AMERICAN CIVIL LIBERTIES UNION FOUNDATION
New Jersey

P.O. Box 32159
Newark, NJ 07102

Tel: 973-642-2086
Fax: 973-642-6523

info@aclu-nj.org
www.aclu-nj.org

AMOL SINHA
Executive Director

MARC BEEBE
President

COMMENTS OF THE AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY AND 25 NEW JERSEY-BASED ORGANIZATIONS ON LAW ENFORCEMENT USE OF FACIAL RECOGNITION

March 10, 2022

Please direct inquiries to: Dillon Reisman, Skadden Fellow, ACLU-NJ (dreisman@aclu-nj) and Molly Linhorst, Staff Attorney, ACLU-NJ (mlinhorst@aclu-nj.org)

I. Introduction

As twenty-six organizations representing a wide cross-section of the New Jersey community, we are heartened to see the Office of the Attorney General (OAG) proactively considering the role new technologies like facial recognition will play in New Jersey's future and its awareness of the dangers that such technologies can pose to civil liberties. The OAG's desire to implement policies and regulations governing law enforcement use of facial recognition technology reflects thoughtful consideration for the rights of New Jerseyans.

We write today, however, to express our view that the use of facial recognition technologies by law enforcement presents a unique threat to our communities' well-being. These technologies jeopardize our ability to live safe, private lives free of constant government intrusion and scrutiny and discourage New Jerseyans from comfortably exercising their constitutional rights to speak freely, associate freely, or freely enjoy their neighborhoods. Although we offer responses to the OAG's prompts for what should be included in a potential law enforcement policy on facial recognition, only one policy adequately addresses our concerns: law enforcement should be banned from using facial recognition technology.

In this comment, we share why facial recognition technologies present serious and insurmountable dangers when used by law enforcement. Facial recognition tools in law enforcement contexts are not particularly good at their job: many routinely misidentify non-white faces, particularly female faces, at higher rates, leading to serious consequences when those identifications lead to increased scrutiny or wrongful arrests. Nor do facial recognition tools replace the need for human analysts, who we already know are often unreliable at identifying faces and can be tricked by erroneous face matches proposed by the tools.

But even if the technology were accurate across races, genders, ages, and all other variables, facial recognition still poses an unacceptable burden to over-policed communities of color and threatens individual constitutional rights. Facial recognition technologies are not merely another

tool in the police's investigative arsenal, but fundamentally change the relationship between the people, their government, and their physical world. They are an obstacle to the public's ability to express themselves, to protest, or to simply carry on their private lives without fear of government intrusion.

We offer our perspective on individual rules and regulations in an appendix to this comment, and commend the OAG for starting this conversation, but we are firm in our belief that such rules are at best a form of harm reduction. Ultimately, the law enforcement use of facial recognition must be banned in its entirety. For these reasons, we conclude that the State cannot safeguard against the dangers these technologies present, and we urge the Office of the Attorney General to adopt a policy prohibiting any and all uses of facial recognition technology by law enforcement in New Jersey.

II. The use of facial recognition by law enforcement exacerbates and perpetuates the over-policing and mass surveillance of Black and Latinx communities, infringes on the fundamental right of people to live public lives free of constant government scrutiny, and should be banned.

By comparing an unknown person's "faceprint" to a gallery of known faces, facial recognition technology grants its users the power to identify unknown people from surveillance videos, body-worn camera imagery, or other image sources. Law enforcement agencies may employ it to generate leads, identify witnesses, or track suspects all at the push of a button. But empowering law enforcement with that technology—even if we were to assume that facial recognition performs with a high-degree of accuracy—comes at a steep price for the public. Facial recognition tools bring about a fundamental change in the public's relationship with the police, the government, and their own communities. The technology introduces a categorically new kind of mass surveillance.

A. Facial recognition tools themselves are too unreliable for law enforcement use: they are worse at identifying darker-skinned people of color, exacerbate human biases, and do not perform well on low-quality images common in law enforcement contexts.

Every stage of facial recognition's development and use introduces a new source of error, the sum of which makes facial recognition tools deeply unreliable within the law enforcement context. The result? Rather than contribute meaningfully to reducing crime, facial recognition tools frequently misidentify suspects and mislead police, with people of color bearing the brunt of these errors.

Inherent racial biases are common in facial recognition algorithms: Facial recognition tools are not built in a vacuum — because of how they are developed, they frequently reflect societal

biases against people of color. Many facial recognition algorithms used today are less accurate when analyzing the faces of darker-skinned individuals. The National Institute of Standards and Technology confirmed this effect in its study of available commercial and academic facial recognition algorithms: many algorithms produced far more "false positives"—that is, they proposed possible identities for unknown faces that were ultimately incorrect—for faces of people of African, Asian, and Native American descent.[1] The disparity was even more pronounced for women than men. Drs. Joy Buolamwini and Timnit Gebru observed similar disparities in their landmark study of mainstream commercial facial analysis tools, which were substantially less effective at analyzing the faces of darker-skinned women.[2] While tools may improve in the future, this is an endemic problem in facial recognition development.

It is distressing that law enforcement might come to rely on a technology with an *empirically proven* tendency towards racially biased results. In real law enforcement terms, a higher rate of false positives for people of color translates into a higher rate of misdirected investigations, undue scrutiny, and, ultimately, wrongful arrests. We should not ask whether we might be able to "tolerate" a certain level of racial disparity in law enforcement's use of facial recognition.

