# SCAN CITY

## A Decade of NYPD Facial Recognition Abuse

**ELENI MANIS, PHD, ALBERT FOX CAHN, ESQ., NAZ AKYOL, AND CAROLINE MAGEE**

**JULY 8, 2021**

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

Supported in part by a grant from the Open Society Foundations and by the John D. and Catherine T. MacArthur Foundation.

## I. Introduction

Facial recognition ("FR") is now a common surveillance tool used by many local law enforcement agencies nationwide. When accurate, it can verify that a person is who they say they are or name an unknown person by locating an image in which they have been identified. But FR is error prone. It misidentifies people in poor quality photos and disproportionately misidentifies people of color, women, and the young and elderly. Police compound this risk by doctoring photos and by accepting low-quality matches that are even more likely mistaken. FR's built-in inaccuracies, compounded by police practices, infringe core Constitutional rights. This paper documents explores legislative responses to police abuse of FR.

## II. Facial Recognition and Its Limitations

FR can perform two basic functions: pair matching (verifying that a person is who they claim to be) and one-to-many matching (identifying an unknown person or scanning a crowd for a known person). For example, FR can compare a traveler's face to the image in their biometric passport to verify the traveler's identity.[1] Similarly, a smartphone with FR-based security can scan and compare a user's face to a stored image of the phone owner's face, allowing only the owner to unlock the phone. This is facial verification, or pair matching: FR compares two images and determines whether they are images of the same person.[2] FR can also identify an unknown person by comparing their image to a gallery of many known faces, or compare unknown faces in a crowd to a list of known individuals. Facebook appears to use one-to-many matching to alert its users to photos they may appear in: it compares a photo of an unknown person to its gallery of known users in search of a match.[3] Police departments controversially use one-to-many matching to try to identify unknown individuals photographed at crime scenes[4] and protests.[5] Live facial recognition operates on the same principle: FR compares many unknown faces in a crowd to an image of a known person, or to images of known people, such as individuals on a police watchlist.[6] This is one-to-many matching, or facial identification.

---

[1] "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," National Institute of Standards and Technology, December 19, 2019, https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects- race-age-sex-face-recognition-software. *See also* Aruni Roy Chowdhury et al., "One-to-Many Face Recognition with Bilinear CNNs," in *2016 IEEE Winter Conference on Applications of Computer Vision (WACV)*, 2016, 1–9, https://doi.org/10.1109/WACV.2016.7477593.

[2] Also known as one-to-one matching.

[3] "What Is the Face Recognition Setting on Facebook and How Does It Work?," Facebook Help Center, accessed June 1, 2021, https://www.facebook.com/help/122175507864081.

[4] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Line-Up" (Center on Privacy & Technology at Georgetown Law, October 16, 2016), https://www.perpetuallineup.org/.

[5] "Ban Dangerous Facial Recognition Technology That Amplifies Racist Policing," Amnesty International, January 26, 2021, https://www.amnesty.org/en/latest/news/2021/01/ban-dangerous-facial-recognition-technology-that- amplifies-racist-policing/.

[6] "Live Facial Recognition," Metropolitan Police (United Kingdom), accessed June 20, 2021, https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/.

Both pair matching and one-to-many matching rely on the same three steps to produce their results. First, FR tools must process the photo of the unknown subject (or "probe").[7] FR works best on probes taken under ideal conditions: good lighting, high resolution, subject facing forward, nothing obscuring their face. In real life, ideal conditions rarely obtain. Ordinary photos of people—"faces in the wild"[8]—frequently have poor lighting, low resolution, subjects in makeup or sunglasses, with limbs obscuring their faces or faces turned away from the camera. The face processing step of FR corrects for these factors, to the limited extent that this is possible, by generating many possible versions of a face or by constructing one "canonical" version of a face.[9]

Under ideal circumstances—a probe photo taken in good light, with high resolution, the subject facing forward, and especially for white, middle-aged men—the best FR can achieve astonishing accuracy (e.g., above 97% for pair matching[10]). But as of 2021, even the best face processing cannot fully compensate for a bad probe photo. For example, the most accurate FR tools exceed an astounding 20% error rate for photos taken by travelers at airport kiosks.[11]

Following face processing, FR engages in feature extraction, generating various measurements of the processed face image.[12] Early FR tools used recognizable measurements such as mouth width, ear length, and other measures of facial "landmarks" to generate a face's signature measurements.[13] Contemporary FR takes mathematically complex measurements with the same goal—generating a set of data points for a face that identify it uniquely.

