GEORGETOWN LAW
Center on Privacy & Technology

Statement of Jameson Spivack, Policy Associate

Center on Privacy & Technology, Georgetown Law

Before the

Maryland General Assembly

In favor of

SB857

Wednesday, March 11, 2020

For more information, contact Jameson Spivack at jameson.spivack@georgetown.edu.

Executive summary

My name is Jameson Spivack and I'm a Policy Associate with the Center on Privacy & Technology at Georgetown Law. I'm testifying in favor of **SB857**, legislation to establish a one-year moratorium on the use of face recognition technology services in the state of Maryland. The key takeaways from my testimony are below:

Maryland has one of the most pervasive and invasive systems of face recognition in the country.

- Over 7 million Maryland driver's license photos and 3 million mugshots are part of a face recognition system accessible not just to state and local government agencies, but federal agencies as well.
- The FBI and ICE can run *direct* face recognition searches on the faces of Maryland residents. They don't need to submit requests through a Maryland state agency, nor do they need to be present in the state. No other state that we know of allows this.

Face recognition allows an unprecedented level of surveillance.

- It gives governments the ability to identify and track many people, in secret, from a distance, based on how they look or where they've been. This gives governments more power than they've ever had.

Face recognition makes mistakes, which can have serious consequences.

- Numerous studies have shown the technology performs differently depending on skin color, age, and gender. These biases, particularly in the context of law enforcement, can perpetuate historic injustices against communities of color.

In the absence of legal constraints, face recognition can be, and has been, misused.

- No matter how accurate or unbiased face recognition becomes, if you input poor data, you will get poor outcomes.
- Law enforcement has been found to submit "flawed face data" in face recognition searches—heavily edited photos, copy and pasted facial features, celebrity lookalikes, and composite sketches. This is fabrication of evidence.

Marylanders have no way of knowing how the government is using face recognition technology, because there is no transparency.

- The public should be informed about how the government is using this potentially harmful technology. So far, the public has been kept in the dark.

The Maryland General Assembly should press pause on face recognition use until the public can have an informed, democratic debate about how—or if—Maryland should use the technology.

- This technology poses real threats, to real people, right now. Maryland should adopt a moratorium to prevent any further harm resulting from this technology.

Testimony

My name is Jameson Spivack and I'm a Policy Associate with the Center on Privacy & Technology at Georgetown Law. The Center is a research organization that has been studying law enforcement and the government's use of face recognition for the past five years. We've written four major reports on the subject,[1] testified before the U.S. Congress,[2] advised policymakers on federal and state legislation, and worked with countless civil society and community organizations around the country to ensure face recognition does not threaten civil rights and liberties.

In 2016, the Center published *The Perpetual Line-Up*,[3] the first comprehensive report on how law enforcement agencies across the country use face recognition technology. *The Perpetual Line-Up* uncovered just how widespread police face recognition is, and the risks it poses to the public. It found that over half of all US adults have their faces in a face recognition database. In most cases, the public was not told that police had access to this tool or that their photos were being searched. Despite face recognition being less accurate than fingerprinting, there was no regulation around how the tool could be used—and few police departments had internal use policies that were publicly available.

Face recognition is inaccurate, prone to bias, and ripe for abuse. In *The Perpetual Line-Up*, we discuss how face recognition frequently makes mistakes, particularly on women and people of color, and that there is little to no testing for accuracy and bias. It also gives the government surveillance capabilities it has never had before. As part of an organization committed to understanding how surveillance disparately impacts vulnerable people, I am worried about how face recognition is being used as a surveillance tool, especially in Black, brown, and low-income communities. I thus urge you to favorably report SB857 for the following reasons.

I. Maryland has one of the most pervasive and invasive systems of face recognition in the country.

If you have a Maryland driver's license, or have been arrested in Maryland, you are subject to unchecked face recognition searches. You are part of a database that is repeatedly searched by police to see whether your face matches a suspect's. Not just state and local police—federal agents as well[4]. This amounts to over 7 million Maryland driver's license photos and over 3

---

[1] For a full list of the Center's publications, *see* https://www.law.georgetown.edu/privacy-technology-center/publications/.

[2] *See* House Hearing on Facial Recognition Technology, House Oversight and Reform Committee, May 22, 2019, https://www.c-span.org/video/?460959-1/house-hearing-facial-recognition-technology.

[3] *See* Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (2016), https://www.perpetuallineup.org/report

[4] *See* Federal Bureau of Investigation, Maryland DPSCS Dashboard Facial Recognition Access, Aug. 26, 2016, https://republicans-oversight.house.gov/wp-content/uploads/2017/03/Maryland-MOU.pdf;

million mugshot photos.[5] Once in this database, you are part of a perpetual line-up, always a potential suspect in a police investigation.

