2019 that the leading facial recognition technologies it tested had "undetectable" differences[2] in accuracy across racial groups, after rigorous tests against millions of images. This would simply not be the case if demographic differences were "inherent" in the technology. These leading technologies are the same ones used in most of today's government and law enforcement applications, reaching the accuracy of fingerprint technology on many measurements, the gold standard for identification.

At the same time, lower performing algorithms among the nearly 200 that NIST tested did show measurable differences of several percentage points in performance across demographics – and this is an issue utmost importance to our industry which is continually addressed. It is critical to understand though, that most still had overall accuracy rates around 99% for all categories.

Widely misconstrued in media accounts is a 2018 report[3] where the claim is that it showed a 35% error rate for facial recognition on photos of black women. In fact, those researchers tested older "face gender classification technologies." Such software used to classify the race, gender, age, etc. of an unknown person in a photo – a technology that is not used for identification, or in law enforcement. Facial recognition, on the other hand, compares two or more images for similarities to help identify a specific person based on their unique facial features. By conflating these technologies and citing research that did not actually evaluate facial recognition accuracy at all, many media reports inaccurately assigned racial disparities[4] to facial recognition that really dealt with a different technology.

Americans Support Current Uses of Facial Recognition

[2] https://www.securityindustry.org/report/what-nist-data-shows-about-facial-recognition-and-demographics/
[3] https://www.media.mit.edu/projects/gender-shades/overview/
[4] https://itif.org/publications/2019/01/27/note-press-facial-analysis-not-facial-recognition

Finally, leading independent polling firm Schoen Cooperman Research recently conducted a nationwide poll on Americans' views of facial recognition technology, commission by SIA.[5] The survey found 68% of Americans believe facial recognition can make society safer, 70% believe it is accurate in identifying people of all races and ethnicities and 66% of believe law enforcement's use of facial recognition is appropriate. The results are consistent with other polling that indicates little public support for banning or heavily restricting this important technology.

On behalf of SIA and its members, we share the goal of ensuing 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 this bill in its current form. We stand ready to provide any additional information or expertise needed as you consider these issues.

Sincerely,

Respectfully,

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

https://www.securityindustry.org/advocacy/policy-priorities/facial-recognition/

CC: Member of the Judicial Proceedings Committee

[5] https://www.securityindustry.org/2020/10/07/extensive-new-poll-finds-most-americans-support-facial-recognition/

SB 587 - Facial Recognition.pdf
Uploaded by: Shellenberger, Scott
Position: UNF

Bill Number: SB 587
Scott D. Shellenberger, States Attorney for Baltimore County
Opposed

WRITTEN TESTIMONY OF SCOTT D. SHELLENBERGER,
STATE'S ATTORNEY FOR BALTIMORE COUNTY,
IN OPPOSITION OF SENATE BILL 587
FACIAL RECOGNITION PRIVACY PROTECTION ACT

Senate Bill 587 greatly hampers the ability of the police to use modern technology to locate possible suspects in crimes by using publicly accessible databases that have been used for years.

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

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

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

The second suspect got away.

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

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

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

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

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

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

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

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

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

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

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

Think of some of the things Senate Bill 587 would prevent. The use of this technology in airports like BWI. You subjecting your face to the public should not the police be able to use the best technology to find the next shoe bomber.

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

Senate Bill 587 is too restrictive and does not allow the police to do their job. It is merely a way to speed up the universe of those who may be suspects but the State must still prove its case.

I urge an unfavorable report.

Maryland State Police Position Paper for SB 587.pd
Uploaded by: Williams, Thomas
Position: UNF

State of Maryland
Department of State Police
Government Affairs Section
Annapolis Office (410) 260-6100

POSITION ON PROPOSED LEGISLATION

DATE: **March 2, 2021**

BILL NUMBER: **Senate Bill 587** **POSITION: Oppose**

BILL TITLE: **Facial Recognition Privacy Protection Act**

This legislation seeks to prohibit the use of Facial Recognition Systems by law enforcement agencies until the agency, which uses the System, creates and submit a bi-annual report related to the development, procurement or use of facial recognition. Each agency would be required to hold public hearings and receive comments as part of the reporting process. This legislation also requires each governmental unit to perform testing of facial recognition services prior to their use, as well as many prohibitions on the use of facial recognition.

Currently, the Facial Recognition System managed by the Department of Public Safety and Correctional Services (DPSCS), is used by 90% of law enforcement agencies in Maryland. Very few agencies are actually using the Facial Recognition application without using the Maryland Coordination and Analysis Center (MCAC) to oversee the use and dissemination of the data. The DPSCS already creates an annual report as to the access and use of its facial recognition application.

The DPSCS system has been in use for years. SB 587 would prohibit the continued use of the system until each agency who used the system to complete an "Accountability Report". Requiring every unit using that platform to create and submit the same report would be duplicative. Instead of one report by the DPSCS, there could potentially be in excess of fifty reports.

The DPSCS has validated the Facial Recognition System platform and manages access to and use of the platform. For each unit of government who needs to access and use the platform to validate its use is impractical and unnecessary, since it has already been validated and is provided as a useful tool to law enforcement.

The use of facial recognition is only a tool or a pointer system like other crime fighting tools. While the Department agrees there should be restrictions on constitutional protected activities; such as marches and protests, there are many valid reasons for its use. A 'timely" notification to the person subject to the use of the technology could jeopardize ongoing criminal investigations. Evidentiary disclosure should be done by the State's Attorney. Also, the identification of the officer and unit making the application undermines the use of confidential sources on prolonged investigations and puts the officer who may be undercover at risk.

For these reasons the Department of State Police urges the Committee to give SB 587 an unfavorable report.