The last step of FR compares faces on their features to make matches. Face verification compares the probe's features and a known face's features to determine if they belong to the same person. Face identification compares a probe's features to the features of many known faces to determine whether the probe matches any of those known faces.

Crucially, these matches are not a sure thing—and match accuracy varies with individuals' race, gender, and age. As discussed, FR's accuracy decreases with decreasing probe quality. But accuracy is also generally lower for Black, Asian, and Indian people and for women, children, and the elderly, when compared to FR tools' accuracy for white, middle-aged men.[14]

---

7 Mei Wang and Weihong Deng, "Deep Face Recognition: A Survey," *Neurocomputing* 429 (March 14, 2021): 215– 44, https://doi.org/10.1016/j.neucom.2020.10.081.

8 "Labeled Faces in the Wild," accessed June 1, 2021, http://vis-www.cs.umass.edu/lfw/ .

9 Wang and Deng, "Deep Face."

10 Wang and Deng, "Deep Face."

11 Patrick J. Grother, Mei L. Ngan, and Kayee K. Hanaoka, "Face Recognition Vendor Test (FRVT) Part 2: Identification," NIST Interagency/Internal Report (NISTIR), September 13, 2019, https://www.nist.gov/publications/face-recognition-vendor-test-frvt-part-2-identification .

12 Wang and Deng, "Deep Face."

13 Shaun Raviv, "The Secret History of Facial Recognition," *WIRED*, January 21, 2020, https://www.wired.com/story/secret-history-facial-recognition/.

14 Wang and Deng, "Deep Face." And NIST 2019.

A 2019 study showed that four major commercial FR tools and four state-of-the-art FR tools misidentified White faces in pair matching 10% of the time, while misidentifying Black and Asian faces almost twice as often.[15] A comprehensive study of FR systems by the U.S. federal government confirmed higher error rates for pair matching of Black and Asian faces, demonstrating error rates up to 100x higher for Blacks and Asians than for Whites, depending on the FR system.[16] That study also found elevated error rates for Black women in one-to-many matching.[17] Even gender classification tools, which predict just the gender of faces in images, show remarkable race and gender bias. A 2018 study of gender classification algorithms by Buolamwini and Gebru showed that the tools misidentified the gender of light-skinned men less than 1% of the time, compared to almost 35% for dark-skinned women.[18] A follow-up audit showed that the FR tools named in the study subsequently reduced their gender and race bias somewhat, while other FR tools still showed outsize bias in gender classification results.[19]

These error rates are disconcerting, but they are the tip of the iceberg, indicating FR's race, sex, and age bias when it is used as intended. In reality, FR users can configure an FR system to return dubious matches that are not recommended by the system's programmers because they do not meet minimum standards for matching.[20] Consider Amazon's Rekognition FR tool.[21] Before banning its FR system for police use entirely, Amazon tried to limit police use of dubious matches (matches that are too likely to be mismatches) by insisting that law enforcement limit itself to higher-quality matches. In 2017, that amounted to the recommendation that police reject matches that are less than 85% certain.[22] In 2018, Amazon upped its recommendation to 95% confidence in an accurate match, then 99% confidence.[23] But when FR is programmed to scrutinize its decisions more carefully and to provide only results with a very high likelihood of success, it rejects dubious matches, returning fewer results. Indeed, FR can return *no* results if there aren't any very good matches. Acknowledging this, Amazon worked privately with police clients to set up lower-than-recommended accuracy levels (or "confidence thresholds") as late as 2019.[24]

---

15 Racial Faces in the Wild: Reducing Racial Bias by Information Maximization Adaptation Network.

16 NIST, "NIST Study Evaluates.

17 NIST, "NIST Study Evaluates."

18 Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," in *Conference on Fairness, Accountability and Transparency* (Conference on Fairness, Accountability and Transparency, PMLR, 2018), 77–91, http://proceedings.mlr.press/v81/buolamwini18a.html.

19 Inioluwa Deborah Raji and Joy Buolamwini, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products," 2019, https://www.media.mit.edu/publications/actionable-auditing-investigating-the-impact-of-publicly-naming-biased- performance-results-of-commercial-ai-products/.

20 Jake Laperruque, "About-Face: Examining Amazon's Shifting Story on Facial Recognition Accuracy," Project On Government Oversight, April 10, 2019, https://www.pogo.org/analysis/2019/04/about-face-examining-amazon- shifting-story-on-facial-recognition-accuracy/.