Federal agencies like ICE and the FBI can run face recognition searches *directly* on your photo, even if you have no criminal history. And neither you nor a Maryland law enforcement officer would know about it, let alone a judge. As long as an officer has a login to the National Crime Information Center (NCIC), they can run face recognition searches on Maryland faces, without going through a Maryland official.[6] An ICE agent in Nebraska, for example, could run a fishing expedition on Maryland residents' faces, seeking undocumented people for deportation. Maryland allows undocumented people to obtain driver's licenses; granting licenses, then handing the photos over to ICE, is a dishonest bait and switch.[7]

Baltimore County police officers used face recognition to surveill, identify, and arrest people at the Freddie Gray protests in 2015.[8] According to documents obtained by ACLU Northern California, Baltimore County police contracted with a company called Geofeedia, which pulled posts and photos from social media accounts of people attending the protests. Police then ran face recognition searches on these photos, identified people with unrelated outstanding arrest warrants, and then targeted these protesters for arrest.[9] This amounts to targeting participants of a public, predominantly Black political event, for completely unrelated charges. Attending a protest, like all political activity, is protected by the First Amendment. If law enforcement uses face recognition to surveill protests and rallies, people will be discouraged from attending. This chills political participation.

II. Face recognition allows an unprecedented level of surveillance.

Face recognition gives governments the ability to identify and track many people, in secret, from a distance, based on how they look or where they've been. This gives governments more power than they've ever had, and defies our expectation of what governments should be able to

---

Evidence of direct ICE access to Maryland's driver's license photos is contained in a letter from the Maryland Department of Public Safety and Correctional Services to Sen. Susan Lee, Sen. Clarence Lam, Del. Dana Stein, and Del. Joseline Peña-Melnyk, on file with the lawmakers and with the author.

[5] *Supra*, note 3, "Maryland," https://www.perpetuallineup.org/jurisdiction/maryland.

[6] *Supra*, note 5

[7] *See* Drew Harwell and Erin Cox, "ICE has run facial-recognition searches on millions of Maryland drivers," *The Washington Post*, Feb. 26, 2020, https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/.

[8] *See* Matt Cagle, "Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color," *ACLU Northern California*, Oct. 11, 2016, https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

[9] *See* Geofeedia Case Study: Baltimore County PD, https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf.

do. It threatens to create a world in which people are watched and identified as they attend a protest, congregate at a place of worship, visit a medical provider, and go about their daily lives. Police generally need a court order to track your location; using face recognition on surveillance camera photos allows police to do just this without any oversight.

Law enforcement agencies themselves have recognized the serious risks that face recognition poses to our civil rights and liberties. In a 2011 Privacy Impact Assessment (PIA), federal and state officials cautioned that with face recognition:

> *"The mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition."*
>
> *"As an instrument of surveillance, identification increases the government's power to control individuals' behavior. It can further inhibit one's ability to be anonymous, which is an important right in a free society."*[10]

To mitigate these risks, the drafters recommend policies that restrict the use of face recognition as a method of public surveillance—a recommendation that has failed to be adopted by law enforcement agencies in Maryland to the detriment of residents' First Amendment rights.

Unchecked, face recognition could create a world without privacy, in which your identity, whereabouts, and behavior are accessible to anyone else. Already, companies like Clearview have built face recognition systems capable of serious privacy violations.[11] In the hands of powerful actors, such as the government, these systems present severe risks to our civil liberties. They threaten to fundamentally alter our lifestyles, chilling speech, political activity, and participation in everyday activities.

III. Face recognition makes mistakes, which can have serious consequences.

Face recognition is not completely accurate, and it is often even *less* accurate on people with dark skin, women, and young people. A recent study by the Department of Homeland Security (DHS) found that face recognition "performance is strongly affected by demographic factors, notably skin [color]," and that image "differences can strongly affect (magnify or eliminate)"

---

[10] *See* International Justice and Public Safety Network, *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field,* June 30, 2011, pg. 2, https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf.

[11] *See* Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times*, Jan. 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

bias issues.[12] In other words, differences in image quality and angle can compound accuracy issues, particularly for demographic groups already vulnerable to worse performance.[13] The National Institute of Standards and Technology (NIST), the country's premier research institution dedicated to bolstering industrial competitiveness, also "found empirical evidence for the existence of demographic differentials in the majority of contemporary face recognition algorithms that [they] evaluated."[14] Biased algorithms could perpetuate the over-incarceration of young Black men; this is particularly troubling as Maryland incarcerates young Black men at a rate higher than any state in the nation.[15]

When face recognition misidentifies someone, it doesn't just let the actual criminal go free. It also puts an innocent person in harm's way. Amara Majeed, a young woman from the Baltimore area, was misidentified as a suspect in the 2019 Easter bombings in Colombo, Sri Lanka. As a result, she received death threats from strangers who saw her photo posted all over the Internet. The Sri Lankan government, who had used face recognition to identify Majeed, quickly apologized for their error—but the damage was already done.[16] These kinds of mistakes have serious, life-altering consequences.

