ACLU
Massachusetts

ACLU of Massachusetts
211 Congress Street, Suite 301
Boston, MA 02110
617-482-3170
www.aclum.org

July 30, 2021

Commission on Facial Recognition
Senator Jamie Eldridge and Representative Michael S. Day, Co-Chairs

Public Comment
Government Use of Facial Recognition Technology

Dear Senator Eldridge, Representative Day, and members of the Commission,

Good morning. My name is Rahsaan Hall. I am the Director of the Racial Justice Program at the ACLU of Massachusetts. I am writing on behalf of the ACLU and our nearly 100,000 members and supporters across the Commonwealth to provide some comments about the government's use of facial recognition technology in Massachusetts.

As a former prosecutor, I know that investigative tools used in the criminal legal system have to be reliable and used in a manner that is consistent with our constitutional rights. The reason for this fidelity to accuracy and constitutional protections is not merely that evidence must stand up to scrutiny in court. Rather, we recognize that criminal prosecutions can result in the deprivation of freedom for individual people—in other words, the caging of human beings. This is no small matter. One mistake on the government's side can cause irreparable harm to entire families and set off a chain of trauma that can last for generations.

Advanced technologies can be effectively used to solve crimes, no doubt. But surveillance technologies like facial recognition also give the government vast new powers to invade our privacy, monitor our speech and association, and digitize and automate racial profiling. Therefore the legislature must impose safeguards to prevent government from abusing its power, or misusing technology in ways that harm individuals and communities.

For these reasons, the ACLU has been concerned with face surveillance and emerging biometric surveillance for many years now. The use of this technology by the government poses unprecedented threats to core civil rights and civil liberties, impedes racial justice, and undermines our open, free, democratic society.

<u>Current law falls short of protecting the public interest</u>

In December 2020, after a long process that included a back and forth with the legislature, Governor Baker signed into law an omnibus police reform bill. The law, codified in Chapter 253 of the Acts of 2020, contains several provisions pertaining to government agencies' use of face surveillance.

We were disappointed that the legislature's initial approach in its conference committee report, which included strong face surveillance provisions to protect racial justice and privacy,[1] was rejected by the Administration. The policy ultimately signed by Governor Baker falls far short of

[1] Steph Solis, Massachusetts Legislature enacts broad police reform bill; next hurdle is Gov. Charlie Baker's veto pen, MassLive, Dec. 02, 2020. https://www.masslive.com/politics/2020/12/massachusetts-legislature-enacts-broad-police-reform-bill-next-hurdle-is-gov-charlie-bakers-veto-pen.html

what we need. It fails to limit non-law enforcement use of facial recognition technology, does not address facial surveillance tracking in public places, does not sufficiently regulate law enforcement's possession and use of the technology to identify people, and is silent on matters related to due process.

Therefore, we respectfully ask that the Commission recommend the legislature strengthen existing face surveillance law to ensure Massachusetts residents and visitors are shielded from discriminatory, dragnet surveillance, and other harms.

Facial recognition technology and racial bias

Facial recognition technology is dangerous when it works and when it doesn't. When it works, this technology can facilitate a massive surveillance infrastructure where everyone is identified, wherever they go, all the time. But research indicates there is substantial racial and gender bias embedded in many face surveillance algorithms, which can lead to wrongful arrests and other harms. These biases were initially discovered by the groundbreaking research of world-renowned MIT scientists Joy Buolamwini and Timnit Gebru,[2] and they are now widely acknowledged by the scientific community.[3]

In December 2019, the non-partisan federal government National Institute of Standards and Technology published a landmark study[4] presenting further evidence that facial recognition algorithms across the board are not ready for prime-time. The researchers found that face recognition algorithms perform more poorly when examining the faces of women, people of color, the elderly, and children — raising serious concerns about police use of the technology across the United States and underscoring the need to tightly regulate government use of the technology.

Various studies have shown face surveillance technology to be racist.[5] But even if the algorithms worked perfectly across demographic differences, the unrestricted use of face surveillance in policing would negatively affect Black people because our communities have traditionally been subject to disproportionate surveillance, harassment, and arrest. Indeed, to date, all of the known cases about people being wrongfully arrested or otherwise punished because of the use of the technology involve Black people, including most recently a young Black girl who was wrongfully ejected from a skating rink after a face surveillance algorithm misidentified her.[6]

Problems with the current face surveillance law and recommended solutions

We have several concerns with the existing law.

First, the law only regulates facial recognition technology as used by law enforcement agencies. It neither prohibits nor regulates when this technology can or cannot be used by other public agencies, like schools or transportation departments. The law should prohibit most government agencies from using this dystopian, biased software.

[2] Joy Buolamwini, "Gender Shades," MIT Center for Civic Media. https://www.media.mit.edu/projects/gender-shades/overview/.

[3] John Basil, Republicans And Democrats Concerned About Face Recognition Technology, Your Erie, July 13, 2021. https://www.yourerie.com/news/local-news/republicans-and-democrats-concerned-about-facial-recognition-technology/

[4] Patrick Grother, Mei Ngan, Kayee Hanaoka, Face Recognition Vendor Test (FRVT)
Part 3: Demographic Effects, NIST, December 2019. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[5] Kade Crockford, How is Face Recognition Surveillance Technology Racist?, ACLU, June 16, 2020. https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/

[6] Kashmir Hill, Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match, The New York Times, December 2020. https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html. See also Dave Gershgorn, Black Teen Barred From Skating Rink By Inaccurate Facial Recognition, The Verge, July 15, 2021. https://www.theverge.com/2021/7/15/22578801/black-teen-skating-rink-inaccurate-facial-recognition

Second, the existing law does not prohibit or regulate the use of facial recognition technologies for purposes of surveillance of public spaces like streets and parks. This is troubling both because the technology performs extremely poorly "in the wild" and because if it were perfected and used to monitor people in public, such tracking would threaten fundamental freedoms.

