NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 22, ISSUE 4: MAY MAY

LAW ENFORCEMENT USE OF FACIAL RECOGNITION: BIAS, DISPARATE IMPACTS ON PEOPLE OF COLOR, AND THE NEED FOR FEDERAL LEGISLATION

Christopher Jones*

For decades, law enforcement agencies across the country have relied on Facial Recognition Technology ("FRT") to assist with investigations, though how the technology is employed is often concealed from the public and remains largely unknown. Compounding this transparency problem, recent research has shown FRT displays a demonstrated bias against people of color, and disproportionately impacts them accordingly. In the absence of any federal law regulating law enforcement's use of FRT, state and local governments have been left to decide for themselves whether, and to what extent, the technology should be regulated in their jurisdictions. With the potential for abuse of FRT so high, Congress must implement federal legislation that establishes FRT standards and guidelines for law enforcement agencies in the United States to follow. To adequately address the problems associated with FRT, the federal legislation must increase transparency, promote accountability, and foster trust between the police and their communities.

TABLE OF CONTENTS

* J.D. Candidate, University of North Carolina School of Law, 2022. The Author would like to thank the entire JOLT Board and Staff, especially Madeline Labovitz, Alessandra Carlton, and Sarah Kirschbaum, for their thoughtful feedback and guidance throughout the editorial process. The Author would also like to thank Professor Joseph E. Kennedy for his insightful comments, and Professors Erika K. Wilson and Ifeoma Ajunwa for their wisdom and assistance.

I. INTRODUCTION

Facial Recognition Technology ("FRT") has long been used by law enforcement agencies as an investigatory tool.[1] FRT is especially useful for police in situations when other means of identification prove to be more difficult.[2] Consider the case of a Florida man fleeing custody in 2017.[3] After successfully bringing the suspect's car to a halt, the police approached the driver's side of the vehicle to find a man, seemingly unconscious after ingesting an unknown substance, with no identification card and whose fingerprints appeared to have been chewed off.[4] With no other way

[1] *See* KRISTIN FINKLEA ET AL., CONG. RSCH. SERV., R46586, FEDERAL LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECHNOLOGY 1 (2020).

[2] *See* Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html [https://perma.cc/AY29-HJQ5].

[3] *See id.*

[4] *Id.* In the police report obtained by the New York Times, the individual's name has been redacted and thus not known to the public. *Id.*

to identify him, the officers ran a photo of the man through their facial recognition database, a statewide program that has been in place for almost twenty years.[5] The database found a likely match for the man's identity, and the police were able to positively identify the suspect despite his unresponsive state.[6] While this unusual example demonstrates a scenario where FRT can be useful for law enforcement, other examples show just how harmful and destructive police use of FRT can be.

Compare the previous example with that of Nijeer Parks, a thirty-three-year-old Black man from New Jersey, who spent ten days in jail after being falsely accused of theft and attempting to hit a police officer with his car.[7] Despite being thirty miles away at the time of the incident, Mr. Parks' image returned as a match in the facial recognition database, and he was subsequently arrested.[8] While Mr. Parks was eventually able to establish an alibi and demonstrate that his arrest was based on a false identification, his arrest was anything but inconsequential.[9] Mr. Parks spent ten days in jail, faced ten years imprisonment if convicted, and was forced to spend nearly $5,000 on representation.[10]

Mr. Parks' case demonstrates a fundamental problem with police use of FRT: repeated assessments have revealed that this technology is much less accurate in identifying people of color, and disproportionately impacts them accordingly.[11] Present day unregulated use of a technology with a demonstrated bias towards people of color has the potential to be abused by law enforcement,

---

[5] *Id.*

[6] Seminole County Sheriff's Office, Arrest Report No. 201700001572 (Feb. 26, 2017).

[7] Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Jan. 6, 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html [https://perma.cc/TXD4-RY3U].

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, WASH. POST (Dec. 19, 2019, 6:43 PM), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/ [https://perma.cc/9JDC-NE4D].

risks violating the civil liberties of members of the community that the police are supposed to protect, and must be examined with rigid scrutiny.[12] As such, there is a clear need for federal legislation that increases transparency of how police use FRT, reduces racial bias present in the technology, prevents long-term surveillance without a warrant, and limits the databases from which law enforcement can run facial recognition searches. Such a law could be enforced at the state and local levels by withholding federal grant funding.[13]

This Article proceeds in five parts. Part II describes how FRT operates and how the technology has been traditionally used in a law enforcement context. Part III examines bias within FRT and how such bias leads to disparities in accuracy rates and impacts among different demographics. Part IV discusses the potential consequences of a faulty arrest, how FRT may implicate the Fourth Amendment, and the claimed, but insufficient, procedural safeguards. Lastly, Part V argues for federal regulation and explains how implementing such regulations can reduce FRT's disparate impact on people of color.

II. BACKGROUND ON FACIAL RECOGNITION AND LAW ENFORCEMENT USE

The origins of FRT can be traced back to the 1960s, when researchers in California began programming computers to recognize human faces using gridlines.[14] During the decades that followed, advancements in technology increased the accuracy and efficiency of FRT to the point where it has become ubiquitous in

---

[12] *See* Thorin Klosowski, *Facial Recognition Is Everywhere. Here's What We Can Do About It.*, N.Y. TIMES (July 15, 2020), https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/ [https://perma.cc/YWU5-JN3L].

[13] FINKLEA ET AL., *supra* note 1, at 12.

