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

Senator Charles E. Sydnor III
Testimony for SB 587
Task Force on Facial Recognition Privacy Protection
Before the Judiciary Committee
On March 31, 2021

Good afternoon Mr. Chairman, members of the Judiciary 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 allow us to study and recommend best practices that will provide some level of 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]

---

[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.

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 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 Task Force will address some of the aforementioned concerns by studying guardrails for the usage of these systems by law enforcement. It will develop accountability mechanisms for the uses of facial recognition services ("FRS"). Additionally, the Task Force will recommend the best reporting system to keep the community informed of the impacts of FRS on citizens' civil rights.

The Task Force will study quality assurance testing by FRS vendors and others. It will also study and form best practices recommendations for FRS technology that allows for human review, and independent inspection. The Task Force also will study best practices pertaining to use of FRS for ongoing surveillance, and at what point should the courts be used to authorize it.

Finally, the Task Force will study and recommend best practices for prosecutors, who use FRS, to disclose it to defense counsel in criminal proceedings. I ask for this committee to move favorably on SB 587.

---

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