21 Drew Harwell, "Amazon Extends Ban on Police Use of Its Facial Recognition Technology Indefinitely," *Washington Post*, May 18, 2021, https://www.washingtonpost.com/technology/2021/05/18/amazon-facial- recognition-ban/.

22 Laperruque, "About-Face."

23 Laperruque, "About-Face."

24 Laperruque, "About-Face."

This is deeply problematic: in the context of policing, bad matches put innocent individuals at risk of police harassment. And because of FR's racial bias, people of color are at greatest risk of being wrongly targeted. When the ACLU set Amazon's system to an 80% confidence level and fed the system probe photos of members of Congress, 28 members (more than 5% of Congress members) were matched with people under arrest.[25] Nearly 40% of the mismatches were people of color, even though people of color make up only 20% of Congress.[26] Decreasing the accuracy threshold for matches produces more matches, including more bad matches, or identifications that are more likely to be false. In the world of Facebook, this has the trivial consequence that users get more notifications about photos they don't really appear in. In law enforcement contexts, however, false matches expose innocent people to dangerous scrutiny by police and immigration agencies.[27]

## III. You're on Camera: Facial Recognition in New York City

NYPD's deployment of facial recognition technology in New York City dates back to at least 2011.[28] While NYPD has gone out of its way to shield its FR use from public view, what NYPD cannot hide is its vast and ubiquitous system of street-level and body-worn cameras, all of which produce camera footage that can be used for FR. If you walk around NYC, you are likely on camera. The City has a vast network of thousands of cameras, some government property and others privately owned, that feed information into one, centralized system: the Domain Awareness System.[29] In 2017, that system reportedly consisted of about 6,000 cameras; by 2019, NYPD's deputy commissioner of information technology reported access to "CCTV from the 20,000 cameras that we have deployed across the city."[30] (In 2021, volunteers for Amnesty International located over 15,000 cameras aimed at NYC intersections alone.[31]) The Domain Awareness System relies on cameras for footage and information, but it is also linked to government photo databases, feeds from automatic license plate readers, and gunshot spotter tools.[32]

---

25 Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots," American Civil Liberties Union, July 26, 2018, https://www.aclu.org/blog/privacy-technology/surveillance- technologies/amazons-face-recognition-falsely-matched-28.

26 Snow, "Amazon's Face Recognition."

27 NIST, "NIST Study Evaluates."

28 Joseph Goldstein and Ali Watkins, "She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database.," *The New York Times*, August 1, 2019, sec. New York, https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html.

29 Ángel Díaz, "Oversight of Face Recognition Is Needed to Avoid New Era of 'Digital Stop and Frisk,'" Brennan Center for Justice, May 31, 2019, https://www.brennancenter.org/our-work/analysis-opinion/oversight-face- recognition-needed-avoid-new-era-digital-stop-and-frisk.
*See also* Mariko Hirose, "Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology," *Connecticut Law Review* 49, no. 5 (September 2017): 1591–1620.

30 "A Conversation with Jessica Tisch '08," Harvard Law Today, July 17, 2019, https://today.law.harvard.edu/a- conversation-with-jessica-tisch-08/.

31 "Surveillance City: NYPD Can Use More than 15,000 Cameras to Track People Using Facial Recognition in Manhattan, Bronx and Brooklyn," Amnesty International, June 3, 2021, https://www.amnesty.org/en/latest/news/2021/06/scale-new-york-police-facial-recognition-revealed/.

32 Hirose, "Privacy in Public Spaces," 1594.

Some parts of NYC are blanketed by these cameras—lower Manhattan, for example, has "clusters of sensors" covering "every city block."[33] In many minority communities, the NYPD operates vans with "3-story surveillance cranes" that capture everyone's movements.[34]

NYPD officers' body-worn cameras generate an additional trove of video footage that may be used for FR analysis. As of February 2019, "all uniformed patrol officers in New York City" are equipped with body-worn cameras.[35] With approximately 36,000 officers, the NYPD is the largest police force in the United States,[36] with over 100 officers per square mile.[37] Body-worn cameras travel with officers wherever they go, meaning that overpoliced communities are also over- surveilled: body cameras generate FR-usable footage of anyone interacting with the police and bystanders.[38] While NYPD's body-worn cameras do not have on-site facial recognition capabilities at this time, if they ever do, "thousands of police officers wearing body-worn cameras could record the words, deeds, and locations of much of the population at a given time."[39]