[14] *See* Jeremy Norman, *Woodrow Beldsoe Originates of Automated Facial Recognition*, HISTORYOFINFORMATION, https://www.historyofinformation.com/detail.php?id=2126 [https://perma.cc/KPP3-98AV]. *See also* Fernande van Schelle, *The Evolution of Facial Recognition: From Bodycams to Video Surveillance*, SEC. INFORMED, https://www.securityinformed.com/insights/evolution-facial-recognition-body-cams-video-co-7121-ga.1535016202.html [https://perma.cc/MX8E-WHLK] (detailing the history of facial recognition technology).

modern society.[15] The Pinellas County Sheriff's Office in Florida, which first started using facial recognition in 2001, provides one of the earliest examples of law enforcement's use of FRT.[16] With access to both state and federal databases, Florida police can currently search nearly fifty million images, and do so an estimated 8,000 times per month without any meaningful oversight.[17] Over the past twenty years, facial recognition searches by law enforcement have become relatively routine at the state and federal level.[18] Indeed, an estimated one in four state and local law enforcement agencies currently have access to facial recognition databases.[19]

A. Facial Recognition Technologies and Processes

FRT is a sub-field of artificial intelligence technology that is used as a method for verifying or identifying individuals based on the features of their face.[20] "[T]here is no one standard system design for facial recognition systems," so FRT encompasses a wide range of technologies and processes that function differently depending on the context.[21] For example, one FRT process can simply detect

---

[15] *See, e.g.,* Klosowski, *supra* note 12 (identifying various ways facial recognition is used today, including at the airport and border to confirm travelers' identities, in stores for tracking shoplifters, at sports arenas and event venues for security, and for securing devices like laptops and phones).

[16] Clare Garvie et al., *Jurisdiction-Florida*, GEO. L. CTR. PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/jurisdiction/florida [https://perma.cc/M27X-YDG8].

[17] *Id.*

[18] *See, e.g.*, Alfred Ng, *Police are Using Facial Recognition for Minor Crimes Because They Can*, CNET (Oct. 24, 2020, 5:00 AM) https://www.cnet.com/news/police-are-using-facial-recognition-for-minor-crimes-because-they-can/ [https://perma.cc/FE9E-6G4Z] ("In a recent court filing, the NYPD noted that it's turned to facial recognition in more than 22,000 cases in the last three years.").

[19] Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/ [https://perma.cc/W7K3-NZXZ] ("FBI face recognition searches are more common than federal court-ordered wiretaps.").

[20] FINKLEA ET AL., *supra* note 1, at 1; *Street Level Surveillance: Face Recognition*, ELEC. FRONTIER FOUND. (Oct. 24, 2017), https://www.eff.org/pages/face-recognition [https://perma.cc/29BS-Y9TY].

[21] FINKLEA ET AL., *supra* note 1, at 2. The different technologies and processes mentioned in this paragraph are technically all considered Facial Recognition Technology.

whether an image contains a face, while another process can analyze a video in real time to determine the identities of those in the video.[22] Alternatively, facial classification algorithms do not identify individuals but instead analyze a face image "to produce an estimate of age, sex, or some other property," while facial recognition algorithms can compare two separate images and produce a measure of similarity for identification purposes.[23]

In what is known as a "one-to-many identification search," facial recognition algorithms compare a single photo (i.e., probe image) against a gallery of images, most typically a database, and return a range of potential matches each with a similarity score indicating how closely related the two images are.[24] FRT algorithms in a one-to-many identification search operate by first identifying specific details on a person's face, such as the distance between and shape of facial features.[25] The technology then converts that data into a mathematical representation, and uses that information to compare against data already collected and stored in the database.[26] In ideal conditions, with perfect lighting, positioning, and resolution, FRT identification and verification results are incredibly accurate.[27] However, many facial recognition systems vary in their ability to correctly identify people when the probe image is not captured in ideal conditions, which is often the case.[28]

---

[22] *Id.* at 2.

[23] *Id.* at 1–2.

[24] *Id.* at 2. A probe image refers to the facial image or template searched against a gallery or database of photos in a facial recognition system.

[25] *Street Level Surveillance: Face Recognition*, *supra* note 20.

[26] *Id.*

[27] *See* William Crumpler, *How Accurate are Facial Recognition Systems – and Why Does it Matter?*, CTR. STRATEGIC & INT'L STUD. (Apr. 14, 2020), https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter [https://perma.cc/RAB2-5HDV] ("[T]his degree of accuracy is only possible in ideal conditions where there is consistency in lighting and positioning, and where the facial features of the subjects are clear and unobscured.").

[28] *See* Valentino-DeVries, *supra* note 2 ("Poorer-quality images are known to contribute to mismatches, and dim lighting, faces turned at an angle, or minimal disguises such as baseball caps or sunglasses hamper accuracy.").

B. Law Enforcement Use of FRT

FRT is one of several biometric technologies used by law enforcement agencies and serves a variety of purposes in a law enforcement context.[29] Today, FRT is mainly used by the police to either confirm someone's claimed identity (face verification) or to identify an unknown face (face identification).[30] The verification and identification functions of FRT have been particularly useful for "generating investigative leads, identifying victims of crimes, facilitating the examination of forensic evidence, and helping verify the identity of individuals being released from prison."[31] FRT is also employed by federal agencies at the U.S. border and in airports to verify travelers' identities.[32] Law enforcement agencies generally use one-to-many identification searches when employing facial recognition to produce a gallery of potential suspects.[33]

Traditionally, police accessed databases comprised of criminal records and information of individuals who had previously been arrested.[34] As part of the standard booking and identification process, police routinely collect and store the DNA, fingerprints, and picture of a person in lawful custody.[35] Similar to fingerprints, the mugshot of an individual processed after an arrest is uploaded to a database where it will remain indefinitely and can be searched by police in the future.[36] As such, allowing police to search mugshot databases does not impinge on most reasonable expectations of privacy because the expectations "of an individual taken into police custody 'necessarily are of a diminished scope.'"[37]

However, police use of FRT is more troubling when they have access to other databases that contain billions of images of

---

[29] *See* FINKLEA ET AL., *supra* note 1, at 4.
[30] Garvie et al., *supra* note 19.
[31] FINKLEA ET AL., *supra* note 1, at 4.
[32] *Id.* at 1.
[33] *Id.* at 5.
[34] Garvie et al., *supra* note 19 ("Historically, FBI fingerprint and DNA databases have been primarily or exclusively made up of information from *criminal* arrests or investigations.").
[35] *See* Maryland v. King, 569 U.S. 435, 458 (2013).
[36] *See Street Level Surveillance: Facial Recognition*, *supra* note 20.
[37] King, 569 U.S. at 461 (quoting Bell v. Wolfish, 441 U.S. 520, 557 (1979)).

