

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



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 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 \(nytimes.com\)](https://www.nytimes.com/2019/08/26/us/politics/china-dna-facial-recognition.html)

¹⁰ [Dahua facial recognition touts 'real-time Uighur warnings' - Los Angeles Times \(latimes.com\)](https://www.latimes.com/2019-08-26/la-fi-dahua-facial-recognition-touts-real-time-ugghur-warnings-2019-08-26)

¹¹ *Id.* at 16.