### *NYPD's FR Systems: Dataworks Plus and Clearview AI*

NYPD uses at least two FR vendors: DataWorks Plus, its main vendor, and Clearview AI, which NYPD has used on an extended trial basis. NYPD has refused to share substantive information about its FR systems, even declining to report the names of these vendors in its legally required surveillance tool reporting.[40] However, documents shared with the Georgetown Law Center on Privacy and Technology in 2016 show that DataWorks Plus supplies "a fully integrated facial recognition solution for the New York City Police Department … for over 2 million records and 12,000 web users."[41] Notwithstanding NYPD's seeming confidence in its vendor, DataWorks Plus was embroiled in a FR-based misidentification scandal in 2020, with one of its managers subsequently admitting to the press that DataWorks does not take a "scientific" approach to FR or conduct accuracy and bias testing.[42]

---

33 Diaz, "Oversight of Face Recognition."

34 Diaz, "Oversight of Face Recognition."

35 "Body-Worn Cameras," New York City Police Department, accessed June 20, 2021, https://www1.nyc.gov/site/nypd/about/about-nypd/equipment-tech/body-worn-cameras.page.

36 "About NYPD - NYPD," New York City Police Department, accessed June 20, 2021, https://www1.nyc.gov/site/nypd/about/about-nypd/about-nypd-landing.page.

37 Ava Kofman, "Real-Time Face Recognition Threatens to Turn Cops' Body Cameras Into Surveillance Machines," *The Intercept*, March 22, 2017, https://theintercept.com/2017/03/22/real-time-face-recognition-threatens-to-turn- cops-body-cameras-into-surveillance-machines/.

38 "Street-Level Surveillance: Body-Worn Cameras," Electronic Frontier Foundation, October 18, 2017, https://www.eff.org/pages/body-worn-cameras.

39 "Street-Level Surveillance: Body-Worn Cameras."

40 "Facial Recognition: Impact and Use Policy" (New York City Police Department, April 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/facial-recognition-nypd-impact- and-use-policy_4.9.21_final.pdf.

41 Ava Kofman, "NYPD Refuses to Disclose Information About Its Face Recognition Program, So Privacy Researchers Are Suing," *The Intercept* (blog), May 2, 2017, https://theintercept.com/2017/05/02/nypd-refuses-to- disclose-information-about-its-face-recognition-program-so-privacy-researchers-are-suing/.

42 Kashmir Hill, "Wrongfully Accused by an Algorithm," *The New York Times*, June 24, 2020, sec. Technology, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

NYPD's extended trial use of Clearview FR was confirmed in April 2021.[43] Clearview AI compares unknown probes to any of "3 billion photos scraped from the web."[44] Unlike DataWorks, which compares probes to mugshots and other photos to which police have long had access, Clearview FR puts nearly any photo on the web within law enforcement's grasp— without any consent from pictured individuals. In effect, Clearview FR forces anyone in its 3 billion photos to stand in a "perpetual line-up."[45] And like DataWorks Plus, Clearview AI's accuracy is a question mark: it does not submit its system for outside testing and its capabilities and accuracy are not publicly known.

### *How NYPD Cheats with Facial Recognition*

NYPD capitalizes on the lack of regulation around FR to cheat with the technology: officers exercise "artistic license" with probe photos to improve their chances of making a match. In May 2019, the Georgetown Law Center on Privacy and Technology documented the kinds of abuses that are "common practice" at NYPD.[46] NYPD's "edits often go well beyond minor lighting adjustments and color correction," the report states, "and often amount to fabricating completely new identity points not present in the original photo."[47] In one infamous example of such abuse, NYPD used a photo of the actor Woody Harrelson as a probe because the officers believed a suspect looked enough like the actor.[48] More commonly, NYPD has replaced features and expressions in a street-camera photo, which can be low quality or taken from a bad angle, with features from mugshots.[49] It has used "3D modeling software to complete partial faces" and to "rotate faces that are turned away from the camera."[50] While the best FR systems can perform such rotations as part of face processing,[51] by feeding manipulated photos to FR, NYPD defeats FR's ability to give an honest estimate of match accuracy.[52] NYPD also likely engages in practices common to police departments across the country, such as using probes with "computer-generated facial features" and "artist sketches."[53] In April 2020, following the publication of the Georgetown report, NYPD promulgated a FR policy banning the use of celebrity lookalikes—but allowing photo alterations to stand.[54]

---

43 Tate Ryan-Mosley, "The NYPD Used Clearview's Controversial Facial Recognition Tool. Here's What You Need to Know," MIT Technology Review, April 9, 2021, https://www.technologyreview.com/2021/04/09/1022240/clearview-ai-nypd-emails/ .

