POGO

PROJECT ON GOVERNMENT OVERSIGHT

July 30, 2021

The General Court of Massachusetts
Special Commission on Facial Recognition
24 Beacon Street, Room 136
Boston, MA 02133

Submitted via email

Dear Senator Eldridge, Representative Day, and members of the commission:

I am writing on behalf of The Constitution Project at the Project On Government Oversight about the need for serious limits on use of face recognition technology. We respectfully ask the commission to recommend the legislature strengthen existing facial recognition law to ensure Massachusetts residents and visitors are shielded from overbroad and pervasive surveillance.

Founded in 1981, the Project On Government Oversight (POGO) is a nonpartisan independent watchdog that investigates and exposes waste, corruption, abuse of power, and when the government fails to serve the public or silences those who report wrongdoing. We champion reforms to achieve a more effective, ethical, and accountable federal government that safeguards constitutional principles. The Constitution Project at POGO centers its work on issues such as guarding against improper and overbroad surveillance, including unchecked face recognition. In 2019, The Constitution Project convened a task force of expert stakeholders including academics, tech experts, civil rights and civil liberties advocates, and law enforcement officials to examine the impact of face recognition surveillance.[1] It concluded that any law enforcement use of face recognition should be subject to strong limits, and it provided a set of policy recommendations to support legislatures in the creation of reasonable but necessary limits.

In December 2020, Governor Charlie Baker signed into law “An Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth,” 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 recognition technology. We support some of those provisions, such as the creation of this commission and the development of independent authorization standards.

The new law’s policies governing police use of the technology, however, are insufficient as safeguards to protect civil rights and civil liberties. Fortunately, lawmakers have addressed these concerns in legislation filed this session in each chamber: H.135, An Act to Regulate Face

[1] Task Force on Facial Recognition Surveillance, Project On Government Oversight, *Facing the Future of Surveillance* (March 4, 2019), https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/.

Surveillance, sponsored by Representatives David Rogers and Orlando Ramos, and S.47, An Act to Regulate Face Surveillance, sponsored by Senator Cynthia Stone Creem.

This bill would improve rules on face recognition in a variety of ways, but there are additional safeguards we believe should be added as well. In particular, we recommend that legislation limiting face recognition include at least five key policy priorities:

1) Requiring that face recognition searches are based on probable cause
2) Limiting use of face recognition to the investigation of serious crimes
3) Prohibiting face recognition from being used as the sole basis for arrests
4) Requiring notice to defendants whenever face recognition is used
5) Prohibiting face recognition from being used for untargeted surveillance

Require Face Recognition Searches Be Based on Probable Cause

Requiring that law enforcement demonstrate probable cause that an unknown person in question has committed a crime before they use face recognition to identify that individual is a critical safeguard for preventing abuse. The primary police use for face recognition is to scan photographs of individuals taken during commission of a crime; demonstrating probable cause in such scenarios should not be an onerous burden for supporting legitimate law enforcement goals.

This requirement is essential to stopping face recognition from being used to catalog and target individuals engaged in constitutionally protected activities such as protesting, participating in political rallies, or attending religious services. The danger of this surveillance technology being misused in such a manner is not theoretical: Police have used face recognition on multiple occasions in recent years to identify peaceful civil rights protesters.[2] Without a probable cause requirement, police could also use face recognition as a dragnet surveillance tool, scanning, identifying, and cataloging individuals' activities on a mass scale.

While last year's legislation establishes some requirements for police to conduct face recognition searches, the probable cause requirement in H.135 and S.47 would prevent mass surveillance and abuse without hampering legitimate law enforcement uses. Further, the legislation makes sensible exceptions, such as an emergency involving immediate danger or the identification of a deceased person.[3] Raising the standard to probable cause would still support law enforcement needs while closing the door to fishing and excess scans to identify people, including during sensitive activities and interactions.

[2] Joanne Cavanaugh Simpson and Marc Freeman, "South Florida police quietly ran facial recognition scans to identify peaceful protestors. Is that legal?" *South Florida Sun Sentinel*, June 26, 2021, https://www.sun-sentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sll5uuaqfbeba32rndlv3xwxi-htmlstory.html; Kevin Rector and Alison Knezevich, "Social media companies rescind access to Geofeedia, which fed information to police during 2015 unrest," *Baltimore Sun*, October 11, 2016, https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html.