law-abiding citizens, often without those individuals' consent.[38] In fact, an increasing number of police departments are now able to supplement facial recognition searches by accessing not only mugshot images but also state driver's license databases.[39] At least twenty-one states currently allow federal agencies unfettered access to Department of Motor Vehicles ("DMV") records containing driver's license and identification card pictures.[40] As a result, an estimated 117 million people–or one in two Americans–unknowingly find themselves in a law enforcement facial recognition network.[41] Allowing police access to state driver's license databases places millions of law-abiding Americans on a potential suspect list for no other reason beyond registering to drive in their respective states.[42] Counterintuitively, the accuracy of FRT actually decreases as the number of people in a database increases given the shared facial similarities of so many people in the world.[43]

Moreover, a few private technology companies have also entered the highly lucrative facial recognition market.[44] Amazon,

---

[38] *See* Zusha Elinson, *Police Use of Facial Recognition With License Databases Spur Privacy Concerns*, WALL ST. J. (June 17, 2018, 7:00 AM), https://www.wsj.com/articles/police-use-of-drivers-license-databases-to-nab-crooks-spurs-privacy-concerns-1529233200 [https://perma.cc/NN4D-4DND].

[39] *Id.*

[40] Kim Miller, *Facial Recognition: Current Uses, Concerns, and State Action,* MULTISTATE (Feb. 19, 2020), https://www.multistate.us/insider/2020/2/19/facial-recognition-current-uses-concerns-and-state-action [https://perma.cc/6BUC-7GHB].

[41] *Half of All American Adults Are in a Police Facial Recognition Database, New Report Finds*, GEO. L. (Oct. 18, 2016), https://www.law.georgetown.edu/news/half-of-all-american-adults-are-in-a-police-face-recognition-database-new-report-finds/ [https://perma.cc/882V-LEE5].

[42] *See* Elinson, *supra* note 38.

[43] *See Street Level Surveillance: Face Recognition*, *supra* note 20. *See also* Adrienne Lafrance, *The Ultimate Facial-Recognition Algorithm*, THE ATLANTIC (June 28, 2016) https://www.theatlantic.com/technology/archive/2016/06/machine-face/488969/ [https://perma.cc/2VNQ-T7S4] (detailing a study conducted by researchers at the University of Washington that found "[a]s the databases grew, machine accuracy dipped across the board").

[44] *See* Rebecca Heilweil, *Big Tech Companies Back Away from Selling Facial Recognition to Police. That's Progress.*, VOX (June 11, 2020, 5:02 PM), https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police [https://perma.cc/3CC9-LKPB]. *See also* Nicole Martin, *The Major Concerns Around Facial Recognition Technology*,

Microsoft, and IBM all sold facial recognition technology to law enforcement up until the summer of 2020, when they announced a temporary pause–a decision influenced by social justice protests across the country and pressure from civil liberties groups.[45] In another example, Clearview AI, a start-up company specializing in facial recognition, compiled a database of more than three billion images scrubbed from online websites and apps such as Facebook, Instagram, and Venmo.[46] Clearview's target consumer was police departments, and its facial recognition software is currently used by approximately 2,400 law enforcement agencies.[47] With access to all the above referenced databases, law enforcement agencies have immense resources at their disposal to conduct facial recognition searches.

III. BIAS AND DISPROPORTIONATE IMPACT ON PEOPLE OF COLOR

FRT relies on machine learning to assist in making decisions, which is the concept that "machines should be able to learn and adapt through experience."[48] The technology gains this experience through training data, which is comprised of data sets that specify to

---

FORBES (Sept. 25, 2019, 3:15 PM), https://www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology/?sh=66f843d84fe3 [https://perma.cc/K87G-EDKM] ("[T]he facial recognition industry is expected to grow $3.2 billion in 2019 to $7.0 billion by 2024 in the U.S.").

[45] Heilweil, *supra* note 44.

[46] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 31, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/U2UD-4YMY].

[47] *Id.*; *see* Kim Lyons, *Use of Clearview AI Facial Recognition Tech Spiked as Law Enforcement Seeks to Identify Capitol Mob*, THE VERGE (Jan. 10, 2021, 12:49 AM), https://www.theverge.com/2021/1/10/22223349/clearview-ai-facial-recognition-law-enforcement-capitol-rioters [https://perma.cc/99SV-WYZ7].

[48] Wayne Thompson et al., *Artificial Intelligence, Machine Learning, Deep Learning and Beyond: Understanding AI Technologies and How They Lead to Smart Applications*, SAS, https://www.sas.com/en_us/insights/articles/big-data/artificialintelligencemachinelearningdeeplearningandbeyond.html [https://perma.cc/RVL7-Q4V5].

the machine what the correct output should be in a given situation.[49] Using the information from this training data, the machine then learns a set of algorithms to be used as a predictive model for other outputs in the future without being explicitly programmed.[50] Machines are not immune from bias, however, and the ability to make accurate predictions can be undermined if the training data the machine originally learned from was flawed.[51]

Algorithmic bias "can emanate from unrepresentative or incomplete training data or the reliance on flawed information that reflects historical inequalities."[52] Implicit biases are pervasive in human beings, and interactions with other social groups can reinforce negative attitudes and strengthen certain stereotypes even unconsciously or indirectly.[53] Since human judgment is required for programming and training data, implicit biases present in humans may creep into the machine's processes and produce biased results.[54]

A. Algorithmic Bias and Classification Accuracy

A growing body of research has demonstrated that FRT exhibits biases which lead to disparities in accuracy rates for different demographic groups and genders.[55] One of the most frequently cited studies identifying the inconsistencies in FRT accuracy rates was conducted in 2018 by researchers Joy Buolamwini from the Massachusetts Institute of Technology and Timnit Gebru from

---

[49] Nicol Turner Lee et al., *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms*, BROOKINGS INST. (May 22, 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/ [https://perma.cc/QCH6-TPJ4].

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] Jerry Kang, *Communications Law: Bits of Bias, in* IMPLICIT BIAS ACROSS THE LAW 132, 144–45 (Justin Levinson & Robert Smith eds., 2012).

[54] ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING 122 (2017).

[55] William Crumpler, *The Problem of Bias in Facial* Recognition, CTR. STRATEGIC & INT'L STUD. (May 1, 2020), https://www.csis.org/blogs/technology-policy-blog/problem-bias-facial-recognition [https://perma.cc/6H5G-5ZA3].

