June 3, 2021

Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology

Across the country, local, state, and federal law enforcement and immigration agencies use face recognition systems to identify, track, and target individuals. More than half of all U.S. adults are already in face recognition databases used for criminal investigations.[1] This technology dramatically expands law enforcement's power and poses severe threats to everyone's safety, wellbeing, and freedoms of expression and association—but especially for Black and Brown communities, Muslim communities, immigrant communities, Indigenous communities, and other people historically and currently marginalized and targeted by policing.

Much of the public debate has focused on the alarming inaccuracy of face recognition systems, particularly on women and people with darker skin.[2] In at least three cases that are publicly known, police have relied on erroneous face recognition identifications to make wrongful arrests of Black men, underscoring the dangerous nature of this technology in the hands of law enforcement.[3]

But improvements in the technology's accuracy will not address the fundamental problem: face recognition expands the scope and power of law enforcement, an institution that has a long and documented history of racial discrimination and racial violence that continues to this day. In the context of policing, face recognition is always dangerous—no matter its accuracy. Throughout our nation's history, law enforcement has used surveillance to silence dissent and to maintain white supremacy, from slave patrols[4] to the FBI's COINTELPRO program. Face recognition and other modern surveillance technologies promise to continue a history that has shown itself to be incompatible with the freedoms and rights of Black and Brown communities.

---

[1] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Geo. L. Ctr. on Privacy & Tech. 42 (Oct. 18, 2016), *available at* https://www.perpetuallineup.org/.
[2] Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* (2018), *available at* http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Patrick Grother, Mei Ngan, Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280, Nat'l Inst. of Standards and Technology (December 2019), available at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[3] 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.
[4] Hassett-Walker, Connie, *The Racist Roots of American Policing: From Slave Patrols to Traffic Stops*, The Conversation (June 2, 2020), available at https://theconversation.com/the-racist-roots-of-american-policing-from-slave-patrols-to-traffic-stops-112816.

Given this history, it's no surprise that many law enforcement agencies have adopted face recognition technologies in secret, without the input or approval of policymakers or the public. In cases where the public has learned of an agency's use of face recognition, key details about how the system works and how it's used often remain concealed, even from criminal defendants. The details that have been uncovered to date are troubling: agencies often run searches on "flawed" face data—matches based on low confidence thresholds, artist-drawn composite sketches, and images that have been heavily edited.[5] The undersigned groups agree that law enforcement's use of face recognition is invasive and harmful to all communities, with severe and disproportionate harms for Black and Brown communities.

The most comprehensive approach to addressing the harms of face recognition would be to entirely cease its use by law enforcement. The six concerns outlined below highlight why the strongest policy action on face recognition is urgently needed.

1. Regardless of technical accuracy, law enforcement use of face recognition systems could exacerbate the harms of policing in communities that are already targeted by the police.

Much attention has been focused on the increased errors in face recognition systems on Black and Brown people.[6] But even if bias could be entirely eliminated from the technology, the use of face recognition will still disproportionately harm Black and Brown communities. This is because, as is the case with any practice or tool of policing, face recognition is more likely to be deployed on Black and Brown communities.[7] As a consequence, the individuals subject to face recognition searches that may lead to targeting by police are disproportionately likely to be of color. In addition, law enforcement's use of mugshot databases for face recognition searches means that Black and Brown people, who are disproportionately targeted for arrest and

[5] Despite the danger of such action causing errors and producing unreliable information, departments edit photos with computer generated imagery, use sketches, or even run scans on celebrity lookalikes in their face recognition systems. *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data* (May 16, 2019), https://www.flawedfacedata.com/.
Additionally, some departments permit matches with low confidence thresholds—meaning a low certainty of the matching being accurate—to be used. For example, Amazon recommended a police department configure its systems to return matches with no minimum confidence threshold even after making public statements that police setting systems to return matches below 99 percent would be irresponsible. *See*, Jake Laperruque, *About-Face: Amazon's Shifting Story on Facial Recognition Accuracy*, The Project On Government Oversight (April 10, 2019), https://www.pogo.org/analysis/2019/04/about-face-examining-amazon-shifting-story-on-facial-recognition-accuracy/

[6] Patrick Grother, Mei Ngan, Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280,* Nat'l Inst. of Standards and Technology (December 2019), *available at* https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[7] One police department found that their use of face recognition on communities of color was up to 2.5 times greater than their proportion of the population being policed. *See* Automated Regional Justice Information System, San Diego's Privacy Policy Development: Efforts & Lessons Learned, 11, *available at* https://drive.google.com/file/d/1ZR2jjiLcBMUKnHTRk1ZC248NbFUqNRww/view?us p=sharing.

incarceration, will be more likely to show up in search results.[8] In this manner, face recognition risks carrying forward historical biases and exacerbating existing biases in the way our communities are policed.

2. Law enforcement use of face recognition threatens individual and community privacy by allowing invasive and persistent tracking and targeting.

Face recognition is already a pervasive part of American policing. Law enforcement agencies routinely use the technology to compare an image from bystanders' smartphones, CCTV cameras, or other sources with face image databases maintained by local, state, and federal agencies. Potentially more than 133 million Americans are included in these databases, with at least thirty-one states giving police access to driver's license images to run or request searches, [9] and twenty-one states giving the FBI access to the same.[10] Law enforcement use of these databases for investigations places millions of Americans in what has been called a "perpetual line-up,"[11] posing particular risk to privacy and access to public space for Black and Brown people, immigrants, and other groups who are routinely targeted by police.

Face recognition, when used with persistent surveillance camera networks, further erodes anonymity in public spaces, allowing law enforcement to perpetually track the movements of nearly any person at any time. Major American cities have piloted persistent face surveillance, which continuously scans live video to identify individuals.[12] Such tracking undermines fundamental rights to association, expression, and privacy.[13] The Supreme Court's 2018 decision in *Carpenter v. United States* held that warrantless location tracking using cell site location data for more than seven days is unconstitutional.[14] Persistent face surveillance can "catalogue every single movement" of individuals in the same way, and it's arguable that such tracking would be unlawful under a *Carpenter* analysis.[15]

3. Law enforcement use of face recognition can chill First Amendment-protected activities.

---

[8] *See* Clare Garvie, Alvaro Bedoya, Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Oct. 18, 2016), note 236, https://www.perpetuallineup.org/findings/racial-bias#footnote236_b52kwrg. https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-GarvieC-20190522.pdf.

[9] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Geo. L. Ctr. on Privacy & Tech. 42 (Oct. 18, 2016), *available at* https://www.perpetuallineup.org/.

[10] *Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains,* Government Accountability Office (June 4, 2019), https://www.gao.gov/products/GAO-19-579T.

[11] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Geo. L. Ctr. on Privacy & Tech. 42 (Oct. 18, 2016), *available at* https://www.perpetuallineup.org/.

[12] Clare Garvie and Laura Moy, *America Under Watch: Face Surveillance in the United States*, (May 16, 2019), https://www.americaunderwatch.com.

[13] *See, e.g.*, *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms.")

[14] 138 S.Ct. 2206 (2018).

[15] *Id.* at 2217, quoting *Jones* at 430 (Alito, J., concurring).

Face recognition presents a serious threat to First Amendment rights. Law enforcement can use face recognition to identify people attending large protests, political events, or religious ceremonies, and catalog individuals' engagement in these First Amendment-protected activities. American history is fraught with efforts to monitor individuals based on dissent[16] or religious beliefs,[17] and face recognition could supercharge that surveillance. The mere threat of face recognition being used to catalog, interfere with, or retaliate against First Amendment-protected activities will in itself chill participation and expression in a way that is not compatible with democratic society.[18]

In 2015, Baltimore police used face recognition amid protests against the police killing of Freddie Gray to find individuals with "outstanding warrants and arrest[ed] them directly from the crowd," in order to disrupt, punish, and discourage protesters.[19] Police in cities including Washington, D.C.,[20] New York City,[21] and Miami[22] also used face recognition to identify protestors during the uprising against anti-Black racism and police violence in 2020. In addition to broad surveillance, face recognition can be too easily warped into a tool for selective prosecution. The ability to pull up face recognition matches for individuals with an active bench warrant for a low-level offense has already been abused to target those exercising their First Amendment rights. In most jurisdictions law enforcement agencies do not even need evidence of a crime committed in order to run a face recognition search. This broad-based face surveillance chills civic engagement and promotes self-censorship. While this threat is significant for existing face recognition technologies, it's even more significant for emerging forms of persistent face surveillance.

4. Law enforcement use of face recognition can easily violate due process rights and otherwise infringe upon procedural justice.

---

[16] Senate Select Committee, Book III: Supplementary Detailed Staff Reports, 94th Cong., 2d sess., 1976, S. Rep. 94–755.

[17] *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, The Muslim American Civil Liberties Coalition & The Creating Law Enforcement Accountability & Responsibility (CLEAR) Project at CUNY School of Law (2013), https://www.law.cuny.edu/wp-content/uploads/page-assets/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

[18] Ryan Calo, The Boundaries of Privacy Harm (July 16, 2010) at 16-17. Indiana Law Journal, Vol. 86, No. 3, 2011, *available at* https://ssrn.com/abstract=1641487.

[19] Kevin Rector & Alison Knezevich, *Social Media Companies Rescind Access to Geofeedia, Which Fed Information to Police During 2015 Unrest,* Balt. Sun (Oct. 11, 2016), https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html.

[20] Justin Jouvenal & Spencer S. Hsu, *Facial Recognition Used To Identify Lafayette Square Protestor Accused of Assault,* Wash. Post (Nov. 2, 2020), https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4_story.html.

[21] James Vincent, *NYPD Used Facial Recognition to Track Down Black Lives Matter Activist*, The Verge (Aug. 18, 2020), https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram.

[22] Kate Cox, *Cops in Miami, NYC Arrest Protestors From Facial Recognition Matches,* Ars Technica (Aug. 19, 2020), https://arstechnica.com/tech-policy/2020/08/cops-in-miami-nyc-arrest-protesters-from-facial-recognition-matches/.

New technologies, including face recognition systems, often allow law enforcement to circumvent existing legal protections for individuals. Due process requirements govern law enforcement actions throughout the criminal legal process, including stop-and-frisks, investigations, searches, arrests, and beyond. Yet, in the twenty years that face recognition has been used in some jurisdictions, defendants' rights to due process protections have been essentially non-existent when it comes to the technology.[23] And because prosecutors and law enforcement often conceal the use of face recognition in criminal trials, it may be difficult, if not impossible to ensure that defendants are able to exercise their Sixth Amendment rights.[24]

The ability to assess the reliability of both the face recognition systems and the ways in which they are used is critical to ensuring due process of law. Protecting due process rights and preserving *Brady*[25] rights would require that law enforcement agencies disclose key details about the design and use of the system that impact the reliability of matches. This includes information about the make and model of the particular system used; the training data and inner workings of that system; and where, when, and how humans make decisions when using the system. Face recognition searches require a number of human decisions, each necessarily bringing in the discretion and subjectivity of the user. Depending on the choices made by the agent using the face recognition system at a number of steps throughout the process, the results of the face recognition system could vary greatly, producing different matches, and different potential evidence.[26] The person making these decisions is also likely the person who will assess matches generated by the system and make the ultimate decision of which is the "match." Because the decisions involved in running face recognition searches can have a profound impact on the process and outcome for those arrested, disclosure of information about each of these steps is important to ensuring the defendant is afforded due process.[27]

Additionally, the right "to be confronted with the witnesses against him" found in the Sixth Amendment of the Constitution is a critical feature of a fair trial. Defendants have the right to cross examine the people involved in creating reports and witnesses who provide identification, and to investigate the tools and tests that provided evidence. Any evidence that is considered "testimonial" in a case should be subject to examination in order to uphold those rights. Face

---

[23] Jennifer Valentino-DeVries, *How The Police Use Facial Recognition, And Where It Falls Short,* N.Y. Times (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

[24] Karen Gullo & Jennifer Lynch, *When Facial Recognition Is Used to Identify Defendants, They Have a Right to Obtain Information About the Algorithms Used on Them, EFF Tells Court*, EFF.org (March 12, 2019), https://www.eff.org/deeplinks/2019/03/when-facial-recognition-used-identify-defendants-they-have-right-obtain.

[25] *Brady v. Maryland*, 373 U.S. 83 (1963). "The *Brady* Rule," or "*Brady* rights," as they are commonly known, require that prosecutors disclose materially exculpatory evidence in the government's possession to the defense.

[26] A face recognition system that leads to arrest, or any investigative or police action, could be impacted and made more or less reliable by a number of factors, including the confidence thresholds used and the dataset of photos used to train the system, and the photo provided to conduct the search. For example, the person running the search can manipulate the photo to make it more accessible to the technology by taking actions such as pasting in eyes, or even substituting an image of a famous actor, as some have done. *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data* (May 16, 2019), https://www.flawedfacedata.com/.

[27] That disclosure should therefore also include information regarding what other matches the system returned.

recognition is increasingly used to identify the accused,[28] meaning that each step in the design and use of the technology must be disclosed in detail to defendants, who then have the right to challenge those procedures and algorithms in court. Complicating these issues, companies often make intellectual property claims to trade secrets to protect their algorithms and prevent their inner workings from coming to light, impeding defendants' rights to confront evidence in court.[29]

[28] 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; Jennifer Valentino-DeVries, How The Police Use Facial Recognition, And Where It Falls Short, N.Y. Times (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

[29] *See, e.g., Wisconsin v. Loomis*, 371 Wis.2d 235, 243 (Wisc. 2016).

5. Face recognition systems used by law enforcement often rely on faceprints that have been obtained without consent.

Developers of face recognition systems often use faceprints obtained without consent and in violation of public trust.[30] A prominent example is Clearview AI, which created a face recognition tool used by over 600 federal, state, and local law enforcement agencies and private companies across the country.[31] To build its data set for matching faceprints, Clearview amassed over 3 billion faceprints by scraping photos from across the Internet, including employment sites, news sites, and social media networks such as Facebook, unbeknownst to the subjects of these images.[32] While the well-known Clearview database is used for running searches, databases used to train face recognition models also often rely on faceprints obtained or used for this purpose without consent. For instance, IBM captured faceprints by annotating user-uploaded images from the photo sharing site Flickr with details like skin tone and facial geometry.[33] Additionally, in January 2021, the Federal Trade Commission settled with photo storage app Everalbum over its misuse of user photos for face recognition purposes, requiring Everalbum to delete face recognition models developed using user photos and videos.[34]

In order to run face recognition searches, law enforcement relies on various sources including driver's license photos and mugshots. The faceprints used to identify possible matches have been collected without consent for that purpose. Many states will run searches against their driver's license photo databases for the FBI.[35] Additionally, states can submit images to the FBI to run against its own face recognition database, which includes mugshots submitted by federal, state, and local agencies. State and local law enforcement agencies also maintain and run searches against their own databases of driver's license and mugshot images from their own jurisdiction, as well as other jurisdictions and even other countries. For example, the Maricopa County Sheriff's Office in Arizona included mugshots from Honduras in its face recognition match database.[36]

Using people's faceprints outside of their original purposes and without their knowledge is an invasion of privacy and violates public trust.

---

[30] Inioluwa Deborah Raji and Genevieve Fried, *About Face: A Survey of Facial Recognition Evaluation*, AAAI 2020 Workshop on AI Evaluation (Feb. 1, 2021), https://arxiv.org/abs/2102.00813.
[31] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[32] *Id.*
[33] Olivia Solon, *Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent*, NBC News (March 12, 2019), https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921.
[34] Federal Trade Commission https://www.ftc.gov/system/files/documents/cases/everalbum_complaint.pdf JD Supra (January 20, 2021), https://www.jdsupra.com/legalnews/alert-ftc-requires-app-developer-to-6691322/.
[35] *Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains*, Government Accountability Office (June 4, 2019), https://www.gao.gov/products/gao-19-579t.
[36] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Geo. L. Ctr. on Privacy & Tech. 42 (Oct. 18, 2016), *available at* https://www.perpetuallineup.org/.

6. In addition to racial bias in how law enforcement uses face recognition, the technology itself poses disproportionate risks of misidentification for Black, Asian, and Indigenous people.

Studies of face recognition algorithms have documented the fact that commercial algorithms available for purchase and used by government entities around the country have inequitable error rates across a number of demographics including race, sex, and age.[37] The National Institute of Standards and Technology's Face Recognition Vendor Test found significant variation in both false positive and false negative error rates[38] across race, sex, and age with the highest false positives for U.S. law enforcement mugshots among Black, Asian, and Indigenous people.[39] In a comparison of match rates by country of origin, photos of people from East African countries had false positive rates 100 times higher than the baseline rate.[40]

CONCLUSION

The evidence that face recognition technology impedes our rights has never been more clear. Even major technology companies have acknowledged the harms of law enforcement use of face recognition. In June 2020, as institutions across the country faced a reckoning over racial equity, IBM, Microsoft, and Amazon announced that they would be halting the sales of their face recognition technology to law enforcement. Now is the moment for national policymakers to address law enforcement use of this technology.

A ban or moratorium on law enforcement use of face recognition is the most effective way to address all of the concerns outlined in this statement. With Congress slow to act, a number of states and localities have taken action. Over a dozen cities across the country have banned face recognition, and multiple states have placed restrictions on its use.[41] Accordingly, it is essential that any federal laws that seek to regulate face recognition do not preempt state and local bans. Given the concerns outlined above, one thing is clear: policymakers must act to protect the public from this dangerous technology now.

---

[37] *See, e.g.,* Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* (2018), *available at* http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[38] A false positive occurs when a person is incorrectly matched to a photo in the database when it is not actually them. A false negative occurs when the system incorrectly fails to match a person to their photo in the database.

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

[40] *Id.* at 40.

[41] Clare Garvie & Jameson Spivack, *A Taxonomy of Legislative Approaches to Face Recognition in the United States* (Sept. 2, 2020), *available at* https://ainowinstitute.org/regulatingbiometrics-spivack-garvie.pdf.

Signatories:

Access Now
Action Center on Race and the Economy
American Civil Liberties Union
Amnesty International USA
Asian Americans Advancing Justice – AAJC
Athena
Brennan Center for Justice
Center for Democracy & Technology
Center on Privacy & Technology at Georgetown Law
Center on Race, Inequality, and the Law at NYU Law
Color of Change
Defending Rights & Dissent
Demand Progress Education Fund
Demos
Electronic Frontier Foundation (EFF)
Electronic Privacy Information Center (EPIC)
Fight for the Future
Free Press
Government Information Watch
Innocence Project
Just Futures Law
Lawyers' Committee for Civil Rights Under Law
Leadership Conference on Civil and Human Rights
Legal Aid Society of New York City
Media Alliance
MediaJustice
Mijente
NAACP Legal Defense and Education Fund, Inc.
National Association of Criminal Defense Lawyers
National Coalition Against Censorship
National Hispanic Media Coalition
New America's Open Technology Institute
Oakland Privacy
OCA – Asian Pacific American Advocates
Open MIC (Open Media and Information Companies Initiative)
Project on Government Oversight
Public Citizen
Restore The Fourth
S.T.O.P. – The Surveillance Technology Oversight Project
Upturn
X-Lab