44 Ryan-Mosley, "The NYPD Used Clearview."

45 Garvie, "The Perpetual Line-Up.

46 Clare Garvie, "Garbage In, Garbage Out: Face Recognition on Flawed Data," Georgetown Law Center on Privacy and Technology, May 16, 2019, https://www.flawedfacedata.com.

47 Garvie, "Garbage In, Garbage Out."

48 Garvie, "Garbage In, Garbage Out."

49 Garvie, "Garbage In, Garbage Out."

50 Garvie, "Garbage In, Garbage Out."

51 Grother, "Face Recognition Vendor Test."

52 Garvie, "Garbage In, Garbage Out."

53 Garvie, "Garbage In, Garbage Out."

54 "Patrol Guide: Facial Recognition Technology" (New York City Police Department, March 20, 2020), https://www1.nyc.gov/assets/nypd/downloads/pdf/nypd-facial-recognition-patrol-guide.pdf.

NYPD also engages in questionable practices around gallery photos—the many identified photos used in one-to-many matching. FR has lower accuracy when used to identify children and lower accuracy when photos of children are used to identify those children later in life.[55] Even the best FR systems are bedeviled by three factors: poor images, injuries to the face and *ageing*.[56] Nonetheless, NYPD integrated its juvenile offender databases into its FR system by 2015 with the support of City Hall and Mayor Bill de Blasio.[57] NYPD now includes "thousands of arrest photos of children and teenagers" in its FR galleries.[58] Given the disproportionate rate at which Black and Latinx children are charged with crimes, the inclusion of their images in FR galleries increases the likelihood that children of color will be targeted by the police.[59]

Indeed, it is clear that FR reinforces racially discriminatory policing. Even in matters as seemingly innocuous as traffic stops, Black and Latinx individuals are generally stopped at greater rates than white drivers.[60] After a stop, they are more likely to be searched than white drivers.[61] Thereafter, they are more likely to be arrested.[62] Because arrest photos are enrolled in police departments' FR galleries, racial discriminatory policing ensures that people of color are at greater risk of future FR-initiated police interactions.[63]

## IV. Constitutional Harms

### *Unconstitutional Searches and Seizures*

Courts are slowly beginning to apply the Fourth Amendment's ban on unreasonable searches to novel tracking technologies like FR.[64] A Fourth Amendment search occurs when police invade an individual's reasonable expectation of privacy.[65] Historically, courts found our expectation of privacy greatest in the home, greatly reduced in cars, and almost completely absent in public spaces.

However, these categories are increasingly blurred by the tracking power of novel technologies. The Supreme Court's decisions in the recent trilogy of Fourth Amendment cases, *Jones*, *Riley*, and *Carpenter*, show the potential for greater protection from location tracking in the future.

---

55 Grother, "Face Recognition Vendor Test."

56 Grother, "Face Recognition Vendor Test."

57 Goldstein and Watkins, "Arrested at 14."

58 Goldstein and Watkins, "Arrested at 14."

59 Goldstein and Watkins, "Arrested at 14.

60 "The Stanford Open Policing Project: Findings," accessed June 20, 2021, https://openpolicing.stanford.edu/findings/.

61 "Stanford Open Policing Project."

62 "Report to the United Nations on Racial Disparities in the U.S. Criminal Justice System," The Sentencing Project, April 19, 2018, https://www.sentencingproject.org/publications/un-report-on-racial-disparities/.

63 Hirose, "Privacy in Public Spaces," 1616.

64 *See generally* Katz v. United States, 389 U.S. 347 (1967). *See also* Hirose, "Privacy in Public Spaces," 1601; Hamann and Smith, "Facial Recognition Technology."

65 *See Katz*, 389 U.S. at 360 (Harlan, J., concurring).

In *United States v. Jones*, police officers used a GPS tracking device on Jones's car to track his location for 28 days without a warrant.[66] Historically, the courts afforded officers broad latitude to track cars on public street, noting that vehicles were visible to any passerby. However, in *Jones*, the Supreme Court struck down the search on a narrow, property-based theory, finding officers had trespassed by attaching a physical tracking device to Jones' care. Notably, Justices Alito and Sotomayor adopted a far broader rationale, noting the GPS tracker provided more comprehensive and persistent location tracking than would be possible with officers using traditional, human surveillance techniques.

