Policing Project
NYU School of Law

NYU School of Law
40 Washington Square South
New York, NY 10012

info@policingproject.org
@policingproject
212.992.6950

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. <u>There is an urgent need to regulate law enforcement use of FRT</u>

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-hg6jkfav2fdz3ccs55bvqjtnmu-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.