Automation bias: Facial recognition tools' performance also relies heavily on human operators and analysts to interpret the tools' results, which introduces human biases into the already technically biased facial recognition process.[3] For example, people often experience "automation bias," where they will put undue weight or trust in a decision or assertion when they are told the decision was made by a machine. One study uncovered this bias in people evaluating facial recognition results: when human evaluators were told that a computer had discovered two faces were identical, they were more likely to accept the match and be more confident the match was correct.[4] If the evaluators were just told to evaluate the face's similarity without any suggestion

---

[1] A "false positive" occurs when the facial recognition tool returns a match between an unknown face and a known identity, but that proposed match is incorrect. Patrick Grother, Mei Ngan & Kayee Hanaoka, National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[2] One major source of this disparity is in the "training" and "benchmark" datasets that are used to develop facial recognition algorithms. Generally, the performance of facial recognition tools is often measured using datasets that contain the faces of mostly light-skinned men. Algorithms may appear to work well on those datasets, when in reality the algorithms have never been trained to recognize darker-skinned women. Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proceedings of Machine Learning Research 1-15 (2018), https://www.media.mit.edu/publications/gender-shades-intersectional-accuracy-disparities-in-commercial-gender-classification/.

[3] The police chief of Detroit, Michigan, in explaining how facial recognition tools require human analysts to interpret their results, estimated that a facial recognition tool working *alone*, without a human analyst, would misidentify subjects about "96 percent of the time." Jason Koebler, *Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time*, Vice (June 29, 2020), https://www.vice.com/en/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time.

[4] Lauren Chambers & Emiliano Falcon-Morano, *Bias All the Way Down: Research Shows Domino Effect When Humans Use Facial Recognition Algorithms*, Privacy SOS (Sep. 22, 2020),

that a computer had already proposed a match, they expressed more doubt that the faces were similar. In law enforcement, this sort of bias induces officers to put undue trust in the identifications made by facial recognition tools even if their own eyes tell them differently.

Cross-racial identification and poor image quality: The error from automation bias compounds when we consider that people are generally worse at *cross-racial* face identification. When presented with a suspect of a different race, analysts may be more likely to defer to an error-prone facial recognition tool's decisions.[5]

Furthermore, the poor quality of the images the police will use for facial recognition —which are often gathered from surveillance videos at bad angles and with poor lighting—also contributes to likely inaccuracies. Facial recognition tools are much less effective when applied to photos in which the subject is not facing the camera straight on, or where the lighting is poor.[6] These conditions also hurt the ability of human analysts to second-guess the computer at the precise moment when the computer is at its least accurate.[7]

Human operator misuse of facial recognition tools: Across the country, officers have come up with many "creative" and unacceptable ways to use the facial recognition tools at their disposal. When the quality of the available probe image is too low for facial recognition to work effectively, many officers will attempt to edit the photo to force the system to generate results. Some officers have even inserted police sketches into facial recognition systems in lieu of live imagery, hoping for usable results.[8]

A study by the Georgetown Center on Privacy & Technology uncovered other shocking and downright strange techniques: from officers editing in a different mouth to change the suspect's expression, to inserting open eyes if the subject's eyes are closed, to mirroring one half of the

---

https://privacysos.org/blog/bias-all-the-way-down-research-shows-domino-effect-when-humans-use-face-recognition-algorithms/ (citing John J. Howard, Laura R. Rabbitt & Yevgeniy B. Sirotin, *Human-Algorithm Teaming in Face Recognition How Algorithm Outcomes Cognitively Bias Human Decision-Making*, PLoS ONE 15(8) (2020), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0237855).

[5] *See State v. Henderson*, 208 N.J. 208, 267 (2011) (explaining that cross-racial identifications tend to be less reliable than same-race identifications) (citing *State v. Cromedy*, 158 N.J. 112, 120 (1999)).

[6] Patrick Grother, Mei Ngan & Kayee Hanaoka, National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT) Part 2: Identification 5 (2019), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf (reporting that "recognition error rates are much higher, often in excess of 20%" when facial recognition is used on poorer quality images that do not capture a person's face fully).

[7] Eleni Manis, Albert Fox Cahn, Naz Akyol & Caroline Magee, *Scan City: A Decade of NYPD Facial Recognition Abuse* 3 (2021), https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/60e5dd3bed032877ec8e3be9/1625677116317/2021.7.7_Scan+City_FINAL.pdf.

[8] *Id.*

subject's face if the other half is obscured, to even combining multiple people's faces into one.[9] One NYPD officer, believing a suspect looked like Woody Harrelson, attempted to use a photo of the celebrity to identify the suspect.[10]

When officers or analysts edit their probe images, or submit sketches, they completely undermine the intended use of the facial recognition system. The practice adds more subjectivity to an already error-prone process and leads the police to rely on methodologies that produce unreliable results. No matter what controls the OAG might put into a place, there is ample room for the police to misuse facial recognition in unexpected and harmful ways.

B. Facial recognition tools will perpetuate the over-policing of communities of color.

Even if facial recognition algorithms themselves were equally accurate at identifying people regardless of race, our past and present reality of racially disparate policing means that facial recognition tools' harms and errors are not felt nor experienced equally. New surveillance technologies frequently subject communities of color to surveillance and control that would not be tolerated in white communities, in large part because they are embedded in an existing infrastructure of biased and racist policing practices.[11] Facial recognition is no exception.

New Jersey's communities of color are already over-policed and over-surveilled.[12] Black and Hispanic drivers are pulled over and arrested at higher rates than white drivers throughout New Jersey.[13] Before legalization, Black people were arrested for marijuana-related offenses at a rate

---

[9] Clare Garvie, Georgetown Center on Privacy & Technology, *Garbage In, Garbage Out* (2019), https://www.flawedfacedata.com/.

[10] *Id.*

[11] For example, a study of the law enforcement use of "Stingrays" (cellphone surveillance trackers) in several cities found that Stingrays were over-concentrated in Black communities relative to white communities with similar levels of crime. George Joseph, *Racial Disparities in Police 'Stingray' Surveillance, Mapped*, Bloomberg CityLab (Oct. 18, 2016), https://www.bloomberg.com/news/articles/2016-10-18/u-s-police-cellphone-surveillance-by-stingray-mapped. *See also* Barton Gellman & Sam Adler-Bell, *The Disparate Impact of Surveillance* 27 (2018), https://tcf.org/content/report/disparate-impact-surveillance/ ("What disquiets us as we look ahead is the strong potential of new technologies, networked and integrated with the ones we have, to compound the harms of unequal treatment with new burdens on those citizens least capable of bearing them.").