Microsoft.[56] In their research, Buolamwini and Gebru revealed that gender classification algorithms–which are distinct from but related to facial recognition algorithms–in three commercially available facial recognition software systems had error rates of just one percent for white men but almost thirty-five percent for women of color.[57] The most significant factor contributing to bias in FRTs is the selection of training data–one frequently used data set is estimated to be more than seventy-five percent male and more than eighty-percent white.[58] "If algorithms are trained on datasets that contain very few examples of a particular demographic group, the resulting model will be worse at accurately recognizing members of that group in real world deployments."[59]

The National Institute of Standards and Technology ("NIST"), a nonregulatory agency within the U.S. Department of Commerce, conducted an independent assessment of the accuracy of FRTs in 2019 and analyzed how facial recognition algorithms from ninety-nine distinct developers performed on faces of different demographics.[60] The assessment confirmed the results of previous research, ultimately finding widespread inconsistencies in accuracy rates across race, sex, and age.[61] Facial recognition algorithms were generally successful in correctly identifying middle-aged white men, whereas the algorithms performed worse on people of color,

---

[56] *See generally* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROCS. ON MACH. LEARNING RSCH. 1, 3–12 (2018) (examining bias in and accuracy of gender classification algorithms).

[57] *Id.* at 9; Crumpler, *supra* note 55.

[58] Crumpler, *supra* note 55; Steve Lohr, *Facial Recognition Is Accurate, if You're a White* Guy, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html [https://perma.cc/VWH4-REUX].

[59] Crumpler, *supra* note 55.

[60] *See* PATRICK GROTHER ET AL., FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 1 (Nat'l Inst. Standards & Tech ed., 2019).

[61] Lauren Chambers, *Five Fast Facts from the Federal Study of Demographic Bias in Facial Recognition*, PRIV. SOS (Feb. 3, 2020), https://privacysos.org/blog/five-fast-facts-from-the-federal-study-of-demographic-bias-in-facial-recognition/ [https://perma.cc/9HMW-KN6G].

women, children, and the elderly.[62] Indeed, the study again found that the error rates were highest for women of color.[63] It inevitably follows that an increased risk of misidentification places a person of color at an increased risk of becoming entangled in a misplaced police investigation and left to deal with the resulting consequences.

B. Historic Discrimination in Policing

While the source of racial bias in FRT is apparent in classification accuracy, disparities are also present in the technology's utilization.[64] Throughout history into present day, discriminatory police practices in the United States have disproportionately impacted people of color.[65] In fact, such practices have origins directly linked to the preservation of slavery in the 18th century.[66] In the South, for example, the primary policing institution at the time consisted of "slave patrols," which were tasked with tracking down escaped slaves and preventing revolts.[67] This discrimination has persisted over the years, as data overwhelmingly demonstrates that Black Americans are far more likely to be stopped and arrested for a variety of crimes than white people are.[68]

The War on Drugs in the mid-1980s provides a salient example: "[r]elative to their numbers in the general population and among

---

[62] 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/ [https://perma.cc/CX6M-BBUY].

[63] *Id.*

[64] Alex Najibi, *Racial Discrimination in Face Recognition Technology*, HARV. UNIV. (Oct. 24, 2020), http://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ [https://perma.cc/NR8M-QLBM].

[65] *See* Olivia B. Waxman, *How the U.S. Got Its Police Force*, TIME (May 18, 2017, 9:00 AM) https://time.com/4779112/police-history-origins/ [https://perma.cc/F9DF-9RSN].

[66] *Id.*

[67] *See id.*

[68] *See generally* Radley Balko, *There's Overwhelming Evidence that the Criminal Justice System is Racist. Here's the Proof.*, WASH. POST (June 10, 2020), https://www.washingtonpost.com/graphics/2020/opinions/systemic-racism-police-evidence-criminal-justice-system/#Misdemeanors [https://perma.cc/7LGJ-366N] (summarizing various studies that show disparities in treatment and evidence of systemic racism in the United States' criminal justice system).

drug offenders, [B]lack Americans are disproportionately arrested, convicted, and incarcerated on drug charges."[69] Police practices in recent years, like stop-and-frisk, have perpetuated this discrimination and disproportionately targeted Black and Latino communities as well.[70] As a result of increased arrests, Black people are significantly overrepresented in the mugshot databases that law enforcement rely on for facial recognition.[71] "The Black presence in such systems creates a feed-forward loop whereby racist policing strategies lead to disproportionate arrests of Black people, who are then subject to future surveillance."[72]

C. Continuous Monitoring of Black Communities

Even if algorithmic biases are addressed and FRT was somehow equally accurate for all races, Black people have been subjected to constant and focused surveillance for centuries.[73] Lantern laws, for example, were a class of statutes in 18th century New York City that required people of color to carry candle lanterns on their person to remain publicly visible if they were outside after dark and not in the company of a white person.[74] Traces of lantern laws have been connected to modern day police practices as well.[75] New York Police Department's ("NYPD") "Omnipresence," as it has been dubbed by one researcher, refers to the police tactic of positioning high-

---

[69] Jamie Fellner, *Race, Drugs, and Law Enforcement in the United States*, 20 STAN. L. & POL'Y REV. 257, 257 (2009).

[70] Rose Lenehan, *What "Stop-and-Frisk" Really Means: Discrimination & Use of Force*, PRISON POL'Y INITIATIVE (Aug. 17, 2017), https://www.prisonpolicy.org/reports/stopandfrisk.html [https://perma.cc/L8AD-VTBL]. Stop-and-frisk refers to the police tactic of temporarily detaining a pedestrian and patting down the outside of their clothing to determine whether the individual is carrying a weapon. *See* Terry v. Ohio, 392 U.S. 1, 12 (1968).

[71] Najibi, *supra* note 64.

[72] *Id.*

[73] Crockford, *supra* note 62.

[74] Claudia Garcia-Rojas, *The Surveillance of Blackness: From the Trans-Atlantic Slave Trade to Contemporary Surveillance Technologies*, TRUTHOUT (Mar. 3, 2016), https://truthout.org/articles/the-surveillance-of-blackness-from-the-slave-trade-to-the-police/ [https://perma.cc/ECR7-88RE].

