ACLU Maryland

Testimony for the Senate Judicial Proceedings Committee
January 15, 2020

SB 46 State's Attorney – Required Disclosure – Facial Recognition and DNA Analysis and Search

INFORMATIONAL

TONI HOLNESS
PUBLIC POLICY DIRECTOR

AMERICAN CIVIL LIBERTIES UNION OFMARYLAND

MAIN OFFICE
& MAILING ADDRESS
3600 CLIPPER MILL ROAD
SUITE 350
BALTIMORE, MD 21211
T/410-889-8555
or 240-274-5295
F/410-366-7838

FIELD OFFICE
6930 CARROLL AVENUE
SUITE 610
TAKOMA PARK, MD 20912
T/240-274-5295

WWW.ACLU-MD.ORG

The ACLU of Maryland supports legislative safeguards to protect the privacy interests of Marylanders against government intrusion, including through the use of facial recognition technology and DNA analysis. Below, we offer some background information about facial recognition technology; concerns about its deployment in Maryland; and recent developments in the courts regarding its use in criminal proceedings. Finally, in light of the many concerns about the technology and its deployment in Maryland, we urge the body to enact a moratorium on its use until it can be further studied.

I. What is Facial Recognition technology?

Facial recognition systems are built on computer programs that analyze images of human faces for the purpose of identifying them. The programs take a facial image, measure characteristics such as the distance between the eyes, the length of the nose, and the angle of the jaw, and create a unique file called a "template." Using templates, the software then compares that image with another image and produces a score that measures how similar the images are to each other.[1]

II. Maryland has been using Facial Recognition technology since 2011

In March 2011, Maryland initiated a system populated by arrest photos. Shortly thereafter, In December of that same year, Maryland executed a memorandum of understanding with the FBI to launch a Facial Recognition Pilot Program and gain access to the national repository of arrest photos. In 2013, the system further enrolled photos from the Maryland Motor Vehicle Administration (MVA) into the database.

III. Facial Recognition Technology raises several concerns

Currently, the database, the Maryland Image Repository System (MIRS), includes over 7 million driver's license and other MVA photos and over 3

1 American Civil Liberties Union, Q&A On Face-Recognition (available at https://www.aclu.org/other/qa-face-recognition, last accessed Feb. 27, 2017).

million arrest photos. Maryland law enforcement can also request searches of the FBI's arrest photo database of 24.9 million photos.[2]

The use of facial recognition technology in Maryland raises at least five concerns: (1) the database is populated by driver's license and arrest photos; (2) flaws in the technology disproportionately affect communities of color; (3) deployment of the technology during First Amendment protected activity has a chilling effect; (4) there are no rules governing law enforcement's access to the database; and (5) the Maryland database has not been audited since its establishment.

The flaws inherent in the facial recognition system coupled with inappropriate deployment of the system demands greater study, oversight, and limitations on its use. Until the technology and its deployment is further studied, we respectfully urge the legislature to issue a moratorium on its use.

a. The population of the Maryland database with driver's license and arrest photos raises concerns

The use of driver's license photos sweeps up law abiding Marylanders into a database used primarily for criminal investigation purposes. These persons have not engaged in any wrongdoing that would justify their inclusion in a criminal investigatory database. Moreover, the collection of information about swaths of Marylanders who are not suspected of committing any crime raises serious privacy concerns.

Equally problematic is the use of arrest photos in the facial recognition database. Many persons are arrested, without charge or conviction—this is disproportionately the case for persons of color, who are arrested at higher rates than whites.[3] Due to the lack of auditing and policies in Maryland, it is unclear whether persons who are arrested but not charged or convicted have their photos expunged from the facial recognition database. The stark racial disparities in who is arrested but not charged in Maryland (overwhelmingly people of color in Baltimore) reinforce the problem of including arrest photos in the database, and highlight the need to impose thoughtful and meaningful regulation

b. Facial Recognition technology has a chilling effect when deployed during First Amendment protected activity

The use of this technology during First Amendment protected activity, such as peaceful public demonstrations, threatens to chill the exercise of these rights. Persons will simply be less willing to publicly demonstrate if demonstrating subjects them to this intrusive level of surveillance. This is especially concerning in light of recent revelations regarding Geofeedia, a social media monitoring software that has been used by law enforcement agencies and was

[2] Perpetual Lineup, Center on Privacy & Technology at Georgetown Law, 2016 (available at https://www.perpetuallineup.org/jurisdiction/maryland).
[3] *Id.*

used in Maryland.[4] The software allows law enforcement to employ facial recognition software to identify faces in photographs of demonstrations posted on social media and cross-reference them with photos of persons with open warrants. Use of facial recognition in this context has obvious chilling effects on the exercise of First Amendment freedoms. A recent study shows that individuals' internet use patterns change substantially when they perceive that they are being monitored.[5] And the choice of which demonstrations will trigger the deployment of the facial recognition technology raises concerns about the targeted use against communities of color.

c. African Americans are at greater risk of being mistakenly identified

Studies show that facial recognition algorithms in use by U.S. law enforcement are statistically worse at identifying Black faces than white faces. As a result, because police investigate the closest match, the software puts innocent Black people at higher risk of police investigation than innocent white people.[6]

d. There are no rules governing access to the facial recognition database

In response to a recent public records request by Georgetown University Law Center, no policies governing the operation of the Maryland's facial recognition system were produced. State officials own comments also demonstrate the lack of any standards governing access to the database.[7] In the absence of any rules, and in the absence of a probable cause standard, the database can be used in racially discriminatory ways, and can be used to target demonstrators who are disfavored by police. The lack of rules also raises the prospect of widespread deployment of real-time face tracking by fixed cameras, which would be an Orwellian nightmare.

e. Maryland's system has never been audited

Since its launch in 2011, Maryland's facial recognition system has never been audited. This means that Maryland's system could be flawed in the functioning of the technology; the population of photos; and the deployment of the technology—without any accountability. In turn, law enforcement's use of the technology remains practically unknown to the public and worse,

[4] Kevin Rector and Alison Knezevich, Baltimore Sun, Social media companies rescind access to Geofeedia, which fed information to police during 2015 unrest (Oct. 11, 2016). Available at http://www.baltimoresun.com/news/maryland/crime/bs-md-geofeedia-update-20161011-story.html

[5] Jonathan W. Penny, Chilling Effects: Online Surveillance and Wikipedia Use, 31 Berkeley Tech. L.J. (September 2016), available at https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2769645.

[6] Clare Garvie and Jonathan Frankle, Facial-Recognition Software Might Have a Racial Bias Problem, The Atlantic (Apr. 7, 2016), available at http://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/.

[7] *See here* a video of a WBAL reporting that Maryland law enforcement agents do not need probable cause prior to accessing the face recognition system. The report is here https://www.youtube.com/watch?v=xrZT9RuJWp4&feature=youtu.be.

unregulated.

IV. The use of Facial Recognition Technology as a *Brady* disclosure is not settled law

In 2015, in the case of *Willie Allen Lynch v. State of Florida*, Prosecutors failed to disclose information about the use of facial recognition technology algorithms that ultimately identified the defendant. The defendant argued that this information was "Brady" evidence, which may exculpate the defendant and that it should therefore have been disclosed to the defense. This case further elucidates the need for greater oversight of the technology's use. We fully expect to see further litigation on the matter.

In closing, we support the bill's intention to regulate the use of facial recognition technology in criminal proceedings, but believe that the use of the technology ought to be halted in order for the body to consider and enact a more comprehensive regulatory system.