[12] *See, e.g.,* ACLU-NJ, *Selective Policing: Racially Disparate Enforcement of Low-Level Offenses in New* Jersey 4 (2015), https://www.aclu-nj.org/files/7214/5070/6701/2015_12_21_aclunj_select_enf.pdf ("In each case, the study identified extreme racial disparities in the number of arrests of Black and White people for low-level offenses."); Udi Ofer & Ari Rosmarin, ACLU-NJ, *Stop-and-Frisk: A First Look: Six Months of Data on Stop-and-Frisk Practices in Newark* 8 (2014), https://www.aclu-nj.org/files/8113/9333/6064/2014_02_25_nwksnf.pdf ("Although [B]lack Newarkers comprise 52 percent of the city's population, they make up 75 percent of total stops by the Newark Police.").

[13] Colleen O'Dea, *State Police Arrest, Charge More Black, Hispanic Drivers Than White*, NJ Spotlight News (July 9, 2021), https://www.njspotlightnews.org/2021/07/nj-state-police-traffic-stops-more-blacks-more-hispanics-more-summonses-more-arrests.

3.45 times higher than white New Jerseyans.[14] The racial disparities in our prisons are even worse: New Jersey's Black residents are incarcerated at a rate *12.5 times* that of whites.[15]

Just as facial recognition tools are not built in a vacuum, they are not deployed in a vacuum — the existing racial disparities in policing will impact how facial recognition tools are employed and how the technology returns face matches. When law enforcement uses facial recognition tools to identify an unknown face, they often compare the image to a "gallery" of known identities drawn from existing mugshots. People with prior interactions with the criminal legal system are more likely to be identified as the objects of suspicion because their mugshots exist in the gallery. This presents the "dirty data" problem[16] implicit in police databases: racist policing practices have resulted in a disproportionate number of arrests of people of color, whose faces then populate police mugshot databases, resulting in increased, wrongful scrutiny by facial recognition searches.

The result is that people who were arrested, photographed, but never convicted of any offense, which disproportionately includes people of color, are subject more than anyone else to the "perpetual line-up" of facial recognition.[17] Facial recognition tools reflect the biased policing of the past and reinforce biased policing into the future.

But the full story of the harm wrought by racial disparities in law enforcement in New Jersey cannot be told just with statistics of disparity: victims of racialized policing experience a serious and unquantifiable trauma.[18] The ongoing scrutiny and suspicion cast on communities of color by racist facial recognition practices only compounds that trauma. The stories of people who were inaccurately matched by facial recognition and wrongfully detained help to illustrate this trauma. For example, Robert Julian-Borchak Williams, a Black man from Detroit, was detained

---

[14] *Racial Disparities in Marijuana Arrests Across New Jersey Worsen, Report Reveals, Making Legalization More Urgent*, ACLU-NJ (Apr. 20, 2021), https://www.aclu-nj.org/news/2020/04/20/racial-disparities-marijuana-arrests-across-new-jersey-worse.

[15] *Report: New Jersey Racial and Ethnic Disparities in Prisons Are Worst in the Nation*, ACLU-NJ (Oct. 19, 2021), https://www.aclu-nj.org/news/2021/10/19/report-new-jersey-racial-and-ethnic-disparities-prisons-are (citing Ashley Nellis, The Sentencing Project, *The Color of Justice: Racial and Ethnic Disparity in State Prisons* (2021)).

[16] *Cf.* Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. Rev. Online 15 (2019), https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/ (describing how policing data from police departments with histories of biased practices established in federal consent decrees, including Newark, can skew the performance of policing tools that rely on that data).

[17] Clare Garvie, Alvaro Bedoya & Jonathan Frankle, Georgetown Ctr. of Privacy & Tech., *The Perpetual Line-up: Unregulated Police Face Recognition in America* (2016), https://www.perpetuallineup.org ("[D]ue to disproportionately high arrest rates, systems that rely on mug shot databases likely include a disproportionate number of African Americans.").

[18] *See, e.g.,* Brief of *Amici Curiae* 66 Black Ministers and Other Clergy Members, *State v. Nyema*, ___ A.3d ___ (N.J. Jan. 25, 2022) (Nos. 082858 & 085146), 2022 WL 211436, https://www.aclu-nj.org/files/2816/2023/9516/2020.5.3_ACLU_brief_Myers_and_Nyema.pdf.

for over 30 hours after a facial recognition system pulled his drivers' license photo from a gallery, and despite the obvious fact that he was not the man in the image from the crime.[19] Closer to home, Nijeer Parks, a Paterson, New Jersey resident, was arrested and held in jail for ten days for shoplifting after being identified by a facial recognition system despite proof that he was thirty miles away at the time of the offense.[20] The trauma done to these men and their families by the use of facial recognition has followed them since their arrests.[21]

Arming the police with mass surveillance tools will not translate to safer communities—it will mean more people of color are scrutinized as "suspects" for crimes they did not commit and subject them to trauma at the hands of the government.[22] As expressed by Black Lives Matter Paterson, it is no wonder that many view facial recognition as the latest iteration of the "ever increasing surveillance and policing of our communities."[23]

C. Facial recognition tools threaten our constitutional rights under the First and Fourth Amendments.

Facial recognition systems are more than law enforcement tools—they enable the government to track where people are going and with whom people are meeting. The knowledge that the government can identify individuals at the push of a button fundamentally changes the public's relationship with their own cities and neighborhoods and can even shape and limit the public's activities. This type of surveillance is the functional equivalent of forcing every person to walk around with their driver's license displayed on their clothing and to carry a GPS tracking device. Facial recognition therefore presents a technology susceptible to government abuse and overreach. These harms violate the public's constitutional rights under the First and Fourth Amendments and analogous provisions of the State Constitution.

---

[19] Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. Times (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

[20] Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. Times (Dec. 29, 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[21] Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*, Wired (Mar. 7, 2022), https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/.