[3] An Act to Regulate Face Surveillance, H.135, 192nd Gen. Ct., 1st Sess. Section 1(d)(1) (Mass. 2021), https://malegislature.gov/Bills/192/H135/; An Act to Regulate Face Surveillance, S.47, 192nd Gen. Ct., 1st Sess. Section 1(d)(1) (Mass. 2021), https://malegislature.gov/Bills/192/S47.

Limit Use of Face Recognition to Investigating Serious Crimes

Another key pillar of effective safeguards on face recognition is limiting its use to the investigation of serious crimes. The concept of limiting use of powerful surveillance tools to top-tier investigations has clear precedent: It has been applied for over 50 years in similar surveillance contexts such as wiretapping.[4]

Face recognition should not be used to stockpile suspects for investigation of minor offenses. In many places, police already use face recognition to investigate minor offenses such as shoplifting less than $15 of goods or stealing a pack of beer.[5] These low-profile cases often receive little scrutiny, so it is more likely that erroneous uses of face recognition—which can stem from a variety of causes such as algorithmic bias, poor image quality, lax software settings, or even pseudo-scientific techniques[6]—will go unnoticed. For minor offences, it's also more likely that potentially exculpatory evidence will not be sought out. This is especially concerning because face recognition can be notoriously inaccurate, especially for women and people of color.[7]

A serious crime limit for face recognition would also prevent the misuse of discretionary powers, including selective targeting of marginalized communities and dissidents. For example, in 2015, as demonstrators protested the death of Freddie Gray in police custody, Baltimore police used face recognition to target protesters, scanning the crowd with the technology to find and arrest anyone who had an outstanding warrant for any offense.[8] Without a serious crime limit, face recognition could be used in this manner on a broad scale, weaponized for selective enforcement of bench warrants for minor offenses and targeted at marginalized communities, political dissidents, and other vulnerable individuals.

[4] 18 USC 2510 *et seq*.

[5] Drew Harwell, "Oregon became a testing ground for Amazon's facial-recognition policing. But what if Rekognition gets it wrong?" *Washington Post*, April 30, 2019, https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/; Ebony Bowden, "How cops used a photo of Woody Harrelson to catch a beer thief," *New York Post*, May 16, 2019, https://nypost.com/2019/05/16/how-cops-used-a-photo-of-woody-harrelson-to-catch-a-beer-thief/.

[6] Police sometimes use face recognition in unreliable ways, such as to conduct scans on sketches, computer-edited images, or even celebrity lookalikes. Clare Garvie, "Garbage In, Garbage Out: Face Recognition on Flawed Data," Georgetown Law Center on Privacy & Technology, May 16, 2019, https://www.flawedfacedata.com/.

[7] Patrick Grother, Mei Ngan, Kayee Hanaoka, National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR 8280 (December 19, 2019), 2, https://doi.org/10.6028/NIST.IR.8280; Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research*, vol. 81 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Joy Buolamwini and Inioluwa Deborah Raji, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products," *AIES '19: Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society* (2019), https://www.media.mit.edu/publications/actionable-auditing-investigating-the-impact-of-publicly-naming-biased-performance-results-of-commercial-ai-products/; Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots," American Civil Liberties Union, July 26, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28; Brendan Klare et al., "Face Recognition Performance: Role of Demographic Information," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6 (December 2012), http://openbiometrics.org/publications/klare2012demographics.pdf.

[8] Rector and Knezevich, "Social media companies rescind access to Geofeedia" [see note 2].

By restricting use of the technology to investigating violent felonies, H.135 and S.47 prevent these risks while still permitting limited use for investigating offenses, such as homicides, that are genuine public safety priorities.[9]

Prohibit Face Recognition from Being Used as the Sole Basis for an Arrest

In addition to the measures above designed to prevent abuse and excess surveillance, effective safeguards on face recognition must also include policies that prevent excess reliance on the technology, which can be prone to error. There are already numerous documented instances when a face recognition misidentification led to a wrongful arrest.[10] While a probable cause warrant to run scans provides significant value, it does not prevent the harms that can arise when law enforcement excessively relies on the results of searches.

Factors that reduce image quality, such as bad lighting, indirect angles, distance, poor cameras, and low image resolution, all make misidentifications more likely. Lax system settings, such as employing a lower confidence threshold to trigger matches[11] or having broad sets of matches appear in search results, increase the potential that law enforcement will receive erroneous matches as well. Even as face recognition software improves in quality—and even if algorithmic bias dissipates—there will always be situation-based limits to how effective the technology is. And there will always be a danger in giving too much credence to matches that could misidentify innocent individuals.