Two years later, in *Riley v. California*, the Supreme Court once again rejected law enforcement's analogies to analog surveillance techniques, striking down warrantless searches of cellphones.[67] Traditionally, police do not need a warrant to search an arrestee's body and possessions. In *Riley*, officers found a cell phone while conducting a routine pat down and proceeded to search the contents, including photos and videos. Prosecutors later used this content to prove arrestee's gang affiliation at trial. The Supreme Court found that searching a cellphone is much more invasive than searching a wallet, as phones contain the "sum of an individual's private life."[68]

Four years later, in *Carpenter v. United States*, the Supreme Court went much further. The Supreme Court struck down prolonged, warrantless cell site location information ("CSLI") tracking. Cellphone providers generate a near-constant record of which cell tower is closest to a phone at any one time.[69] Similar to *Riley*, police tracked Carpenter's movements for more than a week using CSLI. But a crucial difference is that officers never trespassed as in *Riley* to conduct the search. By holding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI," the Court pointed to the court opened the door to numerous analogous challenges.[70] For example, it is unclear why persistent location tracking via FR would be any less constitutionally suspect than via CSLI. Unfortunately, such an expansion of *Carpenter* is not automatic. Chief Justice Roberts' opinion in *Carpenter* explicitly limited the holding to use of CSLI data for more than 7 days.[71]

---

66 United States v. Jones, 565 U.S. 400, 413, 418 (2012) (Alito, J., concurring & Sotomayor, J., concurring).

67 Riley v. California, 573 U.S. 373 (2014).

68 *See Riley*, 573 U.S. at 393.

69 Eric Lode, "Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessor of Phone Under Fourth Amendment," 92 A.L.R. Fed. 2d 1, 2 (2015).

70 Carpenter v. United States, 138 S. Ct. 2206, 2217-2218 (2018) (explaining that time-stamped location data "provides an intimate window into a person's life, revealing [private information about] familial, political, professional, religious, and sexual associations," and noting that location tracking using new technology "is remarkably easy, cheap, and efficient compared to traditional investigative tools, "making it more dangerous, and adding that the retrospective quality of location data gives police access to a category of information otherwise unknowable)

71 *Id.* at 2220. ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval. We do not disturb the application of Smith and Miller or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might
incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security.")

Additionally, even if *Carpenter* were extended to cover FR-based location tracking, that would only address one of the technology's harms. FR is more often used to identify individuals at a single point in time.[72] Furthermore, it is unclear how such a holding would impact the array of government agencies that use FR for non-law enforcement purposes.[73]

### *Seizures: Facial Recognition as Basis for Arrest*

FR can also potentially violate individual's right against unlawful seizure, which prohibits arrests absent probable cause as measured under the "totality of the circumstances."[74] Given FR's unreliability, it is unlikely a purported "match" *alone* establishes probable cause. Currently, many police departments claim never to use FR as the sole basis for an arrest, but officers appear to be doing just that, arresting individuals with no meaningful confirmation of an FR "match." [75] Unfortunately, it may be practically difficult for many arrestees to prove that FR was the sole basis for arrest, making such a challenge more difficult to pursue.[76]

Consider the story of Kaitlin Jackson, a public defense attorney with the Bronx Defenders. In 2018, Jackson represented a man arrested for stealing socks from a T.J. Maxx store, allegedly after "brandishing a box cutter."[77] Jackson's client was arrested months after the alleged crime occurred, prompting Jackson to wonder how the police placed her client at the crime scene months after the fact without forensics.[78] She then found out that the police ran T.J. Maxx's security footage through FR software.[79] The police then "texted the security guard a single photo" of the result and asked: "is this the person?"[80]

---

72 Kristin Finklea et al., "Federal Law Enforcement Use of Facial Recognition Technology" (Congressional Research Service, October 27, 2020), https://fas.org/sgp/crs/misc/R46586.pdf.

73 *See* Lola Fadulu, "Facial Recognition Technology in Public Housing Prompts Backlash," *The New York Times*, September 24, 2019, sec. U.S., https://www.nytimes.com/2019/09/24/us/politics/facial-recognition-technology- housing.html.