[75] R. Joshua Scannell, Electric Light: Automating the Carceral State During the Quantification of Everything 8 (2018) (Ph.D. dissertation, The City University of New York) (on file with author).

intensity floodlights in designated "high crime neighborhoods" that remain illuminated throughout the night.[76] Officers were then physically placed on street corners throughout these neighborhoods, with the ultimate goal of increasing visibility and stopping crime before it starts.[77]

Unsurprisingly, NYPD's Omnipresence was directed at housing projects, which are low-income communities made up almost entirely of people of color.[78] But designation as a "high crime neighborhood" is itself misleading, as policing practices differ significantly by neighborhood and community.[79] Research has "demonstrate[d] that policing is typically more aggressive in neighborhoods that are both economically disadvantaged and populated by a subordinate ethnic minority."[80] Moreover, police surveillance cameras are disproportionately placed in minority communities resulting in constant surveillance that predominantly white communities are not subjected to.[81]

Project Green Light ("PGL") in Detroit, for example, is a surveillance program using facial recognition that installed thousands of cameras at local businesses throughout the city.[82] First implemented in 2016, PGL cameras provide twenty-four-hour surveillance via live feed directly to a "real time crime center" in the police department's headquarters.[83] Officers are then able to run images through Michigan mugshot and driver's license databases,

---

[76] *Id.*

[77] John Surico, *Omnipresence Is the Newest NYPD Tactic You've Never Heard Of*, VICE (Oct. 20, 2014, 1:25 PM), https://www.vice.com/en/article/vdpq7m/omnipresence-is-the-newest-nypd-tactic-youve-never-heard-of-1020 [https://perma.cc/MVH6-2QY6].

[78] *Id.*

[79] Ronald Weitzer & Rod K. Brunson, *Policing Different Racial Groups in the United States*, CPS 2015-2, nr. 25, 129, 136 (2015).

[80] *Id.*

[81] Crockford, *supra* note 62.

[82] Amy Harmon, *As Cameras Track Down Detroit's Residents, a Debate Ensues Over Racial Bias*, N.Y. TIMES (July 8, 2019), https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html [https://perma.cc/VY37-VTEJ].

[83] NOAH URBAN ET AL., A CRITICAL SUMMARY OF DETROIT'S PROJECT GREEN LIGHT AND ITS GREATER CONTEXT 4 (Detroit Community Technology Project ed., 2019).

and "virtually patrol" each PGL location.[84] PGL cameras are not distributed equally, however, and tend to focus surveillance on majority-Black areas while avoiding predominantly white and Asian communities.[85] Detroit represents one of the largest African American populations in the country, as approximately seventy-eight percent of the city's population is Black.[86] This persistent surveillance reflects historical police practices, and "21st century technology advances have made the practice [of continuous monitoring in Black communities] far easier and more widespread."[87] The aforementioned disparities in accuracy rates and current uses of FRT pose significant risks for people of color to be taken advantage of and abused by law enforcement.

IV. NEED FOR FEDERAL LEGISLATION

The impact of bias inherent in FRT and how the technology is utilized is no longer theoretical and has already manifested into very real and tangible harm.[88] The consequences stemming from a mistaken arrest in this context have the potential to affect the victim's future freedom, well-being, relationship with family members, finances, and employment status.[89] Moreover, how the

---

[84] *Id.*; Harmon, *supra* note 82.

[85] Najibi, *supra* note 64.

[86] *QuickFacts, Detroit city, Michigan,* U.S. CENSUS, https://www.census.gov/quickfacts/fact/table/detroitcitymichigan,US/PST045219 [https://perma.cc/CYM8-YPTK].

[87] Andrea Dennis, *Mass Surveillance and Black Legal History*, AM. CONST. SOC'Y (Feb. 18, 2020), https://www.acslaw.org/expertforum/mass-surveillance-and-black-legal-history/ [https://perma.cc/7J7X-SG8Q].

[88] *See* Hill, *supra* note 7.

[89] *See, e.g.,* Melanie Schoenfeld, *Constitutional Amnesia: Judicial Validation of Probable Cause for Arresting the Wrong Person on a Facially Valid Warrant*, 79 WASH. UNIV. L. REV. 1227, 1238 (2001) (establishing that evidence seized in a search incident will not be suppressed even if police arrested the wrong person). *See also* Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/SKY7-VMM4] (discussing impact on family members and employment of individual wrongfully arrested due to false facial recognition match); Rachel Metz, *Beyond San Francisco, More Cities Are Saying No to Facial Recognition*, CNN (July 17, 2019, 5:11 PM), https://www.cnn.com/

police are currently using facial recognition has sparked concerns about the permissible scope of government surveillance in the modern digital age, and how such a practice could violate individuals' constitutional rights.[90] In response, law enforcement agencies argue that there are sufficient procedural safeguards in place to protect against this bias and the resulting consequences, however Part IV(C), *infra*, will examine in more detail how these claimed safeguards do not adequately protect individuals from the harm and misuse of FRT.[91]

A. Tangible Consequences of Mistaken Arrest

A faulty FRT match is not just a minor inconvenience, and an individual might face significant consequences resulting from a mistaken arrest. One such consequence is the possibility that evidence seized in a search incident to arrest will be used against the victim of the misidentification in a future prosecution. Even if it is later established that the wrong person was identified and arrested, police reliance on a facially valid arrest warrant is generally constitutionally acceptable, so long as the mistake was reasonable and supported by probable cause.[92] As such, any fruits of a search incident to the arrest would not be suppressed under the exclusionary rule.[93]

Another possible consequence is a dangerous encounter arising from resisting an unjustifiable arrest–"[p]eople have ended up shot

---

2019/07/17/tech/cities-ban-facial-recognition/index.html [https://perma.cc/Y4M8-4X9G] (detailing physical harm individuals might face).

[90] *See* Natasha Singer & Cade Metz, *Many Facial-Recognition Systems are Biased, Says U.S. Study*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html [https://perma.cc/H5EB-B8G8].

[91] *See* Valentino-DeVries, *supra* note 2.