Current law does not place a limit on how much police can rely on face recognition matches, and unfortunately, as currently written, H.135 and S.47 do not remedy this problem. We recommend these bills be strengthened to prevent face recognition matches from being the sole basis for an arrest, or on their own represent probable cause for a search. This is a key safeguard to preventing harm from over-reliance on misidentifications.

Require Defendants Be Given Notice When Face Recognition Is Used

Like any other complex forensic tool, face recognition's effectiveness can depend on technical factors and manner of use. That is why it is critical that defendants are notified and given the opportunity to examine face recognition technology whenever it is used in an investigation.

[9] H.135, Section 1(d)(1) [see note 3]; S.47, Section 1(d)(1) [see note 3].

[10] Kashmir Hill, "Wrongfully Accused By An Algorithm," *New York Times*, June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; K. Holt, "Facial recognition linked to a second wrongful arrest by Detroit police," *Engadget*, July 10, 2020, https://www.engadget.com/facial-recognition-false-match-wrongful-arrest-224053761.html; Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *New York Times*, December 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[11] Confidence thresholds are a metric built into face recognition systems that acts as a scale for comparing which photos are more or less likely to be a match within that system. When face recognition systems are set to return results at lower confidence thresholds, it leads to matches that are more likely to be misidentifications. Jake Laperruque, "About-Face: Examining Amazon's Shifting Story on Facial Recognition Accuracy," Project On Government Oversight, April 10, 2019, https://www.pogo.org/analysis/2019/04/about-face-examining-amazon-shifting-story-on-facial-recognition-accuracy/.

Defendants have a vested interest in reviewing a variety of factors, such as algorithm quality, the software settings police used, and whether any other potential matches were discovered or investigated, that could provide exculpatory or mitigating evidence. Guaranteeing access to this information is not only critical for due process rights but also acts as an important safeguard to deter corner cutting and sloppy use of face recognition during investigations.

Despite the importance of disclosure, it rarely occurs.[12] In some jurisdictions, law enforcement uses facial recognition thousands of times per month, and defendants almost never receive notice of its use in investigations.[13] Yet even as law enforcement relies on the technology for investigations, they obscure it from examination in court by defendants and judges.[14] In Massachusetts, current law does not provide any due process protections for criminal defendants who have been subject to the use of facial recognition systems.

H.135 and S.47 require that law enforcement agencies and district attorneys make available to criminal defendants and their attorneys all records and information pertaining to face recognition searches performed or requested during investigations.[15] This requirement would protect due process rights and strongly incentivize law enforcement to adhere to the highest standards in their use of face recognition.

Prohibit Face Recognition from Being Used for Untargeted Surveillance

One especially dangerous form of face recognition is in its use not to identify a designated person in an image but rather to conduct untargeted scans of all individuals on video streams.

According to early testing, untargeted face recognition is notoriously inaccurate: In pilot programs in the United Kingdom, South Wales Police had a 91% error rate and London Metropolitan Police had a 98% error rate.[16] In the United States, the technology has not received any type of comparable tests or vetting.

Yet even if untargeted face recognition improves in accuracy, it would still present a serious threat to civil rights and civil liberties. This type of surveillance system could effortlessly monitor individuals' movements, interactions, and activities on a mass scale.

Current law does not regulate the use of face recognition for purposes of surveillance of public spaces, leaving open the possibility of video surveillance systems incorporating untargeted face

[12] Aaron Mak,"Facing Facts," *Slate*, January 25, 2019, https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html.

[13] Jennifer Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short," *New York Times*, January 12, 2020, https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

[14] Face recognition "can play a significant role in investigations, though, without the judicial scrutiny applied to more proven forensic technologies." Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short" [see note 13].

[15] H.135, Section 1(g) [see note 3]; S.47, Section 1(g) [see note 3].

[16] Big Brother Watch, *Face Off: The Lawless Growth of Facial Recognition in UK Policing* (May 2018), 3-4. https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf.

recognition in the future. H.135 and S.47 would pre-empt this danger by prohibiting the use of untargeted face recognition for general public surveillance.[17]

We encourage you to consider bills H.135 and S.47 when you decide on further regulations of face recognition technology. We need strong safeguards to ensure that this technology does not infringe on civil rights and civil liberties, and this legislation offers an effective path for achieving this important goal.

Thank you for your attention and consideration.

Jake Laperruque
Senior Counsel
The Constitution Project at the Project On Government Oversight

[17] H.135, Section 1(d) [see note 3]; S.47, Section 1(d) [see note 3].