[22] Naomi Ishisaka, *Is Surveillance Tech Widening America's Racial Divide?*, GovTech (Oct. 28, 2019), https://www.govtech.com/public-safety/is-surveillance-tech-widening-americas-racial-divide.html.

[23] *See, e.g.*, *Black Lives Matter Paterson Statement on the Use of Facial Recognition Software in New Jersey*, Insider NJ (Feb. 14, 2022), https://www.insidernj.com/press-release/black-lives-matter-paterson-statement-use-facial-recognition-software-new-jersey.

Fourth Amendment harms

The Fourth Amendment to the U.S. Constitution protects against unreasonable searches and seizures, and Article I, Section 7 New Jersey Constitution provides even stronger protections.[24] While the facial recognition jurisprudence is still evolving, the U.S. Supreme Court and New Jersey Supreme Court have examined how other tracking technologies implicate Fourth Amendment rights.

In 2013, the New Jersey Supreme Court concluded that because location tracking technologies have enlarged surveillance capacities so significantly, allowing the police to see "not just where people go—which doctors, religious services, and stores they visit—but also the people and groups they choose to affiliate with and when they actually do so," people must have an expectation of privacy in the records arising from such surveillance.[25] Five years later, the U.S. Supreme Court similarly found a legitimate expectation of privacy in location-based tracking through cell phones under the Fourth Amendment, concluding that the acquisition of these sorts of location-based records generally requires a warrant.[26]

Tracking through facial recognition analysis is at least as dangerous to the public's privacy interests as cell phone location records, and yet we lack virtually any limitations on its use. In finding that location tracking via cell phones was an invasive search requiring a warrant, the U.S. Supreme Court explained that with location tracking, suspects are "effectively [] tailed every moment of every day for five years," and that "only the few without cell phones could escape this tireless and absolute surveillance."[27]

Unlike cell phones, we cannot leave our faces at home. Whenever we walk into a bar, a health clinic, a church, or a political demonstration, facial recognition can subject us to perpetual tracking, an intrusion far more expansive than the sort of cell-phone or GPS tracking previously considered in search and seizure cases.[28] Widespread video surveillance of New Jersey's cities makes that threat real and directly interferes with our enjoyment of our constitutional right to be

---

[24] The list of cases where New Jersey Courts provide greater protection against unreasonable searches and seizures is long. *See*, *e.g.*, *State v. Alston*, 88 N.J. 211, 228-29 (1981) (taking broad view of standing to challenge validity of searches); *State v. Earls*, 214 N.J. 564, 568-69 (2013) (recognizing expectation of privacy in cell phone location information). While federal constitutional jurisprudence "may serve to guide us in our resolution of New Jersey issues, 'we bear ultimate responsibility for the safe passage of our ship.'" *State v. Cooke*, 163 N.J. 657, 670 (2000) (*quoting State v. Hempele*, 120 N.J. 182, 196 (1990)).

[25] *Earls*, 214 N.J. at 587.

[26] *Carpenter v. U.S.*, 138 S. Ct. 2206, 2217 (2018) (concluding that under the Fourth Amendment "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell phone records]").

[27] *Carpenter*, 138 S. Ct. at 2218.

[28] *See id.* (considering the Fourth Amendment implications of cell site location information)*; U.S. v. Jones*, 565 U.S. 400 (2012) (considering the Fourth Amendment implications of police use of GPS tracking devices).

left alone from the government's constant scrutiny.[29] The police's ability to perform a facial recognition search on past stored surveillance videos, potentially capturing the public's past movements for weeks or months, represents a particularly intrusive kind of search.[30] The OAG's proposed "ban on dragnet or real-time surveillance" does not alleviate those Fourth Amendment concerns.

First Amendment harms

Our First Amendment rights under the Federal Constitution and Article I, Section 6 rights under the New Jersey Constitution fare no better against widespread facial recognition use.[31] Those publicly exercising their First Amendment and state constitutional right to protest have been subject to investigation and arrest due to facial recognition.[32] Even short of arrest, mass surveillance has a concrete and negative impact on the public's wellbeing. The "feeling of being watched" can induce people to self-censor, limit their own public activities, and ultimately lose their freedom to live public and safe lives.[33] "Awareness that the government may be watching

---

[29] *See, e.g.,* James Kilgore, *A Model City*, Inquest (Feb. 5, 2022), https://inquest.org/a-model-city (describing the broad scope of surveillance coverage of Camden); Rick Rojas, *In Newark, Police Cameras, and the Internet, Watch You*, N.Y. Times (June 9, 2018), https://www.nytimes.com/2018/06/09/nyregion/newark-surveillance-cameras-police.html (describing Newark's use of surveillance cameras and its program allowing people to view the camera feeds and report crime).

[30] *See U.S. v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring) (arguing that law enforcement's ability to track a person's car via GPS for even just four weeks was "surely" past the line at which the intrusion became a search).

[31] The New Jersey Constitution contains an affirmative right to free speech, which provides greater protections than those found in the First Amendment. *State v. Schmid*, 84 N.J. 535, 557-60 (1980); *compare* N.J. Const. Art 1, Para 6 ("Every person may freely speak, write and publish his sentiments on all subjects") *with* U.S. Const. Amend. 1 ("Congress shall make no law . . . abridging the freedom of speech").

[32] *See, e.g.,* James Vincent, *NYPD Used Facial Recognition to Track Down Black Lives Matter Activist*, Verge (Aug. 18, 2020), https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram; Joanne Cavanaugh Simpson & Marc Freeman, *South Florida Police Quietly Ran Facial Recognition Scans to Identify Peaceful Protestors. Is That Legal?*, S. Fla. Sun Sentinel (Jun. 26, 2021), https://www.sun-sentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sll5uuaqfbeba32rndlv3xwxi-htmlstory.html; Juliette Rihl, *Emails Show Pittsburgh Police Officers Accessed Clearview Facial Recognition After BLM Protests*, PublicSource (May 20, 2021), https://www.publicsource.org/pittsburgh-police-facial-recognition-blm-protests-clearview.

