POGO

PROJECT ON GOVERNMENT OVERSIGHT

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 protestors. Is that legal?" *South Florida Sun Sentinel*, June 26, 2021, https://www.sun-sentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sll5uuaqfbeba32rndlv3xwxi-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 techniques[6] — 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 matches[12] 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 over-reliance 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).