[92] Schoenfeld, *supra* note 89, at 1238 ("[W]hen the police have probable cause to arrest one person, the subsequent arrest of the wrong person based on a reasonable mistake is constitutionally valid."). *See generally* Hill v. California, 401 U.S. 797, 804–05 (1971) (upholding constitutionality of search incident to arrest of defendant who was mistakenly believed to be the individual for whom the police had an arrest warrant).

[93] *See, e.g.,* United States v. Leon, 468 U.S. 897, 922 (1984) (finding that objectively reasonable reliance on a subsequently invalid search warrant does not justify suppression under the exclusionary rule).

and killed when they're misidentified as a wanted suspect."[94] In 2020, Antonio Arnelo Smith, a Black man from Georgia, had the misfortune of being at the same drug store where police responded to a call that an individual was harassing customers.[95] Mistakenly believing that Mr. Smith had an outstanding warrant, police attempted to take him into custody.[96] Mr. Smith pleaded and cooperated with the officers, attempting to convince them that they had the wrong man, to no avail.[97] Knowing that he did nothing wrong, Mr. Smith slightly resisted but was then body slammed to the ground by the police face first with his arms pinned behind his back.[98] Mr. Smith's wrist was broken in the process, and he was eventually let go after police realized their colossal mistake.[99]

A mistaken arrest might also impact those close to the victim, resulting in traumatic experiences for family members and friends who witnessed the faulty arrest. Robert Williams, for example, was wrongfully arrested for theft based on a flawed match in Detroit's facial recognition system.[100] The police arrested Mr. Williams on his front lawn in the presence of his wife and two young daughters, both of whom were visibly distraught.[101] Not able to fully understand the severity or magnitude of what happened to her father, Mr. Williams' five-year-old daughter began playing "cops and robbers" upon his return, frequently accusing her father of stealing items around the house and attempting to "lock him up" in the living room.[102] Mr. Williams and his wife contemplated whether their daughters would need therapy and still consider the entire experience humiliating.[103]

---

[94] Metz, *supra* note 89.

[95] Russ Bynum, *Officer Denies Wrongdoing in Violent Takedown of Wrong Man*, ABC NEWS (Aug. 19, 2020, 4:14 PM), https://abcnews.go.com/US/wireStory/officer-denies-wrongdoing-violent-takedown-wrong-man-72475995 [https://perma.cc/5BJ2-DJY5].

[96] *Id.*

[97] *Id.*

[98] *Id.*

[99] *Id.*

[100] Hill, *supra* note 89.

[101] *Id.*

[102] *Id.*

[103] *Id.*

A mistaken arrest can also negatively impact one's employment status and finances. For instance, arrestees can be subject to lengthy interrogations and may spend considerable time in detention, rendering them unavailable to work. Mr. Williams in the above example initially decided to conceal the arrest from his employer, citing a "family emergency" as the reason why he missed work and broke his four-year record of perfect attendance.[104] In another example, a Texas man named Eduardo Lopez who was mistakenly arrested for felony hit-and-run was fired from his job as a contractor and forced to drain his personal savings in order to post bail.[105] Mr. Lopez said that the police ruined his life, drastically changing it in a matter of minutes.[106] The consequences stemming from a false match and arrest are real and substantial, and individuals are left to pick up the pieces on their own if and when they are eventually released.

B. Fourth Amendment Considerations

Of particular concern for many citizens is the possibility that police will use FRT to track their whereabouts in public for an extended period of time in violation of their constitutional rights.[107] Generally, government observation of public activities is not considered a "search" and does not implicate the Fourth Amendment, which protects against unreasonable searches and seizures, because individuals have a reduced expectation of privacy in public locations.[108] As such, under a traditional reading, police use

---

[104] *Id.*

[105] Fares Sabawi, *'Ruined my Life:' Man Wrongfully Arrested by San Antonio Police Lost Job, Savings*, KSAT (Dec. 22, 2020, 2:45 PM), https://www.ksat.com/news/local/2020/12/18/ruined-my-life-man-wrongfully-arrested-by-sapd-lost-job-savings/ [https://perma.cc/AG8K-K5B3].

[106] *Id.*

[107] Singer & Metz, *supra* note 90 ("Civil liberties experts, however, warn that the technology – which can be used to track people at a distance without their knowledge – has the potential to lead to ubiquitous surveillance, chilling freedom of movement and speech.").

[108] U.S. CONST. amend. IV; Katz v. United States, 389 U.S. 347, 351 (1967); KELSEY Y. SANTAMARIA, CONG. RSCH. SERV., R46541, FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT: SELECT CONSTITUTIONAL CONSIDERATIONS 12 (2020).

of FRT to monitor the activities of individuals in public may not violate the Fourth Amendment.[109] However, as emerging technologies have facilitated government surveillance and allowed for more continuous monitoring, the Supreme Court has indicated a willingness to reexamine how the Fourth Amendment applies to new digital technologies.[110]

In *United States v. Jones*,[111] the Supreme Court condemned police use of a Global Positioning System ("GPS") to track the public movements of an individual over a period of twenty-eight days, holding that the continuous surveillance without a warrant violated the Fourth Amendment.[112] Concurring in the judgment, Justice Alito noted that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[113] Similarly in *Carpenter v. United States*,[114] the Supreme Court held that allowing the government access to cell-site location information, which provides location points cataloguing the user's physical movements, violated the Fourth Amendment and was unreasonable without a warrant.[115] In so holding, the Court stated that "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere," and that access to locational data "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[116]

The decisions in *Jones* and *Carpenter* are suggestive of the Court's intent to prevent long-term surveillance without a warrant. Although the Fourth Amendment's application to FRT remains largely unsettled, the Court in recent years has adopted a more privacy-conscious approach to new digital surveillance technologies, especially given how pervasive such technologies

---

[109] *See* SANTAMARIA, *supra* note 108, at 11–12.

[110] Andrew Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 101, 124–25 (2020).

[111] 565 U.S. 400 (2012).

[112] *Id.* at 404.

[113] *Id.* at 430 (Alito, J., concurring).

[114] 138 S. Ct. 2206 (2018).

[115] *Id.* at 2219.