IV. In the absence of legal constraints, face recognition can be, and has been, misused.

Face recognition has largely operated in the shadows, where it is prone to be misused. As the Center discovered in its report *Garbage In, Garbage Out*, law enforcement uses "flawed" face data when running face recognition searches—faces that mix and match different peoples' features, images that have been heavily edited, celebrity lookalikes, and composite sketches.[17]

---

[12] *See* C. M. Cook, J. J. Howard, Y. B. Sirotin, J. L. Tipton, and A. R. Vemury, "Demographic Effects in Facial
Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 1, no. 1, pg. 32-41, Jan. 2019, https://ieeexplore.ieee.org/document/8636231.

[13] *See* DHS Office of Inspector General, "Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide," Sept. 21, 2018, https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf.

[14] *See* Patrick Grother, Mei Ngan, and Kayee Hanaoka, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," *National Institute of Standards and Technology*, pg. 6, Dec. 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[15] *See* Hannah Gaskill, "Senate Panel Briefed on Disparity in Incarceration," *Maryland Matters*, Jan. 17, 2020, https://www.marylandmatters.org/2020/01/17/judicial-proceedings-committee-holds-hearing-on-equity-in-marylands-justice-system/.

[16] *See* Jeremy C. Fox, "Brown University Student Mistakenly Identified as Sri Lanka Bombing Suspect," *The Boston Globe*, Apr., 28, 2019, https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lankabombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html.

[17] *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data* (2019), https://www.flawedfacedata.com/.

Most infamously, the NYPD identified a suspect using a photo of actor Woody Harrelson.[18] In other cases, officers copy and paste features from different peoples' faces onto one another. They use modeling software to approximate missing facial features in photos. This all amounts to fabrication of evidence.

It doesn't matter how accurate a face recognition system is: if you put garbage data in, you will get garbage data out. And that's exactly what's been happening. Maryland is one of a handful of jurisdictions that allows artist-drawn composite sketches to be run through its face recognition system, as if they were real suspect faces.[19] Its face recognition system comes pre-loaded with photo-editing software, encouraging officers to alter face photos.[20] Editing someone's fingerprint would constitute evidence tampering; this is no different.

V. Marylanders have no way of knowing how the government is using face recognition technology, because there is no transparency.

The public has been kept in the dark about how face recognition is used in Maryland. As of December 2017, Maryland's face recognition system had not been audited for accuracy since it launched in 2011.[21] We have no way of knowing if it has been audited since—the system is that covert. If there's a problem with the technology, in the database of photos, or in how law enforcement is using it, we have no way of knowing.

Law enforcement has failed to disclose to defendants that face recognition was used to identify them. When there is information or evidence that is material to the guilt or innocence of a defendant, the prosecution must turn this over to the defendant in a *Brady* disclosure. Failing to do so is a violation of due process. The results of a face recognition search, when they are used to identify and eventually arrest a suspect, should be disclosed to defendants under *Brady*. Yet, most of the time they aren't.[22] This has resulted in countless due process violations, which will continue until a policy—or a moratorium—is put in place.

---

[18] *See* Michael R. Sisak, "NYPD used Woody Harrelson photo to find lookalike beer thief," *AP*, May 16, 2019, https://apnews.com/4ef0d4bf24764fe3b9b4311c576062b4

[19] *See* Criminal Justice Dashboard: Quick Reference Sheet for Users, obtained from Department of Public Safety and Correctional Services, https://drive.google.com/open?id=0B-MxWJP0ZmePS1p0Z2FkakRGc1U.

[20] *See* Face Plus Case Management - BASIC: User Guide, DataWorks Plus, https://drive.google.com/open?id=0B-MxWJP0ZmePd1VSNzJUUDF4elU.

[21] *See* DPSCS Letter to Chairman Kasemeyer and Chairman McIntosh, Dec. 1, 2017, https://www.mylaw.org/uploads/1/7/7/6/17760533/md-image-repository-system.pdf.

[22] *Supra* note 3, "Transparency and Accountability";
For more specific coverage *see* Benjamin Conrack, "How a Jacksonville man caught in the drug war exposed details of police facial recognition," The Florida Times-Union, May 26, 2017, https://www.jacksonville.com/news/metro/public-safety/2017-05-26/how-jacksonville-man-caught-drug-war-exposed-details-police.

VI. The Maryland General Assembly should press pause on face recognition use until the public can have an informed, democratic debate about how—or if—Maryland should use the technology.

Face recognition technology poses real threats, to real people, right now. I urge the General Assembly to favorably report SB857, legislation to establish a one-year moratorium on the use of face recognition technology services in the state of Maryland. In that time, Marylanders should have a serious conversation about the potential risks and benefits of the technology. A moratorium should remain in place until the legislature passes strict, comprehensive regulation that affords Marylanders the protections they need from this potentially harmful technology.