[33] Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 Geo. Mason. L. Rev. 409, 434–35 (2014). It has been long understood that surveillance—and the knowledge that one is under surveillance—alters behavior and can be used as a means of social control: English philosopher and social theorist Jeremy Bentham first theorized about "panopticons"—government buildings designed around a central tower allowing officials to spy on building's residents, without their knowledge, at any moment—in the late 18th century. Since Bentham's time, the prescient model of the "panopticon" has become a reality in the electronic surveillance tools available to state institutions. *See* Mitchell Gray, *Urban Surveillance and Panopticism: Will We Recognize the Facial Recognition Society?*, 1 Surveillance & Soc'y 314 (2003), https://pdfs.semanticscholar.org/9d04/bc3118d56ef03efc690decea2ddc8cd105d3.pdf.

chills associational and expressive freedoms."[34] Minority viewpoints are silenced when people feel they cannot speak safely.[35] The First Amendment recognizes that anonymous speech is part and parcel of free speech,[36] but facial recognition threatens our ability to speak anonymously in public, let alone our freedom to go to a sensitive doctor's appointment, attend church, or visit a gay bar without the government's constant awareness.

And again, data retained from surveillance cameras can always give law enforcement the ability to retroactively track someone throughout their day. Knowing that this potential always exists, people will still feel the oppression of constant surveillance and undue scrutiny under the threat of push-button identification.

This is to say nothing of the threat of "run-of-the-mill" law enforcement officer misuse of policing tools: officers have used the means at their disposal to subpoena businesses for their own personal vendettas,[37] to track people's cars outside of investigations with GPS devices,[38] and stalk people using pretextual traffic stops.[39] An Associated Press report uncovered more than 300 incidents of police abusing access to law enforcement databases between 2013 and 2015, including cases where officers tracked ex-girlfriends to harass them, their friends, or their partners.[40] Giving the police access to facial recognition tools invites trouble and heightens the power differential between the police and the public they serve.

The First and Fourth Amendment violations threatened by facial recognition represent a concrete harm—they represent damage done to our ability to live freely without the invasive, behavior-altering, and speech-limiting effects of constant government surveillance. The infrastructure of

---

[34] *U.S. v. Jones*, 565 U.S. 400, 416 (2012) (explaining the harms accompanying the use of GPS tracking devices).

[35] Karen Turner, *Mass Surveillance Silences Minority Opinions, According to Study*, Wash. Post (Mar. 28, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/mass-surveillance-silences-minority-opinions-according-to-study/.

[36] *Talley v. California*, 362 U.S. 60 (1960).

[37] Jeff Goldman & Chris Sheldon, *N.J. Detective Accused of Investigating Relative's Car Crash Faces Misconduct Charge*, NJ.com (Feb. 1, 2022), https://www.nj.com/cape-may-county/2022/02/nj-detective-accused-of-investigating-relatives-car-crash-faces-misconduct-charge.html.

[38] Anthony G. Attrino, *Police Officer Charged with Stalking After Tracking Device Found on Vehicle, Authorities Say*, NJ.com (Jan. 29, 2022), https://www.nj.com/cape-may-county/2022/01/police-officer-charged-with-stalking-after-tracking-device-found-on-vehicle-authorities-say.html.

[39] Suzanne Russell, *NJ State Trooper Pleads Guilty After Unlawfully Stopping, Stalking Women on Turnpike*, MyCentralJersey.com (Aug. 17, 2021), https://www.mycentraljersey.com/story/news/crime/2021/08/17/nj-state-trooper-michael-patterson-guilty-plea/8164101002/.

[40] Sadie Gurman, *Across US, Police Officers Abuse Confidential Databases*, Associated Press (Sept. 28, 2016), https://apnews.com/article/699236946e3140659fff8a2362e16f43 (reporting cases where police officers used law enforcement tools to stalk victims of domestic violence, journalists, and neighbors).

facial recognition is one of the "most uniquely dangerous surveillance mechanism[s] ever invented" and must be treated that way.[41]

Conclusion

For all of the reasons detailed above, the only ethical and practical response to the serious harm and Constitutional violations posed by facial recognition tools is to ban them outright from law enforcement use. No matter how much the state may constrain their use, prescribe rules for human analysis, or impose technical metrics on their procurement, facial recognition tools seriously degrade our privacy in public spaces. They threaten our ability to speak freely and act freely. They impose massive burdens on our already overpoliced and over-surveilled communities of color. As organizations whose perspectives are informed by and grounded in the concerns and experiences of New Jerseyans, we can only reach one conclusion: New Jersey must ***ban law enforcement use of facial recognition tools.*** Anything less would represent a loss of civil liberties and a blow to racial justice.[42]

Signed,

American Civil Liberties Union of New Jersey

All of Us or None, South Jersey

American Friends Service Committee Prison Watch

Antiracism in Action

Association of Criminal Defense Lawyers of New Jersey

Bayard Rustin Center for Social Justice

Faith in New Jersey

Latino Action Network Foundation

LatinoJustice PRLDEF

Libertarians for Transparent Government

---

[41] Woodrow Harzog & Evan Selinger, *Facial Recognition Is the Perfect Tool for Oppression*, Medium (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.

[42] The Acting Attorney General has made clear that racial justice "is a top priority" and identifying the "moral obligation to act now to promote racial justice and equity for underserved communities." https://www.njoag.gov/programs/racial-justice/.

Make the Road New Jersey

National Organization for Women of New Jersey

New Jersey Alliance for Immigrant Justice

New Jersey Coalition to End Domestic Violence

New Jersey Office of the Public Defender

New Jersey Prison Justice Watch

Newark Communities for Accountable Policing

Our Revolution Essex

Our Revolution Monmouth

Our Revolution Trenton Mercer

People's Organization for Progress

Salvation and Social Justice

Unidad Latina en Acción NJ

UU FaithAction NJ

Volunteer Lawyers for Justice

Wind of the Spirit Immigrant Resource Center

APPENDIX: EVALUATION OF POLICY MEASURES TO REGULATE FACIAL RECOGNITION

The prohibitions, rules for human analysis, and technical measures proposed by the OAG merit a thoughtful response. Below, we examine and provide feedback on rules, restrictions, and measures that could be used to limit facial recognition. Ultimately, these measures do not sufficiently address our concerns—at best, they might only reduce the most severe harms felt by law enforcement's use of facial recognition.