Face surveillance technology works best when using front-facing, clear, high-resolution, high-light images. However, even under those conditions, it can fail. Notably, the federal government testing mentioned above was run in a quality-controlled research setting using standardized photographs, such as police mugshots and visa application portraits — and it *still* showed major inaccuracies.

Using these algorithms to identify faces in "wild" photographs taken from surveillance footage will only worsen demographic disparities because those photos are often very low-quality. For example, in 2017, police in London used face surveillance technology on live video to attempt to identify people on a hotlist at a carnival. Unsurprisingly, the system wrongfully identified people 98 percent of the time.[7] Police in Wales reported similarly bad outcomes: 91 percent failure.[8] "On 31 occasions police followed up the system saying it had spotted people of concern," the Guardian reports of the test, "only to find they had in fact stopped innocent people and the identifications were false."[9]

Even if the technology worked perfectly, it would raise extremely serious civil rights issues. People in Massachusetts should be able to walk around their communities, visit friends and family, seek medical treatment, go to church, and attend political events without worrying that the government is secretly keeping tabs on their every movement, habit, and association. A jealous police officer should not be able to use facial recognition to monitor the activities of their girlfriend; a star-struck officer should not be able to pursue celebrity sightings; and an officer with a political grudge should not be able to surveil a candidate or elected official.

For these reasons and others, the law should prohibit the use of facial analysis and identification algorithms to analyze video data, both live and historical.

Third, the existing law does not restrict law enforcement agencies from acquiring and possessing a facial recognition system. The law merely mentions the Registrar of Motor Vehicles and the State Police as possessing face surveillance systems but does not explicitly restrict other agencies from buying or leasing their own systems.

This leaves the door open for every local law enforcement agency to acquire and use its own facial recognition system, with wild variations of system quality and operational knowledge. This could result in dozens or even hundreds of systems from different vendors or even developed in-house. Each and every one of them could legally operate with different levels of accuracy and reliability, using different training and operating procedures.

We cannot allow this to happen in the Commonwealth. Chaotic and decentralized implementation of facial recognition technology is bad from both a prosecutorial and a civil rights perspective, and makes effective accountability, transparency, and oversight nearly impossible.

The law must therefore centralize government use of facial recognition for investigative purposes, and limit the agencies that can possess the technology.

[7] Vikram Dodd, UK Police Use Of Facial Recognition Technology A Failure, Says Report, May 14, 2018, The Guardian. https://www.theguardian.com/uk-news/2018/may/15/uk-police-use-of-facial-recognition-technology-failure.

[8] Id.

[9] Id.

Fourth, the existing law fails to require a probable cause warrant for law enforcement use of facial recognition technology as an investigative technique. The warrant is the gold standard for invasive government searches, and it must be applied here.

Fifth, existing law allows the use of the technology in all criminal investigations without any limitation. Government use of facial recognition technology is extremely privacy invasive, and therefore should not be used to attempt to identify a person for minor offenses such as trespassing, shoplifting, or jaywalking. Facial recognition searches should only be authorized in the most serious types of criminal investigations, investigations of serious violent felonies. As a former prosecutor I am well aware of the need to investigate offenses that have resulted in grave injury or death, and in those rare instances use of this technology is warranted.

Sixth, the existing law does not provide any due process protections for criminal defendants that have been subject to the use of facial recognition systems. The law should be explicit on this point to ensure prosecutors are not intentionally or unintentionally violating people's constitutional rights to a fair trial by withholding information about the use of technology that effectively constitutes a digital witness.

Seventh, the existing law does not provide any enforcement mechanism to ensure public officials comply with the law. The law must include a fruit of the poisonous tree exclusion, to ensure government officials comply with its provisions. Ideally, the law should also include a private right of action, so individuals can hold the government accountable to the law.

Finally, the existing law only regulates facial recognition and does not mention or provide for other remote biometric recognition technologies that are as risky and harmful as facial recognition.[10] The law should prohibit the uses of these untested, dangerous technologies. If government officials want to use them in the future, they can come back to the legislature to request narrow permissive uses subject to civil rights and civil liberties protections. We shouldn't continue to allow government agencies to put the technology cart before the regulation horse.

Thankfully, lawmakers have addressed these concerns in legislation filed this session. H.135, sponsored by Representatives Rogers and Ramos, and S.47, sponsored by Senator Creem, would fill these gaps and provide the protections Massachusetts residents deserve. The legislation is almost identical to the language agreed to by the House and Senate in the initial conference report for last year's police reform legislation.

Face surveillance can be used in limited, tightly regulated circumstances to advance legitimate police investigations, but the existing law does not sufficiently protect racial justice, due process, privacy, or First Amendment rights. Therefore, we respectfully urge Commissioners to recommend the legislature address these gaps and enact H.135 and S.47.

Thank you for your attention and consideration.

[10] Lauren Rhue, Emotion-Reading Tech Fails The Racial Bias Test, The Conversation, January 3, 2019. https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404. See also Lisa Feldman Barrett, et al. Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements, Psychological Science in the Public Interest, vol. 20, no. 1, July 2019, pp. 1–68, DOI: 10.1177/1529100619832930.