74 Illinois v. Gates, 462 U.S. 213 (1983).

75 Garvie, "Garbage In, Garbage Out." (Explaining that the NYPD has stated that they use the results of facial recognition searches as possible matches only, which must not be used as positive identification.)

76 Garvie, "Garbage In, Garbage Out." "The NYPD made 2,878 arrests pursuant to face recognition searches in the first 5.5 years of using the [FR] technology."

77 Lane Brown, "There Will Be No Turning Back on Facial Recognition," New York Magazine Intelligencer, November 12, 2019, https://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html.

78 Brown, "No Turning Back."

79 Brown, "No Turning Back."

80 Brown, "No Turning Back."

Shockingly, the prosecution refused to dismiss the case, despite the fact that Jackson's client has an alibi—his wife was in labor at the time of the alleged theft, he was in the delivery room, and presented pictures of himself at the hospital.[81] As of April 2021, three ongoing court cases are also contesting false FR matches as wrongful and insufficient grounds for arrest, and in one case, as evidence of racial discrimination.[82] At the center of each case is a Black man wrongfully arrested on the basis of an incorrect FR match: Michael Oliver, wrongly arrested by the Detroit police; Robert Williams, also wrongly arrested by the Detroit police, and Nijer Parks, wrongly arrested and held for 10 days by the New Jersey police.[83]

When facial recognition is used as evidence, it raises separate Sixth Amendment concerns. Normally, the *Brady* rule requires prosecutors to disclose any exonerating evidence to defendants. Despite this requirement, prosecutors have been allowed to withhold the false "matches" that FR software created in an investigation.[84]This is significant, as many systems return hundreds of potential "matches" with each search, greatly reducing the persuasiveness of an FR "match" to a jury.

Defendants may also be able to suppress FR evidence at trial through the *Frye* and *Daubert* standards scientific evidence. Under *Frye* evidence must be generally accepted by the scientific community to be admitted.[85] *Daubert* measures general acceptance, but it also incorporates four additional prongs to the analysis, creating a more permissive standard for admission.[86] Until the courts strike down FR, the cost will not be borne equally. Justice Sotomayor has noted that uncheck surveillance disproportionately victimizes BIPOC communities, and FR is no different.[87] The sad truth is that in "a world where the police are free to direct surveillance technologies to anyone without any suspicion, the scrutiny is likely to fall on communities of color."[88]

---

81 Brown, "No Turning Back."

82 Drew Harwell, "Wrongfully Arrested Man Sues Detroit Police over False Facial Recognition Match," *Washington Post*, April 14, 2021, https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest- lawsuit/.

83 Drew Harwell, "Wrongfully Arrested Man Sues Detroit Police over False Facial Recognition Match," *Washington Post*, April 14, 2021, https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest- lawsuit/.

84 *See* Lynch v. State, 260 So. 3d 1166 (Fla. 1st Dist. Ct. App. 2018).

85 Frye v. United States, 293 F. 1013, 1014 (D.C. Cir. 1923).

86 *See* Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579 (1993).

87 *See* Utah v. Strieff, 136 S. Ct. 2056, 2070 (2016) (Sotomayor, J., Dissenting).

88 Hirose, "Privacy in Public Spaces," 1616.

### *Chilling Effects and Hampering Free Expression*

Facial recognition also threatens free expression, potentially chilling public dissent.[89] During the 2015 protests of the police killing of Freddie Gray, Baltimore police used facial recognition to identify and arrest protesters."[90] More recently, police departments and the FBI requested photos of those protesting the police killings of Breonna Taylor and George Floyd.[91] FR searches make it far cheaper and easier for police to track protesters, potentially chilling participation, particularly by undocumented individuals and those with criminal justice involvement. Such tracking is antithetical to the First Amendment right to *anonymous* speech and assembly, undocumented by police.[92]

## V. Emerging Legislation

Pioneering municipalities have already taken measures to ban and regulate police use of FR. In 2019, San Francisco was the first U.S. city to ban local police use of FR.[93] In 2020, Vermont passed the first state law banning government use of FR without express legislative approval.[94] Massachusetts followed with a ban on government use of FR or biometric surveillance without a court order.[95] In February 2021, Virginia followed suit, banning local and campus police use of FR without state legislative approval.[96] As of May 2021, at least seven states and twenty municipalities have regulated police or government use of FR, and twenty additional states are currently considering such bills.[97] A number of these bills include private rights of action, NDA bans, acquisition approval measures, and evidentiary exclusion provisions.[98]

---

89 For relevant Supreme Court decisions see Kristine Hamann and Rachel Smith, "Facial Recognition Technology: Where Will It Take Us?," *American Bar Association Criminal Justice Magazine*, Spring 2019, https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial- recognition-technology/.