[116] *Id.* at 2217 (quoting Jones, 565 U.S. at 415 (Sotomayor, J., concurring)).

have become in modern society.[117] Law enforcement's ability to search FRT databases and retroactively piece together a target's movements in public are similar to the actions of the government that were condemned in *Carpenter*. The relative ease of mass surveillance now warrants some form of judicial supervision and heightened privacy interests for individuals, regardless of whether the surveillance is of activities conducted in public.

C. Claimed Procedural Safeguards Are Insufficient

A common reassurance in defense of FRT is that there are sufficient procedural safeguards in place to protect against bias because a positive facial identification is to be used by the police as "an investigative lead only and is not probable cause for arrest."[118] Indeed, this assertion is supported in many law enforcement guidelines on FRT use[119] and has generally not been accepted by courts as sufficient enough to supply probable cause.[120] However, police are not transparent in how they employ facial recognition, and law enforcement agencies often deny requests for information or fail to disclose their policies to the public.[121] Moreover, many law enforcement agencies are not subject to any sort of review or internal

---

[117] Ferguson, *supra* note 110, at 122–23.

[118] Hill, *supra* note 89.

[119] *See, e.g.*, James O'Neill, *How Facial Recognition Makes You Safer*, N.Y. TIMES (June 9, 2019), https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html [https://perma.cc/Z36Z-9JYE] ("[N]o matter how compelling [the leads are], they must be verified to establish probable cause for an arrest. No one can be arrested on the basis of the computer match alone."). *See also* MICHIGAN STATE POLICE, FACIAL RECOGNITION – FREQUENTLY ASKED QUESTIONS 1 (Sept. 2019), https://www.michigan.gov/documents/msp/Facial_Recognition_FAQ_666807_7.pdf [https://perma.cc/4WCG-WF4Z] ("[A positive identification] is considered to be an investigative lead only, requiring the investigator to continue the criminal investigation before making any final determinations, up to and including arrest.").

[120] *See, e.g.*, People v. Reyes, 69 Misc. 3d 963, 967, 133 N.Y.S.3d 433, 436 (N.Y. Sup. Ct. 2020) ("[A] facial recognition 'match' has never been admitted at a New York criminal trial as evidence that an unknown person in one photo is the known person in another . . . . Facial recognition analysis thus joins a growing number of scientific and near-scientific techniques that may be used as tools for identifying or eliminating suspects, but that do not produce results admissible at a trial.").

[121] Garvie et al., *supra* note 19.

auditing regarding their use of FRT, which removes any mechanism to detect misuse or hold officers accountable.[122]

Further, what limited safeguards are in place can be easily maneuvered around by the police. For example, one way to "verify" an FRT match is to present the returned image in a lineup to an eyewitness for identification.[123] However, a history of suggestive identification procedures and research demonstrate that eyewitness identification is often fallible.[124] Witnesses do not often have ample time to study every intricacy of a perpetrator's face, "and the malleable nature of human memory and visual perception makes eyewitness testimony one of the most unreliable forms of evidence."[125]

In 2019, for example, a twenty-five-year-old Black man from Detroit named Michael Oliver made headlines after he was arrested due to an FRT misidentification.[126] In that case, a teacher called 911 after witnessing a group of students fighting in the parking lot of his school and recorded the encounter on his cell phone until the police arrived.[127] An unidentified man caught on the video then grabbed the phone out of the teacher's hand and subsequently smashed it on the

---

[122] *Id.*

[123] Hill, *supra* note 89 ("In this case, however, according to the Detroit police report, investigators simply included Mr. Williams's picture in a '6-pack photo lineup' they created and showed to [the witness], and she identified him.").

[124] *How Eyewitness Misidentification Can Send Innocent People to Prison*, INNOCENCE PROJECT (Apr. 15, 2020), https://innocenceproject.org/how-eyewitness-misidentification-can-send-innocent-people-to-prison/ [https://perma.cc/YY9X-LJ4G]. Eyewitness misidentification is the leading cause of wrongful convictions according to the Innocence Project, and on a national level, sixty-nine percent of exonerations based on DNA have involved eyewitness misidentification. *Id.*

[125] Greg Hurley, *The Trouble with Eyewitness Identification Testimony in Criminal Cases*, NAT'L CTR. STATE CTS., https://www.ncsc.org/trends/monthly-trends-articles/2017/the-trouble-with-eyewitness-identification-testimony-in-criminal-cases [https://perma.cc/7V8H-HCXE].

[126] Elisha Anderson, *Controversial Detroit Facial Recognition got Him Arrested for a Crime He Didn't Commit*, DET. FREE PRESS (July 11, 2020, 11:42 AM), https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/ [https://perma.cc/T4HC-RLU9].

[127] *Id.*

ground.[128] Detroit police ran the cellphone footage through their facial recognition database which returned a match on Mr. Oliver, who was then arrested for felony larceny despite his innocence.[129] While Mr. Oliver was only the second known person to be falsely arrested based on a faulty facial recognition match, his case demonstrates that this recent problem is starting to have real, devastating effects that the claimed procedural safeguards do not adequately protect against.[130]

After returning as a positive match in the facial recognition database, the police included Mr. Oliver's image in a photo lineup along with other suspects and presented it to the teacher, who positively identified Mr. Oliver as the perpetrator.[131] While there were some similarities in facial features between Mr. Oliver and the actual perpetrator of the crime, there were considerable differences in hair style and body type.[132] Significantly, Mr. Oliver has tattoos all over his arms and hands, whereas the man's skin in the cellphone footage was completely free from tattoos.[133] While it should have been abundantly clear that the facial recognition program and the victim had both identified the wrong person, the supposed procedural safeguards in place did nothing to prevent Mr. Oliver from being falsely accused and arrested of a felony he did not commit.

In their defense to concerns of insufficient transparency, some law enforcement agencies argue that they are not required to disclose their use of facial recognition to accused or arrested individuals, as states differ on what investigative materials must be revealed during litigation.[134] The Supreme Court case *Brady v.*

---

[128] *Id.*

[129] *Id.*

[130] Natalie O'Neill, *Faulty Facial Recognition Led to His Arrest – Now He's Suing*, VICE (Sept. 4, 2020, 9:39 AM), https://www.vice.com/en/article/bv8k8a/faulty-facial-recognition-led-to-his-arrestnow-hes-suing [https://perma.cc/9Q6D-W2X8].