A. The OAG would have to institute strict principles and prohibitions for law enforcement use of facial recognition.

The OAG has already identified several principles that should constrain any use of facial recognition by law enforcement:

Prohibition on the improper collection of personal images: Law enforcement must never use tools that search through images collected from non-governmental sources or when people have not given their consent to the use of the images for law enforcement purposes. We commend the OAG for continuing to recognize the necessity of the prohibition on Clearview AI, [43] and encourage the OAG to expand on this prohibition to exclude tools that search through databases that have not been previously vetted or approved of by state officials.

Prohibition on "dragnet" or "real-time" surveillance: Our civil liberties demand that facial recognition tools never be used to track people in real-time in public. But in addition to a ban on real-time surveillance, the OAG should similarly bar the use of facial recognition on any video recording whatsoever, even if not "real-time." For example, the danger of "dragnet" surveillance still exists if the police were to use facial recognition retrospectively on video feeds saved from surveillance cameras deployed across a city, particularly in light of the Fourth Amendment interests jeopardized by perpetual tracking.[44]

Prohibition on using results to justify arrests: We agree with the OAG that the results of a facial recognition search must never be used as a basis to justify an arrest or to prosecute an individual.[45] To that end, facial recognition results must be excluded from any process to obtain

---

[43] *See* Kashmir Hill, *New Jersey Bars Police From Using Clearview Facial Recognition App*, N.Y. Times (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/technology/clearview-ai-new-jersey.html.

[44] *Carpenter*, 138 S. Ct. at 2218 (noting that data logging practices for surveillance technologies make it so the "police need not even know in advance whether they want to follow a particular individual, or when," enhancing the harm to Fourth Amendment rights when police track a person retrospectively).

[45] There is state-wide precedent for this rule: Maine's law curtailing law enforcement use of facial recognition establishes that "facial surveillance data does not, without other evidence, establish probable cause justifying arrest, search or seizure." 25 M.R.S. § 6001(2)(E) (2021), *available at* https://legislature.maine.gov/statutes/25/title25sec6001.html. *See also Maine Enacts Strongest Statewide*

an arrest warrant. Facial recognition results may never be presented to a magistrate to show probable cause justifying an arrest.

In addition to the above prohibitions, we considered the following governance principles that could be used to constrain facial recognition use by law enforcement. We ultimately find that these principles are insufficient to fully address our concerns:

1) **Limiting the use of facial recognition to only serious crimes:** Only a limited class of criminal matters could ever begin to justify law enforcement's use of facial recognition, if it can be justified at all. For example, it should not be conceivable that facial recognition could be used to investigate anyone's conduct at a protest or while merely walking down the street. Facial recognition cannot be allowed to become a routine policing tool or pretextual excuse.

2) **Requiring transparency and public reporting:** Democratic accountability requires that the public have access to information about police tools and how they are used. To that end, any law enforcement agency utilizing facial recognition technology must make public any equipment purchased or obtained, the policy limitations placed on its use, and statistics regarding the cases in which facial recognition is used. Law enforcement agencies would also have to make their practices available for inspection by external, independent auditors who could evaluate the efficacy and harms of the agencies' use of facial recognition tools and publish their results. Unfortunately, when it comes to existing data collection and publication in law enforcement, particularly data and public reporting related to racial disparities, practices in New Jersey are extremely lacking.[46]

3) **Requiring disclosures to defendants:** The use of facial recognition in an investigation must be consistent with the state's obligations to afford defendants due process and ensure that defendants effectively have the ability to confront the witnesses against them.[47] For that reason, defendants must be given all records of facial recognition queries made in an investigation leading to their arrests, including the results of any search—including those not implicating the

---

Facial Recognition Regulations in the Country, ACLU (June 30, 2021), https://www.aclu.org/press-releases/maine-enacts-strongest-statewide-facial-recognition-regulations-country.

[46] *Selective Policing*, *supra* note 12, at 4 ("We were unable to gauge the full extent of the [racial] disparities because of serious flaws in the data collection practices of each police department.").

[47] *See, e.g., Power, Pervasiveness and Potential: The Brave New World of Facial Recognition Through a Criminal Law Lens (And Beyond)*, New York City Bar Association, Criminal Courts Committee (August 2020), https://www.nycbar.org/member-and-career-services/committees/reports-listing/reports/detail/facial-recognition-through-a-criminal-law-lens (collecting cases examining the constitutional implications of facial recognition technology).

defendant—and the identities of officers involved in the search.[48] Defendants must also have the opportunity to confront officers and analysts who managed the facial recognition search process.

4) Prohibiting the use of Motor Vehicle Commission and other public agency data sources: Driver's license photos, for example, are a much sought-after source of images of "known persons" for facial recognition. When people sign up for licenses, they are not consenting to be subjected to constant investigation and scrutiny. If law enforcement relies on the MVC or other public agencies' photograph databases to run facial recognition searches, there would be no realistic means for the public to avoid the harms accompanying constant surveillance. For that reason, it must be made clear that MVC databases (or similar state-wide, non-law-enforcement databases) can never be used for facial recognition.

5) Prohibiting the use of mugshots of people never convicted: As our comment explains, New Jersey law enforcement polices communities of color at a disproportionate rate. This can have a material impact on facial recognition in the form of mugshot databases. Given that Black and Latino people are overrepresented in arrests, they will also be overrepresented in databases of mug shots taken at the time of arrest.[49] This disproportionately subjects people of color from over-policed communities, most of whom will never be convicted of any crime, to a potential lifetime of electronic surveillance.[50] For that reason, mugshot databases should be avoided. It is unlikely that an acceptable law enforcement database of faces exists that would not bring similar concerns.

Ultimately, the decision for which database is better to use—MVC databases or mugshot databases—is a no-win scenario: law enforcement can either rely on mugshot databases, which will systemically reproduce racial bias and disparate policing, or on driver's license photos, which subjects the entire state to a constant privacy intrusion.

6) Prohibiting the use of private sources of surveillance imagery: Communities must have the ability to hold the police accountable and oversee what the police do in their neighborhoods. That accountability is particularly threatened when surveillance technologies rely

---

[48] *See* Khari Johnson, *The Hidden Role of Facial Recognition Tech in Many Arrests*, Wired (Mar. 7, 2022), https://www.wired.com/story/hidden-role-facial-recognition-tech-arrests (explaining that it's rare for defendants to be told that a facial recognition system played a role in their identification and arrest).

[49] Garvie et al., *supra* note 12.

[50] At a minimum, the OAG could at least limit the use of facial recognition only to mugshots where the individual was convicted, and ensure that expungements result in the exclusion of mugshots from all facial recognition databases. But this does not fully alleviate racial disparities from the remaining mugshots. And even when arrest records are sealed or expunged, mug shots may inevitably remain in databases because of improper or overlooked data management. *See, e.g.,* Eli Hager, *Your Arrest Was Dismissed. But It's Still in a Police Database.*, Marshall Project (July 18, 2019), https://www.themarshallproject.org/2019/07/18/your-arrest-was-dismissed-but-it-s-still-in-a-police-database.

on *private* infrastructure. Technologies like the Amazon Ring video doorbell, for example, give the police virtually unlimited access to video feeds covering hundreds of thousands of homes, all without a warrant.[51] The use of video and image data derived from these kinds of private sources directly conflicts with the OAG's desire to prevent facial recognition from becoming a "dragnet," and thus must be banned.

7) Prohibiting local police departments from independently acquiring and using facial recognition technology: New Jersey contains over 550 law enforcement agencies. The sheer size of our state's law enforcement system makes it difficult to account for all the ways that local police departments might use or abuse facial recognition tools, even in the face of strict OAG guidelines. The OAG must therefore outright prohibit local law enforcement agencies from acquiring facial recognition tools, and instead institute uniform processes to ensure consistent state-level oversight.[52]

8) Prohibiting cross-jurisdictional facial recognition requests: Any rules the OAG institutes on the use of facial recognition would be a dead letter if agencies could circumvent them by forwarding facial recognition requests to other jurisdictions. Without any means of oversight over how other jurisdictions manage their facial recognition tools, the OAG must prohibit law enforcement from turning to out-of-state agencies to conduct searches.

9) Ensuring facial recognition policies comply with the Immigrant Trust Directive and other laws restricting cooperation with federal immigration enforcement: Consistent with the Attorney General's Immigrant Trust Directive and other laws,[53] the OAG would have to make clear to law enforcement agencies that the Directive applies to any facial recognition tools and databases, particularly those that may rely on Motor Vehicle Commission data. We expect that the Directive's requirement that no New Jersey agency provide federal immigration authorities any access to local law enforcement databases or equipment[54] applies equally to facial recognition tools and the databases they rely on.

10) Prohibiting all non-identification uses of facial analysis technology: Although facial recognition tools used by law enforcement focus on identifying unknown faces, some facial recognition or facial analysis tools can be used for other categorization or analysis purposes. For example, some commercial facial analysis tools claim to be able to categorize people by gender

---

[51] Lauren Bridges, *Amazon's Ring Is the Largest Civilian Surveillance Network the US Has Ever Seen*, Guardian (May 18, 2021), https://www.theguardian.com/commentisfree/2021/may/18/amazon-ring-largest-civilian-surveillance-network-us.

[52] This is the approach taken by Massachusetts and Maine, which require local law enforcement to request facial recognition assistance through other, more centralized agencies. *See* 25 M.R.S. § 6001, *supra* note 45; Mass. Gen. Laws c. 6 § 220(b), https://www.mass.gov/info-details/mass-general-laws-c6-ss-220#(e)-.

[53] Att'y Gen. Dir. No. 2018-6 v2.0, available at https://www.nj.gov/oag/dcj/agguide/directives/ag-directive-2018-6_v2.pdf.

[54] *Id.* at § (II)(B)(3).

(i.e., "is the person in the image a man or woman?") or detect people's emotional state (i.e., "is the person happy, sad, angry, disgusted, confused, or excited?" commonly known as "affect" or "emotion" recognition). More extreme examples include sexual orientation classification or even "criminality" prediction, all based on the notion that these characteristics of a person can be determined from facial features alone. At worst, many of these tasks resemble the pseudoscience of "phrenology," an outdated attempt to ascertain personal traits "by measuring the shape and size of a person's skull."[55] Technologies that claim to perform these tasks are grounded in racism,[56] sexism, homophobia, and transphobia[57]—there is no legitimate basis for their use.

B. Human analysis procedures could begin to regulate how human operators use facial recognition tools, but they cannot fully anticipate the ways such tools and their results might be misused.

Facial recognition systems are not purely "technical" in their construction or their application. Rather, facial recognition systems are "socio-technical"—their development and use rely on the complex interaction between human actors and computers. Any procedures for human analysis must recognize this. Officers or analysts using the facial recognition tools are part and parcel of the system. Even if a facial recognition tool has an advertised accuracy rate or record of performance, the choices that human analysts make with that tool will impact its performance, with a high likelihood of negative consequences. Given the novelty of facial recognition for ordinary policing purposes, we lack confidence that any set of procedures could safeguard against the harms of facial recognition. At a minimum, the OAG would have to consider instituting the following procedural protections:

1) Before initiating a facial recognition search, officers must obtain a warrant: Like many electronic searches, facial recognition queries should require that an officer obtain a

[55] Joshua A. Kroll, *ACM Tech Brief: Facial Recognition*, ACM Technology Policy Council (February 2022), https://dl.acm.org/doi/pdf/10.1145/3520137.

[56] Gender recognition, for example, can fail spectacularly for women of color: major commercial gender classification systems have seen error states as high as 35% for darker-skinned women (compared to less than 1% error for lighter-skinned men). Buolamwini & Gebru, *supra* note 2; *see also* Lauren Rhue, *Emotion-Reading Tech Fails the Racial Bias Test*, The Conversation (Jan. 3, 2019), https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404 (explaining that emotion recognition tools show racial bias, as they are more prone to evaluate Black faces as angrier than white faces).

[57] The very enterprise of gender classification is questionable, as it assumes a binary gender classification and routinely misgenders transgender and nonbinary people. *See* Morgan Klaus Scheuerman, Jacob M. Paul & Jed R. Brubaker, *How Computers See Gender: An Evaluation of Gender Classification in Commercial Face Analysis and Image Labeling Services*, 3 Proc. ACM Human-Computer Interaction 144 (2019), https://dl.acm.org/doi/pdf/10.1145/3359246.

warrant or court order before using the tool.[58] That court order or warrant must only issue after a finding that there is probable cause that the subject of the facial recognition search committed an enumerated offense.[59]

2) Human analysts must not alter photos: As explained in our above comment, officers frequently come up with "creative" and abusive ways to use facial recognition tools, such as by editing images before they feed them into the tool, feeding in images of people they consider look-a-likes to the subject, or feeding in police sketches. These kinds of abuses of the tool are unacceptable and render the tool's results invalid. Any reliance on those results is misplaced, and likely to result in harmful impacts on the wrong suspects. Although rules could be instituted to admonish law enforcement officers if they edit photos, we doubt that the OAG could effectively anticipate and prohibit all of the possible misuses of facial recognition tools.

3) Human analysts must follow best practices in eyewitness identification when evaluating facial recognition results: Facial recognition tools require human analysts to identify the unknown person from a list of proposed candidates. Many of the problems that exist with eyewitness identification in general—which the N.J. Supreme Court has found troublesome before[60]— persist with facial recognition tools.

The Attorney General's guidelines for eyewitness identification must, at a minimum, be carried forward to the use of facial recognition,[61] including:

1) When choosing whether to include a candidate in a final candidate list, two analysts must "independently conclude that the same photo is a possible match."[62]
2) If candidate images are presented to a witness, the officer administering the array must be different than the officers involved in the investigation.
3) To combat automation bias and other forms of suggestion, witnesses or any other individuals considering the candidate list should never be notified that a facial recognition system identified a suspect in the investigation or that it contributed photos to the candidate list. They must especially not be shown each candidate's similarity score.

---

[58] Mass. Gen. Laws c. 6 § 220(b) ("A law enforcement agency may perform such a facial recognition search for the following purposes . . . to execute an order, issued by a court or justice authorized to issue warrants in criminal cases . . .")

[59] 25 M.R.S. § 6001, *supra* note 45 (requiring "probable cause to believe that an unidentified individual in an image has committed [a] serious crime").

[60] *See Henderson*, 208 N.J. at 283 (holding that much of the scientific evidence on the problems with eyewitness testimony, including mugshot exposure bias, contaminating effects of extrinsic information, and the influence of identification procedures, are reliable, useful, and legally significant).

[61] *Attorney General Guidelines for Preparing and Conducting Out-of-Court Eyewitness Identifications* (rev. 2021), https://www.nj.gov/lps/dcj/agguide/Photo-Lineup-ID-Guidelines.pdf.

[62] Garvie, *supra* note 9.

Finally, and perhaps most importantly, the entire analysis procedure must be recorded. Any positive identifications or nonidentifications must be included in all records. The record must be provided in its entirety to any future defendants during discovery.

4) **If using the candidate list for investigative leads, the candidates must be sufficiently corroborated:** Given the errors inherent in facial recognition tools and the breadth of candidates such tools can generate, the use of candidate lists as investigative leads must be limited. A person's presence on a candidate list *alone* cannot be a reason to initiate more intrusive investigations. There must be corroborative evidence, in the form of a positive identification via a photo array, a concrete nexus between the suspect and the crime (beyond merely the photo identification), or some other piece of information.[63]

C. Technical measures to track the accuracy and performance of facial recognition would be required by any sound policy on facial recognition, but are ultimately insufficient to address the impact facial recognition has on racial disparities in policing and civil liberties.

We encourage the OAG to continue to look towards the National Institute of Standards and Technology's Face Recognition Vendor Test for guidance on facial recognition. However, technical metrics will never be sufficient to ensure that facial recognition serves the public without hurting our communities.

The OAG must expect that false positives will be inevitable if it allows the use of facial recognition. The prohibitions, principles, and procedures we consider above would go part of the way in protecting individuals from erroneous facial recognition matches. But as advocates for civil rights and liberties, we are not technologists and therefore are not in a position to prescribe what the most acceptable "false positive rate" is for individual facial recognition tools. How a tool's "false positive rate" might impact the actual performance of law enforcement's facial recognition process can only be determined through empirical study of facial recognition used "in the wild" by law enforcement. The ultimate impact of facial recognition on racial bias in policing or civil liberties cannot be measured through the tool alone.

This also illustrates the importance of transparency by public agencies using facial recognition technology and the technology's vendors. If public agencies use facial recognition, independent external auditors would have to be able to evaluate its performance in practice. Agencies must demand that their facial recognition vendors make any machine learning models, training data, software, internal studies, or other data or information available for public inspection. Trade secrecy must not be a shield against public accountability.[64]

---

[63] *See id.*

[64] *See, e.g.*, Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 Stanford L. Rev. 1243 (2018), https://review.law.stanford.edu/wp-

content/uploads/sites/3/2018/06/70-Stan.-L.-Rev.-1343.pdf (arguing that the use of "trade secret evidence" in criminal cases harms defendants).