90 "Street-Level Surveillance: Face Recognition," Electronic Frontier Foundation, October 24, 2017, https://www.eff.org/pages/face-recognition.

91 Dave Gershgorn, "Facial Recognition Is Law Enforcement's Newest Weapon Against Protesters," OneZero, June 3, 2020, https://onezero.medium.com/facial-recognition-is-law-enforcements-newest-weapon-against-protestors- c7a9760e46eb.

92 NAACP v. Alabama, 357 U.S. 449, 1174 (1958). *See also* "Anonymity," Electronic Frontier Foundation, accessed June 28, 2021, https://www.eff.org/issues/anonymity.

93 S.F., CAL., ADMINISTRATIVE CODE ch. 19B, §§ 19B.1-19B.8 (2019).

94 S. 124, 2020 Gen. Assemb., (Vt. 2020).

95 S. 1385, 191st Gen. Ct. (Mass. 2020).

96 H. 2031, 2021 Gen. Assemb., Spec. Sess. I. (Va 2021)

97 Julie Carr Smyth, "States Push Back Against Use of Facial Recognition by Police | California News | US News," US News & World Report, May 5, 2021, https://www.usnews.com/news/politics/articles/2021-05-05/states-push- back-against-use-of-facial-recognition-by-police .

98 "State Facial Recognition Policy," Electronic Privacy Information Center, accessed June 28, 2021, https://epic.org/state-policy/facialrecognition/.

New York City and New York State have taken first steps toward regulating police use of FR. The NYC City Council voted to require NYPD to publicly report its FR and surveillance tools for the first time in January 2020. The Public Oversight of Surveillance Technology Act ("POST Act") requires NYPD to issue an "impact and use policy" explaining how each of its surveillance technologies work and describing steps taken to protect city residents' privacy.[99] At the state level, NYS Assembly Bill A768 (2021-2022 session) would prohibit the use of an FR identification as the sole factor determining the existence of probable cause for arrest.[100] NYS Senate Bill S79 (2020-2021 session) would ban police use of FR and biometric surveillance tools and establish a task force to consider policies that might enable the tools' limited use.[101]

No federal laws regulate FR at this time, but two recent legislative efforts are worth noting. In March 2019, Senator Roy Blunt (R-MO) introduced Bill S.847 in the U.S. Senate Commerce, Science, and Transportation Committee. The bill, if enacted, would protect consumers from corporations' FR, requiring commercial FR users to be up front about their tools and to obtain consumers' consent before identifying or tracking them.[102] In February 2020, Senator Jeff Merkley (D-OR) introduced Bill S.3284 regulating private and government use of FR to the U.S. Senate Homeland Security and Governmental Affairs Committee. The bill, if enacted, would prohibit any individual from setting up an FR-enabling camera, from using FR, or from using information obtained via FR, until Congress enacts appropriate FR legislation.[103] The bill includes a private right of action, permitting an individual to sue in civil court for violations.[104] It cuts off federal funding for state and local FR.[105]

## VI. CONCLUSION

Like other police departments across the country, the NYPD has been dangerously reliant on FR with serious consequences for the civil, constitutional, and privacy rights of New Yorkers. Creative litigation strategies, encouraged by some modest reassurance from the Supreme Court, can provide protection from the dangers of FR, especially to criminal defendants. For broad protection from police overuse and abuse of FR, however, strong legislation at the municipal and federal levels is urgently necessary.

99 N.Y.C., N.Y., ADMINISTRATIVE CODE § 14-188 (2020).
100 A.B. 768, 2021-2022 N.Y. Leg. Sess. (referred to Governmental Operations Comm., Jan. 06, 2021)
101 S.B. 79, 2021-2022 N.Y. Leg. Sess. (referred to Internet and Technology Comm., Feb. 24, 2021)
102 Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (as introduced in the Senate, Mar. 14, 2019).
103 Ethical Use of Facial Recognition Act, S. 3284, 116th Cong. (as introduced in the Senate, Feb. 12, 2020).
104 *Id.* § 5(a)
105 *Id.* § 5(b)

Surveillance Technology
Oversight Project, Inc.
40 Rector Street
9th Floor
New York, NY 10006
www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT