LDF Legal Defense Fund

Advancing racial justice since1940

January 19, 2024

The Honorable Merrick Garland
Attorney General of the United States
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530

The Honorable Alejandro Mayorkas
Secretary of Homeland Security
Washington, DC 20528

Dear Attorney General Garland and Secretary Mayorkas:

Founded by Thurgood Marshall in 1940, the NAACP Legal Defense and Educational Fund, Inc. (LDF) is the nation's oldest civil rights law organization. LDF was launched at a time when America's aspirations for equality and due process of law were stifled by widespread state-sponsored racial inequality. Since its founding, LDF has relied on the Constitution and federal and state civil rights laws to pursue equality and justice for Black Americans and other marginalized communities. LDF's mission has always been transformative: to achieve racial justice, equality, and an inclusive society. As part of that work, LDF has forged longstanding partnerships with impacted communities, organizers, researchers, and attorneys to challenge and reform unlawful and discriminatory policing practices across the country, including law enforcement's use of technology and algorithmic systems in a racially discriminatory manner. These technologies, coupled with their use by law enforcement agencies, directly threaten the lives, liberty, rights, and dignity of Black people and other marginalized communities.

We submit the following comments in response to the request from the Department of Justice (DOJ) and the Department of Homeland Security (DHS) for public input regarding law enforcement agencies' use of facial recognition technology; fingerprint and iris biometric technologies; DNA biometric technologies, including familial searching, probabilistic genotyping software, and predictive phenotyping; and person-based predictive policing algorithms (collectively, "advanced technologies"). These comments focus on law enforcement's use of facial recognition and predictive algorithms.

I. Law Enforcement's Use of Advanced Technologies Is Likely to Exacerbate Existing Racial Biases in the Criminal Legal System.

While advanced technologies[1] are promoted within and outside of law enforcement agencies as increasing efficiency in policing and reducing crime in communities, these technologies both exacerbate and replicate racial bias and discrimination by law enforcement. To better understand concerns regarding law enforcement's use of advanced technologies, it is necessary to examine how pre-existing racial bias and discrimination in law enforcement practices result in the hyper-surveillance, disproportionate criminalization, and mass incarceration of Black people and other marginalized communities through these technologies.

[1] We include references to gunshot detection systems in these comments in addition to the technologies covered in 13(e) because it is an algorithmic, automated technology (while more rudimentary than those powered by artificial intelligence) about which more information has become publicly available. The impacts of gunshot detection systems are illustrative of the impacts that should be expected by law enforcement's use of the technologies covered in 13(e) given similar data sources.

40 Rector Street
5th Floor
New York, NY 10006

700 14th Street NW
Suite 600
Washington, DC 20005

260 Peachtree Street NW
Suite 2300
Atlanta, GA 30303

naacpldf.org
212-965-2200

Modern day law enforcement agencies in America disproportionately enforce laws, with the threat and use of violence, against Black people and other marginalized communities. Across a spectrum of law enforcement activities, racial disparities are ever present in pedestrian stops,[2] traffic stops, searches,[3] and arrests.[4] For example, literature regarding racial disparities in traffic stops establishes that: Black men are most at risk of traffic stops and once stopped, they are most at risk of search, even though the "hit rate" (probability of finding contraband) is lowest for this group.[5] Evidence suggests that Black drivers are on average 2–3x more likely to be stopped than white drivers.[6]

Currently popular strategies such as "hot spot policing" also perpetuate aggressive and disparate policing in Black communities with severe consequences. Hot spot policing focuses law enforcement presence, surveillance, and enforcement activity on targeted communities and can employ advanced technologies, including gunshot detection systems, to identify "hot spots" that lead to increased encounters between residents in those communities and police.[7] Communities targeted as "hot spots" are frequently under-resourced and comprised disparately of Black people due to historic residential segregation and continuing disparate investments.[8]

Gunshot detection systems are often used alongside the technologies at issue in this review. Their deployment in predominantly Black and Brown communities illustrates how increased police encounters from their usage contribute to racially biased policing.[9] An analysis of the Chicago Police Department's use of SoundThinking (formerly known as "ShotSpotter")

---

[2] A 2021 study of the New York City Police Department's stop-and-frisk program found that Black and Latinx people stopped by police were more likely to be frisked and subjected to non-weapon force than white people. Philip J. Levchak, *Stop-and-Frisk in New York City: Estimating Racial Disparities in Post-Stop Outcomes*, J. Crim. Just., Mar.–Apr. 2021, at 1, https://www.sciencedirect.com/science/article/abs/pii/S0047235221000040.

[3] A large-scale analysis of 100 million traffic stops carried out by 21 state patrol agencies and 35 municipal police departments over about a decade found evidence of racial bias in police searches. Emma Pierson et al., *A Large-Scale Analysis of Racial Disparities in Police Stops Across the United States*, 4 Nature Hum. Behav. 732 (2020), https://www.nature.com/articles/s41562-020-0858-1.

[4] A meta-study found that the single most common factor included in analysis of police decision-making was civilian race or ethnicity. Meta-analysis of 4,500 sources/studies shows that minority suspects are more likely to be arrested than white suspects by 32-52%, or six percentage points higher than non-minority populations. *See* Yinthe Feys, *Worldwide Views on Police Discretion: A Scoping Review Regarding Police Decision-Making* (2023); Tammy Rinehart Kochel et al., *Effect of Suspect Race on Officers' Arrest Decisions*, 49 Criminology 473 (2011).

[5] These results have been replicated across inter-state panels from 4 to 21 states, and across jurisdictions from small town to city and state levels. *See generally*, Frank R. Baumgartner et al., *Racial Disparities in Traffic Stop Outcomes*, 9 Duke F.L. & Soc. Change 21 (2017); Pierson et al., *supra* note 3; Kevin Roach et al., *At the Intersection: Race, Gender, and Discretion in Police Traffic Stop Outcomes*, 7 J. Race Ethnicity & Pol. 239 (2022); *see also* Derek A. Epp & Macey Erhardt, *The Use and Effectiveness of Investigative Police Stops*, 9 Pol. Grps. & Identities 1016 (2021); Kelsey Shoub et al., *Race, Place, and Context: The Persistence of Race Effects in Traffic Stop Outcomes in the Face of Situational, Demographic, and Political Controls*, 5 J. Race Ethnicity & Pol. 481 (2020).

[6] Shoub et al., *supra* note 5, at 3.

[7] *See* DOJ grant to East Palo Alto for gunshot detection system to identify "two to four shooting hot spots. . . ." *The ShotSpotter Gunshot Detection System and Hot Spots Analyses*, Bureau of Just. Assistance (Aug. 6, 2012), https://bja.ojp.gov/funding/awards/2012-db-bx-0001.

[8] *See* Margery Austin Turner & Solomon Greene, *Causes and Consequences of Separate and Unequal Neighborhoods*, Urb. Inst., https://www.urban.org/racial-equity-analytics-lab/structural-racism-explainer-collection/causes-and-consequences-separate-and-unequal-neighborhoods (last visited Jan. 14, 2024) ("America's history of residential segregation has produced a system of neighborhoods that are not only separate but structurally unequal," and these communities are subject to "hot spot" policing); *see also* Robin Smyton, *How Racial Segregation and Policing Intersect in America*, Tufts Now (June 17, 2020), https://now.tufts.edu/2020/06/17/how-racial-segregation-and-policing-intersect-america.

[9] *See* MacArthur Just. Ctr., *ShotSpotter Creates Thousands of Unfounded Police Deployments, Fuels Unconstitutional Stop-and-Frisk, and Can Lead to False Arrests*, End Police Surveillance, https://endpolicesurveillance.com (last visited Jan. 14, 2024).

40 Rector Street
5th Floor
New York, NY 10006

700 14th Street NW
Suite 600
Washington, DC 20005

260 Peachtree Street NW
Suite 2300
Atlanta, GA 30303

naacpldf.org
212-965-2200

revealed that 86% of the police dispatches from the technology are not associated with any criminal activity, and only 9.1% of these responses identified a gun-related criminal offense.[10] Moreover, officers with the Chicago Police Department have been involved in changing ShotSpotter data after an incident.[11]

The consequences of increased interactions with law enforcement can be severe given how Black people are subjected to racially disparate threats and uses of violence,[12] police killings,[13] and other adverse outcomes in health,[14] education, economic status, and civic engagement.[15] The use by law enforcement of advanced technologies that are invasive and faulty encodes bias and threatens to amplify and exacerbate systemic racism in policing for Black and other marginalized communities.

II. Advanced Technologies Used by Law Enforcement Are Often Inaccurate and Ineffective, Perpetuate Racial Bias, and Do Not Promote Public Safety.

A. Evidence Shows Facial Recognition Systems Perpetuate Racial Bias, and Their Use by Law Enforcement Results in Discriminatory Policing.

1. Facial Recognition Systems Are Error-Prone.

Facial recognition systems are inaccurate, and these errors exacerbate racial biases in policing. The technology is error-prone for people with darker skin and for features associated with Black people, Asian people, women, and transgender or nonbinary people.[16] A report by the

---

[10] *Id.*; Hannah Cheves, *ShotSpotter Is a Failure. What's Next?*, MacArthur Just. Ctr. (May 5, 2022), https://www.macarthurjustice.org/blog2/shotspotter-is-a-failure-whats-next/; Joseph M. Ferguson & Deborah Witzburg, City of Chi. Off. of Inspector Gen., *The Chicago Police Department's Use of ShotSpotter Technology* (2021), https://igchicago.org/wp-content/uploads/2021/08/Chicago-Police-Departments-Use-of-ShotSpotter-Technology.pdf; Press Release, SoundThinking, Shotspotter Changes Corporate Name to SoundThinking and Launches Safetysmart Platform for Safer Neighborhoods (Apr. 10, 2023), https://www.soundthinking.com/press-releases/shotspotter-changes-corporate-name-to-soundthinking-and-launches-safetysmart-platform-for-safer-neighborhoods/.

[11] *See* Todd Feathers, *Police Are Telling ShotSpotter to Alter Evidence from Gunshot-Detecting AI*, VICE (July 26, 2021), https://www.vice.com/en/article/qj8xbq/police-are-telling-shotspotter-to-alter-evidence-from-gunshot-detecting-ai.

[12] Even while controlling for arrest demographics, participating departments revealed racial disparities across multiple levels of force severity. *See* Phillip Atiba Goff et al., Ctr. for Policing Equity, *The Science of Justice: Race, Arrests, and Police Use of Force* (2016), https://policingequity.org/images/pdfs-doc/CPE_SoJ_Race-Arrests-UoF_2016-07-08-1130.pdf.

[13] Police kill more than 300 black Americans—at least a quarter of them unarmed—each year in the United States. *See* Jacob Bor et al., *Police Killings and Their Spillover Effects on the Mental Health of Black Americans: A Population-based, Quasi-Experimental Study*, 392 Lancet 302 (2018).

[14] A 2020 study of adolescents, using data from the Fragile Families and Child Wellbeing Study, found that personal and vicarious police contact was positively associated with depressive symptoms. Additionally, more intrusive police contact (e.g., frisks and searches) was positively associated with depressive symptoms. Lastly, the researchers found that the association between police contact and depressive symptoms was concentrated among girls participants and Black participants. Kristin Turney, *Depressive Symptoms Among Adolescents Exposed to Personal and Vicarious Police Contact*, 11 Am. Socio. Ass'n 91 (2020), https://journals.sagepub.com/doi/10.1177/2156869320923095.

[15] Aaron Stagoff-Belfort, Daniel Bodah & Daniela Gilbert, Vera Inst. of Just., *The Social Costs of Policing* (2022), https://www.vera.org/downloads/publications/the-social-costs-of-policing.pdf (discussing consequences of policing on health, education, economic well-being and civil and social engagement).

[16] Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, WIRED (July 22, 2019), https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/; Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018),

40 Rector Street
5th Floor
New York, NY 10006

700 14th Street NW
Suite 600
Washington, DC 20005

260 Peachtree Street NW
Suite 2300
Atlanta, GA 30303

naacpldf.org
212-965-2200

National Institute of Standards and Technology found that Black and Asian people may be between ten and up to one hundred times more likely to be misidentified by facial recognition systems than white men, depending on the algorithm used.[17] Additionally, for one-to-many matching,[18] the research team saw higher rates of false positives for Black women.[19] As noted by the team, "differentials in false positives in one-to-many matching are particularly important because the consequences could include false accusations."[20] Finally, even if the technology became accurate across demographic groups, law enforcement's use of facial recognition technologies would still worsen the disparate policing, surveillance, and criminalization of Black and Brown communities because of the systemic racial bias in policing practices discussed above.[21]

In the law enforcement context, these errors result in significant harm and can lead to false arrests, wrongful incarceration, and detrimental lifelong consequences. To date, six people are known to have been falsely accused of a crime due to law enforcement's use of facial recognition systems. All six are Black people.[22] Errors leading to additional false arrests likely exist but are difficult to ascertain because law enforcement's use of facial recognition is usually not disclosed.[23] Moreover, the vast majority of people accused of crimes agree to plea deals rather

---

https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28; Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proceedings Mach. Learning Rsch. 1 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; *Facial Recognition: Analyzing Gender and Intersectionality in Machine Learning*, Gendered Innovations, https://genderedinnovations.stanford.edu/case-studies/facial.html#tabs-2 (last visited Jan. 18, 2024).

[17] See Patrick Grother et al., Nat'l Inst. of Standards & Tech., U.S. Dep't of Com., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, Interagency Internal Report 8280 2 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf (evaluating 189 software algorithms from 99 developers on their ability to correctly identify individuals in (1) one-to-one matching and (2) one-to-many matching, two of the most common uses of facial recognition technology); see also NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software, Nat'l Inst. of Standards & Tech. (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software#:~:text=According%20to%20a%20new%20study,recognition%20algorithms%20exhibit%20demographic%20differentials.

[18] A "one-to-many" matching system is when software takes an "unknown face and compares it to a large database of known faces to determine the unknown person's identity." William Crumpler, How Accurate Are Facial Recognition Systems – and Why Does It Matter?, Ctr. for Strategic & Int'l Stud. (Apr. 14, 2020), https://www.csis.org/blogs/strategic-technologies-blog/how-accurate-are-facial-recognition-systems-and-why-does-it.

[19] Grother et al., *supra* note 17, at 63; *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, *supra* note 17.

[20] *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, *supra* note 17.

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

[22] Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, N.Y. Times (Aug. 6 2023), https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html#:~:text=Handcuffed%20in%20front%20of%20her,to%20be%20searched%20for%20evidence.

[23] Jake Laperruque, *Limiting Face Recognition Surveillance: Progress and Paths Forward*, Ctr. for Democracy & Tech. (Aug. 23, 2022), https://cdt.org/insights/limiting-face-recognition-surveillance-progress-and-paths-forward/#:~:text=Currently%20two%20states%20%E2%80%94%20Colorado%20and,recognition%20was%20used%20in%20investigations (noting only 2 states "require the government to disclose the use of face recognition to defendants before a trial").

40 Rector Street
5th Floor
New York, NY 10006

700 14th Street NW
Suite 600
Washington, DC 20005

260 Peachtree Street NW
Suite 2300
Atlanta, GA 30303

naacpldf.org
212-965-2200

than risk lengthy sentences, preventing scrutiny of officers' investigative methods leading to their arrests.[24]

Of the known cases, on January 9, 2020, Detroit Police Department (DPD) officers drove to Robert Williams's home and arrested him for a crime that he did not commit.[25] Mr. Williams's unlawful arrest and incarceration was the result of an erroneous facial recognition match, which was generated using a low-resolution probe image of an individual's face that was barely illuminated and Mr. Williams's outdated license photo.[26] As one officer aptly put it, "the computer got it wrong."[27] Mr. Williams later recounted that he "spent the night sleeping on the cold concrete floor of a filthy, overcrowded cell next to an overflowing trash can. No one came to talk to me or explain what I was accused of – or why. Meanwhile, my family spent the night at home without me, scared for me and for what my false arrest would mean for all of us."[28]

Mr. Williams, however, is not the only person in Detroit that suffered from this kind of misidentification through facial recognition. On May 15, 2019, a detective captured a still image from a victim's phone, and the facial recognition search returned Michael Oliver as an investigative lead.[29] Michael Oliver was not the person pictured in the probe image; however, on July 31, 2019, Mr. Oliver was arrested while driving to work.[30] As a result of Mr. Oliver's arrest, his car was impounded, he was forced to wait "anxiously" behind bars for two and a half days with little information about what he was accused of,[31] and he lost his job. According to Mr. Oliver, "it was like everything fell, like everything went down the drain," and it took about a year for his life to return to normal.[32]

In addition, on February 16, 2023, Porcha Woodruff, who was eight months pregnant at the time, was confronted by six DPD officers while getting her two kids ready for school.[33] Using a probe image captured from a gas station camera, a facial recognition search conducted by DPD officers identified Ms. Woodruff as a suspect of a criminal investigation.[34] When Ms. Woodruff asked the detective leading the investigation if "the victim [mentioned that] the female was 8 months pregnant?,"[35] the response was simply, "No."[36] In the holding cell, Ms. Woodruff

---

[24] *See* Lindsey Devers, Bureau of Just. Assistance, U.S. Dep't of Just., *Plea and Charge Bargaining* 3 (2011), https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/pleabargainingresearchsummary.pdf (90-95 percent of cases result in plea bargaining).
[25] Tate Ryan-Mosley, *The New Lawsuit That Shows Facial Recognition Is Officially a Civil Rights Issue*, MIT Tech. Rev. (Apr. 14, 2021), https://www.technologyreview.com/2021/04/14/1022676/robert-williams-facial-recognition-lawsuit-aclu-detroit-police/.
[26] *Id.*; Complaint at 3, Williams v. City of Detroit, No. 2:21-cv-10827-GAD-APP (E.D. Mich. Apr. 13, 2021).
[27] Complaint at 37, *supra* note 26.
[28] Robert Williams, *I Did Nothing Wrong. I Was Arrested Anyway.*, ACLU (July 15 2021), https://www.aclu.org/news/privacy-technology/i-did-nothing-wrong-i-was-arrested-anyway.
[29] 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/; Natalie O'Neill, *Faulty Facial Recognition Led to His Arrest—Now He's Suing*, VICE (Sept. 4, 2020), https://www.vice.com/en/article/bv8k8a/faulty-facial-recognition-led-to-his-arrestnow-hes-suing.
[30] O'Neill, *supra* note 29.
[31] *Id.*
[32] Johnson, *supra* note 29.
[33] Jennifer Henderson, *Black Mom Sues City of Detroit Claiming She Was Falsely Arrested While 8 Months Pregnant by Officers Using Facial Recognition Technology*, CNN (Aug. 8, 2023), https://www.cnn.com/2023/08/07/us/detroit-facial-recognition-technology-false-arrest-lawsuit/index.html.
[34] *Id.*
[35] Complaint at 11, *Woodruff v. City of Detroit*, No. 5:23-cv-11886-JEL-APP (E.D. Mich. Aug. 3, 2023), ECF No. 1.
[36] *Id.*

40 Rector Street
5th Floor
New York, NY 10006

700 14th Street NW
Suite 600
Washington, DC 20005

260 Peachtree Street NW
Suite 2300
Atlanta, GA 30303

naacpldf.org
212-965-2200

experienced contractions and spasms, had a possible panic attack, and became dehydrated.[37] She later commented that "she was embarrassed to be arrested in front of her neighbors and that her daughters were traumatized.'"[38]

Due to widely known errors of its usage, facial recognition has been prohibited in contexts with far less severe risks than those inherent in law enforcement investigations. In December 2023, the Federal Trade Commission banned Rite Aid for five years from using facial recognition for surveillance purposes.[39] From 2012 to 2020, Rite Aid had used AI-powered facial recognition to create a database of "persons of interest" believed to have previously engaged in shoplifting or other criminal activity at their stores; the database included individuals' pictures, names, and criminal background data, all without consumers' knowledge or consent.[40] This system "generated thousands of false-positive matches," disproportionately misidentifying women and Black, Latino, and Asian people as "'likely' shoplifters."[41] "Employees, acting on false positive alerts, followed customers around its stores, searched them, ordered them to leave, called the police to confront or remove customers, and publicly accused them, sometimes in front of friends or family, of shoplifting or other wrongdoing."[42] The injuries suffered by Mr. Williams, Mr. Oliver, and Ms. Woodruff demonstrate how law enforcement's use of facial recognition carries even more severe consequences than those experienced by Rite Aid's customers, and should similarly be prohibited.

2. Invasive Facial Recognition Systems Are Concentrated in Black and Other Marginalized Communities Due to Racially Biased Surveillance Patterns.

Law enforcement's use of networks of surveillance cameras results in heightened surveillance of predominantly Black and Brown communities.[43] Atlanta, nicknamed "the Black Mecca"[44] due to its large Black population, is the most surveilled city in the United States given

---

[37] Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, *supra* note 22.
[38] *Id.*
[39] Press Release, FTC, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without.
[40] *Id.*
[41] *Id.*; Johana Bhuiyan & agencies, *Rite Aid Facial Recognition Misidentified Black, Latino and Asian People As 'Likely' Shoplifters*, *Guardian* (Dec. 20, 2023), https://www.theguardian.com/technology/2023/dec/20/rite-aid-shoplifting-facial-recognition-ftc-settlement#:~:text=The%20FTC%20said%20in%20a,shoplifting%20or%20other%20criminal%20behavior%E2%80%9D.
[42] Press Release, FTC, *supra* note 39.
[43] *See* Patrick Toomey & Ashley Gorski, *The Privacy Lesson of 9/11: Mass Surveillance Is Not the Way Forward*, ACLU (Sept. 7, 2021), https://www.aclu.org/news/national-security/the-privacy-lesson-of-9-11-mass-surveillance-is-not-the-way-forward; *see What's Wrong with Public Video Surveillance?*, ACLU (Feb. 25, 2002), https://www.aclu.org/other/whats-wrong-public-video-surveillance; *see also* Denise Lavoie, *Court Finds Baltimore Aerial Surveillance Unconstitutional*, AP (June 24, 2021), https://apnews.com/article/baltimore-courts-503b2eb629abf94c25edf4111baf64bd; Faine Greenwood, *How to Regulate Police Use of Drones*, Brookings Inst. (Sept. 24, 2020), https://www.brookings.edu/techstream/how-to-regulate-police-use-of-drones/ (describing law enforcement's use of drones to spy on alleged drug deals and homeless encampments, and to arrest three Black Lives Matter protesters).
[44] Teresa Wiltz, *How Atlanta Became a City I Barely Recognize*, POLITICO (Sept. 16, 2022), https://www.politico.com/news/magazine/2022/09/16/atlanta-black-mecca-inequality-00055390 ("Atlanta is, in many ways, the 'Black Mecca[.]'").

40 Rector Street
5th Floor
New York, NY 10006

700 14th Street NW
Suite 600
Washington, DC 20005

260 Peachtree Street NW
Suite 2300
Atlanta, GA 30303

naacpldf.org
212-965-2200

the number of surveillance cameras it contains per capita.[45] Similarly, despite the size of New York City's five boroughs, the New York City Police Department's surveillance cameras are concentrated in the neighborhood of East New York, Brooklyn, where more than 90 percent of residents are not white.[46] Networked surveillance cameras are sometimes coupled with facial recognition software; together, they allow law enforcement agencies to surveil and track entire communities.

After capturing images from a surveillance camera, police may run a captured image against any number of databases—both public and private—using a facial recognition algorithm to identify the person(s) on the surveillance cameras. This commonly includes Department of Motor Vehicles databases and databases of jail booking photos.[47] Surveillance cameras coupled with facial recognition technology are also employed by federal law enforcement agencies, including the U.S. Immigration and Customs Enforcement (ICE), U.S Customs and Border Protection (CBP),[48] and the Federal Bureau of Investigation (FBI).[49] It is estimated that almost half of American adults—over 117 million people, as of 2016—have photos within a facial recognition network used by law enforcement.[50] The use of surveillance cameras, facial recognition software, and databases containing driver's license and state identification photos exposes millions of people to a "perpetual line-up."[51]

The use of one's photo in these perpetual line-ups often occurs without the consent, or even awareness, of the individuals pictured, creating additional privacy implications.[52] At least one facial recognition technology company, Clearview AI, has contracted with law enforcement agencies across the country and mines public platforms and/or photo databases, such as social

---

[45] Jurgita Lapienytė, *This Is the Most Heavily Surveilled City in the US: 50 CCTV Cameras Per 1,000 Citizens*, Cybernews (Sept. 28, 2021), https://cybernews.com/editorial/this-is-the-most-heavily-surveilled-city-in-the-us-50-cctv-cameras-per-1000-citizens/ ("Atlanta is the most surveilled city with a ratio of 48.93 cameras per 1,000 people.").

[46] Sidney Fussell, *The All-Seeing Eyes of New York's 15,000 Surveillance Cameras*, WIRED (June 3, 2021), https://www.wired.com/story/all-seeing-eyes-new-york-15000-surveillance-cameras/#:~:text=NYC's%20most%20surveilled%20neighborhood%20is,nonwhite%2C%20according%20to%20city%20data.

[47] Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, Wash. Post (July 17, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/; *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/.

[48] *See id.*; Johana Bhuiyan, *A US Surveillance Program Tracks Nearly 200,000 Immigrants. What Happens to Their Data?,* Guardian (Mar. 14, 2022), https://www.theguardian.com/us-news/2022/mar/14/us-immigration-surveillance-isap.

[49] Neema Singh Guliani, *The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database*, ACLU (June 7, 2019), https://www.aclu.org/news/privacy-technology/fbi-has-access-over-640-million-photos-us-through; Jay Stanley & Nicola Morrow, *ACLU Seeks Information on Government's Aerial Surveillance of Protesters,* ACLU (Aug. 4, 2020), https://www.aclu.org/news/national-security/aclu-seeks-information-on-governments-aerial-surveillance-of-protesters ("The government is using a deeply invasive, coordinated aerial surveillance campaign to monitor Black Lives Matter protests, gather information, and surveil people exercising their First Amendment rights.").

[50] Alex Najibi, *Racial Discrimination in Face Recognition Technology*, Sci. in the News (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

[51] Clare Garvie et al., *The Perpetual Line-Up*, Geo. Law Ctr. on Priv. & Tech. (Oct. 18, 2016), https://www.perpetuallineup.org/. There is also a high concentration of Black and Brown people in police-created gang databases. For example, the NYPD maintains a database of 42,000 "gang affiliates"—99 percent Black and Latinx—with no requirements to prove suspected gang affiliation. In fact, certain police departments use gang member identification as a productivity measure, incentivizing false reports. Najibi, *supra* note 50.

[52] *See* 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.

40 Rector Street
5th Floor
New York, NY 10006

700 14th Street NW
Suite 600
Washington, DC 20005

260 Peachtree Street NW
Suite 2300
Atlanta, GA 30303

naacpldf.org
212-965-2200

media platforms and security footage, for the datasets supporting its technology—all without the captured person's knowledge or consent.[53] In fact, a person's face could be used to create and train a facial recognition algorithm without that person having ever uploaded a photo or consented to its use.[54] When facial recognition technology is shared with law enforcement agencies, police may run hundreds of thousands of searches for an identification, using any photo, against a broad range of available databases, without those in the database ever being informed of law enforcements' access to these photos or use of such searches.[55] If the technology identifies a match, their identifying biometric information is then available for use across multiple law enforcement agencies at the push of a button.[56]

Amnesty International's Ban the Scan project found that "New Yorkers living in areas at greater risk of racist stop-and-frisk policing are likely to be more exposed to invasive facial recognition technology."[57] In the Bronx, Brooklyn, and Queens, the concentration of facial recognition compatible CCTV cameras were higher in neighborhoods with a higher proportion of non-white residents.[58] The researchers also found that a Black Lives Matter protester walking a sample route to a protest in Washington Square Park would be surveilled for approximately 100% of their journey.[59]

---

[53] Police in Miami worked with Clearview AI, which extracts faceprints without their consent. Connie Fossi & Phil Prazan, *Miami Police Used Facial Recognition Technology in Protester's Arrest*, NBC 6 (Aug. 17, 2020), https://www.nbcmiami.com/investigations/miami-police-used-facial-recognition-technology-in-protesters-arrest/2278848/ (noting that Miami police worked with Clearview AI to extract faceprints from billions of people faceprints in a Black-led protest against police violence). Clearview AI's app carries extra risks because law enforcement agencies are uploading sensitive photos to the servers of a company whose ability to protect its data is untested. Hill, *supra* note 52; *see also Facial Recognition Under Scrutiny As Clearview AI's Practices Ruled Illegal in Canada*, IFSEC Insider (Feb. 16, 2021), https://www.ifsecglobal.com/video-surveillance/facial-recognition-under-scrutiny-as-clearview-ais-practices-ruled-illegal-in-canada/ (ruling by Canadian government that Clearview AI's collection of biometric information from its citizens without their knowledge or consent is illegal).

[54] *See* Joseph Goldstein & Ali Walker, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database.*, N.Y. Times (Aug. 1, 2019), https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html.

[55] Katie Canales, *Thousands of US Police Officers and Public Servants Have Reportedly Used Clearview's Controversial Facial Recognition Tech Without Approval*, Bus. Insider (Apr. 6, 2021), https://www.businessinsider.com/clearview-ai-facial-recognition-thousands-police-departments-2021-4; *see also* Press Release, Surveillance Tech. Oversight Project, S.T.O.P. Condemns NYPD for 22K Facial Recognition Searches (Oct. 23, 2020), https://www.stopspying.org/latest-news/2020/10/23/stop-condemns-nypd-for-22k-facial-recognition-searches.

[56] For example, the Chicago and Detroit Department camera systems allow officers to run facial recognition software against any captured images. Blair Paddock, *Chicago Police Using Controversial Facial Recognition Tool*, WTTW (Jan. 30, 2020), https://news.wttw.com/2020/01/30/chicago-police-using-controversial-facial-recognition-tool (In a statement, the Chicago Police Department said it is: "using a facial matching tool to sort through its mugshot database and public source information in the course of an investigation triggered by an incident or crime."); Bryce Huffman, *What We Know So Far About Detroit's Controversial Use of Facial Recognition*, Bridge Detroit (July 22, 2021), https://www.bridgedetroit.com/what-we-know-so-far-about-detroits-controversial-use-of-facial-recognition/ ("Detroit police use facial recognition technology to compare pictures of a suspect with a database of images culled from public records, social media and other sources.").

[57] Amnesty Int'l, *Inside the NYPD's Surveillance Machine,* Ban the Scan, https://banthescan.amnesty.org/decode/ (last visited Jan. 15, 2024).

[58] *Id.*

[59] *Id.*

40 Rector Street
5th Floor
New York, NY 10006

700 14th Street NW
Suite 600
Washington, DC 20005

260 Peachtree Street NW
Suite 2300
Atlanta, GA 30303

naacpldf.org
212-965-2200

In Detroit's Project Green Light, surveillance cameras are placed throughout the city of Detroit—a predominantly Black city[60]—at businesses, apartment complexes, and schools.[61] The cameras constantly collect data and surveil residents' daily life.[62] And because Detroit police can run their facial recognition software against the entire state of Michigan's driver's licenses, state IDs, and criminal databases, they are able to conduct a virtual line-up of almost *every* Michigan resident.[63] However, the cameras are not distributed equally: "surveillance correlates with majority-Black areas, avoiding [w]hite and Asian enclaves."[64]

Other advanced technologies used by law enforcement that surveil individuals' movement and communications are also disproportionately deployed in communities that are majority Black and Brown. In Baltimore, for instance, "stingrays"–a form of cell phone surveillance–were deployed by police "in the city's most intensely segregated non-white neighborhoods."[65] An investigation in Oakland, California found that automated license plate readers (ALPRs) were concentrated in Black and Brown communities, even though automobile offenses predominantly took place elsewhere.[66] A 2013 review of open records suggested similar disparities regarding ALPR deployment in Boston as well.[67] Though nationwide, police surveillance and use of facial recognition software subject all who are surveilled to life-altering and irreversible harms, the risk is exponentially higher for Black and Brown people,[68] who are disproportionately at risk for police misidentification[69] and wrongful arrest.[70]

---

[60] *QuickFacts: Detroit City, Michigan*, U.S. Census Bureau, https://www.census.gov/quickfacts/fact/table/detroitcitymichigan,MI/PST045221 (last visited Jan. 17, 2024).
[61] Rebecca Smith, Univ. of Mich. Carceral State Project, *Project Green Light: Surveillance and the Spaces of the City* (2021), https://storymaps.arcgis.com/stories/14dd97b35cbb4a4298786c75855f8080
[62] *See* Clare Garvie & Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, Geo. Law Ctr. on Priv. & Tech. (May 16, 2019), https://www.americaunderwatch.com/.
[63] Paul Egan, *Never Arrested? Michigan State Police Still Likely Has Your Photo in Its Database*, Detroit Free Press (Mar. 11, 2019), https://www.freep.com/story/news/local/michigan/2019/03/11/michigan-statepolice-facial-recognition-database/3102139002/.
[64] Najibi, *supra* note 50.
[65] George Joseph, *Racial Disparities in Police 'Stingray' Surveillance, Mapped*, Bloomberg (Oct. 18, 2016), https://www.bloomberg.com/news/articles/2016-10-18/u-s-police-cellphone-surveillance-by-stingray-mapped.
[66] Ángel Díaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, Brennan Ctr. for Just. (Sept. 10, 2020), https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations#footnoteref27_e1e9k13.
[67] Kade Crockford, *Data Suggests Boston Police Targeted Black & Working Class Areas for Surveillance*, ACLU (Dec. 17, 2013), https://www.aclu.org/news/privacy-technology/data-suggests-boston-police-targeted-black-working-class.
[68] Robert Williams, a Black man who was wrongfully arrested at his home after Detroit police's use of facial recognition software and surveillance systems, commented that "[a]s any other person would be, I was angry that this was happening to me. As any other [B]lack man would be, I had to consider what could happen if I asked too many questions or displayed my anger openly — even though I knew I had done nothing wrong." Robert Williams, *I Was Wrongfully Arrested Because of Facial Recognition. Why Are Police Allowed to Use It?*, Wash. Post (June 24, 2020), https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology/.
[69] Facial recognition technology frequently misidentifies individuals with darker skin, resulting in higher error rates. According to the National Institute of Standards and Technology, even the top-performing facial recognition software algorithms misidentify Black people at a rate five to ten times higher than they do white people. Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, WIRED (July 22, 2019), https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/; *see also* Orion Rummler, *How AI Police Surveillance Treats People of Color*, Axios (Sept. 7, 2019), https://www.axios.com/2019/09/07/surveillance-people-color-race.
[70] Robert Williams, *I Was Wrongfully Arrested Because of Facial Recognition*, *supra* note 68.

40 Rector Street
5th Floor
New York, NY 10006

700 14th Street NW
Suite 600
Washington, DC 20005

260 Peachtree Street NW
Suite 2300
Atlanta, GA 30303

naacpldf.org
212-965-2200

B. Predictive Policing Systems Are Also Inaccurate, Perpetuate Racial Bias, and Contribute to Discriminatory Policing.

A recent investigation found that a popular predictive policing software, Geolitica (formerly known as PredPol), was accurate less than 1% of the time.[71] In 2016, ProPublica found that the COMPAS recidivism prediction tool falsely labeled Black defendants as future criminals at a rate almost twice that of white defendants.[72] Yet, software marketed as "predictive policing" continues to be developed and sold to law enforcement while increasing the disparate criminalization of Black and Brown people, especially Black and Brown youth.

"Predictive policing" tools claim to determine whether a criminalized conduct will occur, either in a certain location (place-based) or by a certain person (person-based),[73] though the distinction may be somewhat artificial, as variables used even in person-based systems reflect place-based practices.[74] Yet, prior arrests or encounters with law enforcement reflect policing patterns and strategies, not simply the actions of individuals under scrutiny.[75] The reliance of these systems on data, rather than human inputs, creates the faulty impression that the tools are objective, unbiased, and accurate. However, in actuality, this data reflects police activity, including racially biased practices, that has already occurred; thus, police departments are relying upon their own past activity to purport future "predictions" about an individual or a location.[76] In

---

[71] Aaron Sankin & Surya Mattu, *Predictive Policing Software Terrible at Predicting Crimes*, (Oct. 2, 2023), The Markup (Oct. 2, 2023), https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes.

[72] Julia Angwin et al., *Machine Bias,* ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[73] Tim Lau, *Predictive Policing Explained*, Brennan Ctr. for Just. (Apr. 1, 2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained ("Predictive policing involves using algorithms to analyze massive amounts of information in order to predict and help prevent potential future crimes. Place-based predictive policing, the most widely practiced method, typically uses preexisting crime data to identify places and times that have a high risk of crime. Person-based predictive policing, on the other hand, attempts to identify individuals or groups who are likely to commit a crime — or to be victim of one — by analyzing for risk factors such as past arrests or victimization patterns.").

[74] The Pasco (Florida) County Sheriff's Office, for example, used a risk assessment to put students on an "At-Risk Youth" or "At-Risk Target" list and label them as potential future criminals. The overall system is person-based, but the criteria used to score the students include type and number of crimes a given student is accused of, which may reflect greater presence of law enforcement in particular schools and discretionary decisions by officers and school officials to use criminal legal means to resolve an incident. *See* Neil Bedi & Kathleen McGrory, *Pasco's Sheriff Uses Grades and Abuse Histories to Label Schoolchildren Potential Criminals. The Kids and Their Parents Don't Know.*, Tampa Bay Times (Nov. 19, 2020), https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/school-data/.

[75] *See* 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. 192 (2019).

[76] Lau, *supra* note 73 (describing "how some police departments rely on 'dirty data' — or data that is 'derived from or influenced by corrupt, biased, and unlawful practices,' including both discriminatory policing and manipulation of crime statistics—to inform their predictive policing systems."); *see also* Will Douglas Heaven, *Predictive Policing Algorithms Are Racist. They Need to Be Dismantled.*, MIT Tech. Rev. (July 17, 2020), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/ (noting that some pretrial algorithms still use predictors that are out of date, like predicting that a defendant without a landline phone is less likely to show up in court); Dorothy E. Roberts, *Book Review: Digitizing the Carceral State*, 132 Harv. L. Rev. 1695, 1708 (2019) (book review), https://harvardlawreview.org/wp-content/uploads/2019/04/1695-1728_Online.pdf ("Computerized risk assessments are based on data taken from a social context that has already been shaped by hierarchies of race, class,

40 Rector Street
5th Floor
New York, NY 10006

700 14th Street NW
Suite 600
Washington, DC 20005

260 Peachtree Street NW
Suite 2300
Atlanta, GA 30303

naacpldf.org
212-965-2200

other words, predictive policing tools merely predict where future policing will occur, because they make their recommendations using data of prior enforcement activities.[77] One set of researchers tracked the use of "dirty data" in predictive policing algorithms and found that nine of the thirteen jurisdictions they studied employed historically racially biased source material.[78] Thus, algorithm-induced feedback loops often serve as justification for continued discriminatory policing of Black and Brown communities.[79]

Predictive programs increase deployment of officers, and thus encounters, in Black and Brown communities. An analysis of the predictive policing software PredPol found that the company sent more than 5.9 million crime predictions to law enforcement agencies across the country—including law enforcement in California, Florida, Texas, and New Jersey—with the same recurring patterns.[80] PredPol "predicted" little to no criminalized conduct in neighborhoods with predominantly white and middle-to-upper income residents, but, by contrast, PredPol "targeted relentlessly" neighborhoods with predominantly Black, Latinx, and/or low-income families.[81] In Los Angeles, predictive policing programs that were designed to identify "chronic offenders" and "problem areas"–such as Operation Laser and PredPol–consistently reinforced and contributed to the disparate and aggressive policing of Black communities.[82] Journalists investigating PredPol reported that "Geolitica predicted crime at a rate slightly better than blindly throwing darts at a map."[83]

Predictive tools that build databases of individuals purportedly at risk of being involved in criminal conduct also perpetuate racial bias in policing through "digital profiling." An analysis of Chicago's Strategic Subject List (SSL)[84] found a strong association between the algorithmically

---

and gender. Predictive algorithms package this unequal social structure into a score that necessarily reflects individuals' privileged or disadvantaged positions. The aphorism 'garbage in, garbage out' captures an important aspect of data collection but doesn't capture the nature of built-in structural bias. Inequality in, inequality out is more apt.").

[77] Caroline Haskins, *Academics Confirm Major Predictive Policing Algorithm Is Fundamentally Flawed*, VICE (Feb. 14, 2019), https://www.vice.com/en/article/xwbag4/academics-confirm-major-predictive-policing-algorithm-is-fundamentally-flawed (noting that "[b]ecause this data is collected as a by-product of police activity, predictions made on the basis of patterns learned from this data do not pertain to future instances of crime on the whole," which explains why "'predictive policing is aptly named: it is predicting future policing, not future crime.'"); *see also* Danielle Ensign et al., *Runaway Feedback Loops in Predictive Policing*, 81 Proceedings Mach. Learning Rsch. 1 (2018).

[78] Richardson, Schultz & Crawford, *supra* note 75, at 20.

[79] Ishmael Mugari & Emeka E. Obioha, *Predictive Policing and Crime Control in the United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing*, Social Scis, 2021, at 1, https://doi.org/10.3390/socsci10060234.

[80] Aaron Sankin et al., *Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them*, Gizmodo (Dec. 2, 2021), https://gizmodo.com/crime-prediction-software-promised-to-be-free-of-biases-1848138977 (describing how PredPol recommended police spend more time in the very neighborhoods that were already disproportionately Black, Brown, poor, had experienced increased policing previously, and had most problems with biased policing).

[81] *Id.*; *see also* Heaven, *supra* note 75.

[82] *See* Johana Bhuiyan, *LAPD Ended Predictive Policing Programs Amid Public Outcry. A New Effort Shares Many of Their Flaws*, Guardian (Nov. 8, 2021), https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform.

[83] Aaron Sankin & Surya Mattu, *How We Assessed the Accuracy of Predictive Policing Software*, The Markup (Oct. 2, 2023), https://themarkup.org/show-your-work/2023/10/02/how-we-assessed-the-accuracy-of-predictive-policing-software.

[84] Chicago Police Department's Strategic Subject Algorithm created a risk assessment score known as the Strategic Subject List or "SSL." The scores were purported to reflect a person's "probability of being involved in a shooting

40 Rector Street
5th Floor
New York, NY 10006

700 14th Street NW
Suite 600
Washington, DC 20005

260 Peachtree Street NW
Suite 2300
Atlanta, GA 30303

naacpldf.org
212-965-2200

derived SSL risk score and the race/ethnicity of the arrested individual, validating concerns that risk scores are inherently biased and discriminately target people of color.[85] An Amnesty International study of the UK's Metropolitan Police Service Gangs Violence Matrix, a police intelligence system designed to identify individuals linked to gangs, found that the use of the matrix has become "digital profiling," where the factors used to identify a gang member are racialized and conflate elements of youth urban culture with criminality.[86] Black boys and young men constitute more than 75% of individuals in the Gang Matrix, and 40% of the people listed in the system have no record of prior involvement in reported violence in the past two years.[87] Ninety-nine percent of the New York City Police Department's gang database is comprised of Black and Latinx people,[88] while 95% of Chicago's database was comprised of Black and Latinx people before it was shuttered by an oversight board.[89] DHS fusion centers, which resemble predictive policing by aggregating "suspicious activity reports" to inform how law enforcement resources will be deployed, draw their data from Black and Brown communities—e.g., 75 percent of suspicious activity reports from a Los Angeles fusion center involved people of color.[90] These practices illustrate the "dirty data" which may be used to inform predictive policing algorithms.

III. Use of FRT and Predictive Algorithms by Law Enforcement Remain Largely Concealed, and Efforts to Create Transparency Have Thus Far Been Dismissed.

Advanced technologies are deployed by law enforcement despite concerns regarding transparency, oversight, and accountability. The opacity surrounding these technologies—including their design, their variables and algorithms, the datasets on which they rely, and their decision-making processes—often leaves communities in the dark about when, or how they are used. The people subject to advanced technologies are often unaware of the risk of exposure to the tools and have no access to the data upon which the tools rely.[91] For example, the Pasco County Sheriff's Office placed students on an "At-Risk Youth" or "At-Risk Target" list created with an

---

incident either as a victim or an offender." In 2019, the program ended, but the dataset has been retained for historical reference. *Strategic Subject List*, Chi. Data Portal, https://data.cityofchicago.org/Public-Safety/Strategic-Subject-List-Historical/4aki-r3np/about_data (last visited Jan. 12, 2024).

[85] *See* Andrea L. DaViera et al., Risk, Race, and Predictive Policing: A Critical Race Theory Analysis of the Strategic Subject List, Am. J. Comm'y Psych., 2023, at 1, https://doi.org/10.1002/ajcp.12671.

[86] Amnesty Int'l, *Trapped in the Matrix: Secrecy, Stigma, and Bias in the Met's Gangs Database* 30 (2018), https://www.amnesty.org.uk/files/201805/Trapped%20in%20the%20Matrix%20Amnesty%20report.pdf?HSxuOpdpZW_8neOqHt_Kxu1DKk_gHtSL ("[T]he conflation of certain elements of urban youth culture with violent offending is heavily racialised and reinforces a perception of [B]lack boys and young men, in particular, as a risk to public safety.")

[87] *Id.* at 3.

[88] Jocelyn Strauber & Jeanene Barrett, N.Y.C. Dep't of Investigation, *An Investigation into NYPD's Criminal Group Database* 34 (2023), https://www.nyc.gov/assets/doi/reports/pdf/2023/16CGDRpt.Release04.18.2023.pdf.

[89] Chris Tye, *Oversight Commission Shuts Down Chicago Police Gang Database*, CBS News (Sept. 7, 2023), https://www.cbsnews.com/chicago/news/oversight-commission-shut-down-chicago-police-gang-database/.

[90] Dario McCarty, *The Anti-Blackness of Surveillance*, Berkeley Pol. Rev. (Jan. 20, 2021), https://bpr.berkeley.edu/2021/01/20/the-anti-blackness-of-surveillance/.

[91] For example, between 2018 and 2021, more than one in thirty-three U.S. residents were potentially subject to police patrol decisions directed by a crime-prediction software called PredPol. Sankin et al., *Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them*, *supra* note 80. Additionally, the NYPD revealed that, in 2019, it used ten years of manually collected historical crime data to develop its predictive policing tool and teach it to detect crime patterns. Rachel Levinson-Waldman & Erica Posey, *Court: Public Deserves to Know How NYPD Uses Predictive Policing Software*, Brennan Ctr. for Just. (Jan. 26, 2018), https://www.brennancenter.org/our-work/analysis-opinion/court-public-deserves-know-how-nypd-uses-predictive-policing-software.

40 Rector Street
5th Floor
New York, NY 10006

700 14th Street NW
Suite 600
Washington, DC 20005

260 Peachtree Street NW
Suite 2300
Atlanta, GA 30303

naacpldf.org
212-965-2200

algorithmic risk assessment, which identified certain students as likely to commit future crimes thus subjecting the identified children to persistent and intrusive monitoring without any notice to parents or other guardians.[92] This lack of transparency is further complicated by vendors and developers who routinely claim a proprietary interest in the underlying algorithms to their technologies.[93] Yet, no independent validation or testing is required before these technologies are deployed.

Stakeholders' inability to access data that an algorithm uses—or an explanation of an algorithmic system's decision regarding an individual—in a law enforcement context poses significant risks to the life and liberty of people subjected to the technologies. For example, law enforcement's unfettered use of facial recognition technology, which incorporates publicly available photo datasets that expose people to government identification and tracking[94] without their knowledge and largely without independent oversight,[95] raises grave concerns about the potential infringement of individuals' rights. In a report by the U.S. Government Accountability Office, of the 42 federal agencies surveyed that deploy facial recognition technology, at least six agencies reported using facial recognition technology on images of activities that implicate First Amendment protections.[96] And yet, there is very little data collected and made publicly available about the activities of individual law enforcement officers or agencies, including their use of facial recognition technology, that would permit public oversight. The public does not know the demographic characteristics of persons searched, the justification for each search, what technology was used, how the search was conducted, or the outcomes of searches.[97] Subsequently, people are provided with little or no information regarding the role a facial recognition system played in law enforcement's investigative or enforcement activity, the recourse to challenge its use, or the ability to contest abuses or errors.[98]

---

[92] *See* Petition for Writ of Mandamus ¶ 16, *CAIR-Florida v. Nocco*, No. 157331829 (Fla. Cir. Ct. Sept. 13, 2022); Bedi & McGrory, *supra* note 74; Mark Lieberman, *Using Student Data to Identify Future Criminals: A Privacy Debacle*, EDUCATION WEEK (Mar. 24, 2020), https://www.edweek.org/technology/using-student-data-to-identify-future-criminals-a-privacy-debacle/2020/11.

[93] *See* Rashida Richardson, *Racial Segregation and the Data-Driven Society: How Our Failure to Reckon with Root Causes Perpetuates Separate and Unequal Realities*, 36 Berkeley Tech. L.J. 1051, 1087 (2021).

[94] *See* Ryan Mac, Caroline Haskins & Logan McDonald, *Clearview's Facial Recognition App Has Been Used By the Justice Department, ICE, Macy's, Walmart, and the NBA*, BuzzFeed News (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

[95] Clare Garvie, *Garbage In, Garbage Out: Face Recognition On Flawed Data*, Geo. Law Ctr. on Priv. & Tech. (May 16, 2019), https://www.flawedfacedata.com/ ("There are no rules when it comes to what images police can submit to face recognition algorithms to generate investigative leads.").

[96] U.S. Government Accountability Office, Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks, https://www.gao.gov/products/gao-21-518#:~:text=Six%20agencies%20reported%20using%20the,images%20of%20suspected%20criminal%20activity. (last visited Jan. 18, 2024)(" Six agencies reported using the technology on images of the unrest, riots, or protests following the death of George Floyd in May 2020.").

[97] *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition On Flawed Data*, Geo. Law Ctr. on Priv. & Tech. (May 16, 2019), https://www.flawedfacedata.com/ ("The NYPD made 2,878 arrests pursuant to face recognition searches in the first 5.5 years of using the technology [,] Florida law enforcement agencies . . . run on average 8,000 searches per month of the Pinellas County Sheriff's Office face recognition system, [but] [m]any other agencies do not keep close track of how many times their officers run face recognition searches and whether these searches result in an arrest.").

[98] *See* Lauren Feiner & Annie Palmer, *Rules Around Facial Recognition and Policing Remain Blurry*, CNBC (June 12, 2021), https://www.cnbc.com/2021/06/12/a-year-later-tech-companies-calls-to-regulate-facial-recognition-met-

40 Rector Street
5th Floor
New York, NY 10006

700 14th Street NW
Suite 600
Washington, DC 20005

260 Peachtree Street NW
Suite 2300
Atlanta, GA 30303

naacpldf.org
212-965-2200

Predictive policing and other surveillance tools also operate in obscurity. Little is known about what criteria or data sets the algorithms rely upon. Moreover, information regarding how these technologies will be deployed and used by law enforcement agencies, and the likely impacts of predictive policing tools, is often inaccessible. The New York City Police Department's (NYPD), for example, has consistently refused calls by advocates and public officials to increase transparency of its surveillance technology. After a 2019 article disclosed the NYPD's use of a predictive policing tool called "Patternizr,"[99] the NYPD described the information fed into this system but refused to disclose the data sets responsive to public record requests seeking the information.[100] The NYPD later drew criticism when it introduced the "DigiDog" surveillance technology without properly notifying City officials or publicly reporting it, as required by the Public Oversight of Surveillance Technology (POST) Act.[101] Even more recently, the NYPD rejected the vast majority of transparency measures that were recommended by an oversight agency, and repeatedly refused to attend public hearings regarding police surveillance practices.[102] Similarly, ShotSpotter, which is overwhelmingly concentrated in communities of color,[103] refuses to disclose information pertaining to its algorithms and noise classification system. ShotSpotter's aversion to transparency makes it difficult for the public and courts to assess the effectiveness of its technology.[104]

IV. Additional Measures Are Needed to Prevent Potential Violations of People's Civil Rights by Law Enforcement's Use of Facial Recognition Technologies and Predictive Algorithms.

Law enforcement's use of facial recognition and predictive policing technology cannot be addressed without a reckoning of the systemic racism and police violence in our current public safety systems in the United States. Until we transform our public safety systems, law enforcement's use of facial recognition and predictive policing technology will only exacerbate the systemic harm that officers and agencies cause to communities of color even without such

with-little-progress.html; *see also* Aaron Mak, *Facing Facts: A Case in Florida Demonstrates the Problems with Using Facial Recognition to Identify Suspects in Low-Stakes Crimes*, Slate (Jan. 25, 2019), https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html.

[99] Andrew Liptak, *The NYPD Is Using a New Pattern Recognition System to Help Solve Crimes*, The Verge (Mar. 10, 2019), https://www.theverge.com/2019/3/10/18259060/new-york-city-police-department-patternizer-data-analysis-crime.

[100] Tim Lau, *supra* note 73.

[101] Rocco Parascandola, *NYPD Is in the Dog House over Leasing of Robotic Hound*, N.Y. Daily News (Apr. 22, 2021), https://www.nydailynews.com/2021/04/22/nypd-is-in-the-dog-house-over-leasing-of-robotic-hound/; *Public Oversight of Surveillance Technology (POST) Act Impact and Use Policies*, NYPD, https://www.nyc.gov/site/nypd/about/about-nypd/policy/post-act.page (last visited Jan. 16, 2024).

[102] Greg B. Smith, *For Third Time, NYPD Blows Out of Council Hearing on High-Tech Surveillance*, The City (Oct. 31, 2023), https://www.thecity.nyc/2023/10/31/nypd-drones-surveillance-council-hearing/.

[103] Todd Feathers, *Gunshot-Detecting Tech Is Summoning Armed Police to Black Neighborhoods*, VICE (Jul7 19, 2021), https://www.vice.com/en/article/88nd3z/gunshot-detecting-tech-is-summoning-armed-police-to-blackneighborhoods?fbclid=IwAR3W9CjNa1QVLHk8JrutFG85RKIwHYcBAfuqTRVv5iSziwkh-uyC4sa43qg ("In all four cities, the data shows that the sensors are also placed almost exclusively in majority Black and brown neighborhoods, based on population data from the U.S. Census."); MacArthur Just. Ctr., *supra* note 9 ("In Chicago, ShotSpotter is only deployed in the police districts with the highest proportion of Black and Latinx residents. ShotSpotter deployments are concentrated only in those neighborhoods.").

[104] Letter from Elec. Priv. Info. Ctr. to Merrick Garland, Att'y Gen. of the U.S., U.S. Dep't of Just. (Sept. 27, 2023), https://epic.org/documents/epic-letter-to-attorney-general-garland-re-shotspotter-title-vi-compliance/#_ftn34; *see also* Brendan Max, SoundThinking's Black-Box Gunshot Detection Method: Untested and Unvetted Tech Flourishes in the Criminal Justice System, 26 Stan. Tech. L. Rev. 193, 229–30 (2023).

40 Rector Street
5th Floor
New York, NY 10006

700 14th Street NW
Suite 600
Washington, DC 20005

260 Peachtree Street NW
Suite 2300
Atlanta, GA 30303

naacpldf.org
212-965-2200

technology.[105] Thus, the use of technologies like such as predictive policing and facial recognition by law enforcement should be categorically prohibited.

Many cities have rightfully implemented a complete ban on law enforcement's use of facial recognition technology.[106] San Francisco's "Stop Secret Surveillance Ordinance" warned of its propensity to "exacerbate racial injustice and threaten our ability to live free of continuous government monitoring."[107] In 2020, Amazon and IBM stopped selling facial recognition technology to law enforcement agencies, and Microsoft announced it would not sell the technology until there were regulations in place.[108] These governmental and private actions to cease support of law enforcement's use of facial recognition resulted from grave concerns about probable dangers. The federal government should follow suit.

The OMB's recent Draft Memorandum,[109] which outlines minimum risk-management practices for rights-impacting AI, currently only applies to AI used by federal agencies. It does not require that AI systems funded with federal dollars comply with the same minimum risk-management practices.[110] To the greatest extent permitted by law, federal agencies should ensure that grant funding programs and federally-funded AI systems comply with the minimum risk-management practices outlined in OMB's memo. The guidance developed pursuant to Sec.13(e)(iii)(C) of Executive Order 14074 for state and local law enforcement's use of covered technologies should incorporate the OMB's risk-management standards for rights-impacting technologies, particularly the requirements of impact assessments, and a prohibition on the use of such technologies if disparate impacts cannot be adequately mitigated.[111]

---

[105] *See* Letter from NAACP Legal Def. & Educ. Fund, Inc., to Sheila Jackson Lee & Andy Biggs, U.S. House of Representatives (July 20, 2021), https://www.naacpldf.org/wp-content/uploads/2021.07.20-LDF-Statement-on-Law-Enforcement-U_Emily-Fisher-1.pdf.

[106] Fight for the Future, *Ban Facial Recognition*, https://www.banfacialrecognition.com/map/ (last visited Jan. 16, 2024).

[107] Sarah Emerson, *San Francisco Bans Facial Recognition Use by Police and the Government*, VICE (May 14, 2019), https://www.vice.com/en/article/wjvxxb/san-francisco-bans-facial-recognition-use-by-police-and-the-government.

[108] Rebecca Heilweil, *Big Tech Companies Back Away from Selling Facial Recognition to Police. That's Progress.,* VOX (June 11, 2020), https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police.

[109] 88 Fed. Reg. 75635 (Nov. 3, 2023), https://www.govinfo.gov/content/pkg/FR-2023-11-03/pdf/2023-24269.pdf; Memorandum from Shalanda D. Young, Executive Office of the President, Off. of Mgmt. & Budget, to the Heads of Executive Departments and Agencies RE: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence (Nov. 3, 2023), https://ai.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-Public-Comment.pdf.

[110] NAACP Legal Def. & Educ. Fund, Inc., Comment Letter on Off. of Mgmt. & Budget Draft Memorandum on Advancing Governance, Innovation, and Risk Management for Agency's Use of Artificial Intelligence (AI) (Dec. 5, 2023).

[111] *Id.*

40 Rector Street
5th Floor
New York, NY 10006

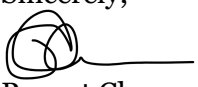
700 14th Street NW
Suite 600
Washington, DC 20005

260 Peachtree Street NW
Suite 2300
Atlanta, GA 30303

naacpldf.org
212-965-2200

We appreciate the opportunity to comment on this important issue and your engagement with the civil rights community on this matter. We look forward to continued engagement. Should you have any questions, please do not hesitate to reach out to Puneet Cheema, LDF's Manager of the Justice in Public Safety Project at pcheema@naacpldf.org and Avatara Smith-Carrington, Strategic Initiatives Law & Policy Fellow, at acarrington@naacpldf.org.

Sincerely,



Puneet Cheema, Manager, Justice in Public Safety Project
Avatara Smith-Carrington, Fellow, Strategic Initiatives Department
David Moss, Fellow, Justice in Public Safety Project
Ananya Karthik, Gardner Fellow
NAACP Legal Defense and Educational Fund, Inc.

40 Rector Street
5th Floor
New York, NY 10006

700 14th Street NW
Suite 600
Washington, DC 20005

260 Peachtree Street NW
Suite 2300
Atlanta, GA 30303

naacpldf.org
212-965-2200