[131] Anderson, *supra* note 126.

[132] *Id.*

[133] *Id.*

[134] Valentino-DeVries, *supra* note 2.

Maryland[135] guides required disclosures in criminal cases.[136] In *Brady*, the Court established that the prosecution must traditionally disclose all exculpatory evidence to the accused upon request, and that failing to do so violates due process.[137] While FRT's classification as "exculpatory evidence" has not yet been cemented, its current treatment in lower courts indicates *Brady* disclosures will not remedy the current procedural safeguards' shortcomings.

Recently, a Florida Appellate Court had the opportunity to consider *Brady's* application to FRT.[138] In *Lynch v. Florida*,[139] a man convicted of selling crack cocaine claimed that the facial recognition system had misidentified him, and argued that the prosecution should have to disclose the other photos that returned as possible matches in the FRT database as part of a *Brady* disclosure.[140] The defendant believed that the other photos would have cast doubt on the prosecution's case, and the State violated *Brady* by failing to share this information.[141] The court in this case held that the prosecution was not required to disclose such information, and the defendant did not meet the burden to prevail under *Brady*.[142] To overcome *Brady*, the defendant would have had to show that the result of the trial would have been different had the State disclosed the other possible matches, which he failed to do.[143] *Lynch* represents one of the only judicial rulings on law enforcement's use of FRT and suggests that a defendant's right to information regarding such practices may be limited.[144] The failed procedural safeguards, paired with the opaque nature of FRT use by law enforcement, further increases distrust between the police and their communities and must be regulated before more harm is done.[145]

---

[135] 373 U.S. 83 (1963).
[136] *Id.* at 83.
[137] *Id.* at 87.
[138] *See* Lynch v. Florida, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018).
[139] *Id.*
[140] *Id.* at 1168.
[141] *Id.* at 1169–70.
[142] *Id.* at 1170.
[143] *Id.*
[144] Valentino-DeVries, *supra* note 2.
[145] *See, e.g.*, Klosowski, *supra* note 12 ("When the public doesn't know how these facial recognition systems work or how accurate they are, the public doesn't

V. CURRENT FRT REGULATION AND PROPOSED GUIDELINES

As an understanding of the harmful consequences of FRT becomes more prevalent, and in the absence of any national law or policy, some lawmakers at the state and local level have enacted legislation to address and regulate law enforcement's use of FRT.[146] However, lawmakers have struggled to determine which regulations to implement due to the often competing viewpoints on FRT use.[147] On one hand, many law enforcement agencies argue that FRT is crucial to ensure public safety and acts as a valuable crime-fighting resource.[148] Admittedly, in cases where FRT has been used appropriately, individuals suspected of violent crimes have been apprehended, victims previously unknown have been identified, and inmates incarcerated due to mistaken witness identification have been cleared.[149] Additionally, the public is generally supportive of FRT use–more than half of Americans trust law enforcement to use the technology responsibly.[150] On the other hand, opponents of FRT

---

know whether these systems are being used appropriately, especially in law enforcement.").

[146] Heilweil, *supra* note 44 ("There is currently no comprehensive federal law governing facial recognition, and some localities have taken up the task themselves of regulating the technology.").

[147] Shira Ovide, *A Case for Facial Recognition*, N.Y. TIMES (Nov. 11, 2020), https://www.nytimes.com/2020/11/11/technology/facialrecognitionsoftwarepolice.html?action=click&module=RelaedLinks&pgtype=Article [https://perma.cc/ATC6-GJBC].

[148] *Id.*

[149] *See* FINKLEA ET AL., *supra* note 1, at 4. *See also* O'Neill, *supra* note 119 (detailing how the N.Y.P.D. used facial recognition to apprehend a man accused of raping a woman); *see also* Kate Conger et al., *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html [https://perma.cc/3AJ4-6HYX].

[150] Aaron Smith, *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, PEW RSCH. CTR. (Sept. 5, 2019), https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/ [https://perma.cc/JE9C-HTF3]. Pew Research Center conducted a representative survey of 4,272 U.S. adults and found that the public is generally accepting of law enforcement's use of facial recognition technology. *Id.* However, the public is less accepting of other entities such as advertisers or tech companies' use of facial recognition technology. *Id.* Moreover, the results varied across different

want strict limitations on how FRT is employed, citing privacy concerns, racial bias, and violations of civil liberties.[151] As such, lawmakers must engage in a careful balancing act when crafting legislation and implementing guidelines in their jurisdictions.

A. Existing FRT Regulation

Due to the lack of any uniform federal regulation, state and local regulation of FRT differs significantly.[152] At the local level, San Francisco became the first major American city to ban the use of FRT by law enforcement and other related agencies.[153] The "Stop Secret Surveillance" ordinance, which was passed in 2019, directly limited the San Francisco Police Department's ability to use FRT and restricted its ability to restart any testing of such tools moving forward.[154] Oakland, California and Somerville, Massachusetts have also implemented similar laws outright banning police use of FRT.[155]

At the state level, lawmakers from California, New Hampshire, and Oregon have enacted legislation that prohibits police from using FRT to analyze footage captured on their body cameras.[156] In July of 2020, the Massachusetts Senate passed an omnibus police reform bill that would have placed a moratorium on police use of FRT until December of 2021 so that an independent commission could review the use of this technology and make recommendations to the legislature.[157] Had the bill passed in the House, Massachusetts would have been the first state in the nation to completely stop, and

---

demographic groups. *Id.* For example, younger adults were generally less accepting than older adults, and smaller shares of Black and Hispanic adults than white adults believed law enforcement use of FRT was acceptable. *Id.*

[151] Valentino-DeVries, *supra* note 2.

[152] Ng, *supra* note 18 ("The US has no federal regulations on facial recognition, leaving thousands of police departments to determine their own limits.").

[153] Conger et al., *supra* note 149.

[154] Shirin Ghaffary, *San Francisco's Facial Recognition Technology Ban, Explained*, VOX (May 14, 2019, 7:06 PM), https://www.vox.com/recode/2019/5/14/18623897/san-francisco-facial-recognition-ban-explained [https://perma.cc/AX43-BLPM].

[155] *See* Miller, *supra* note 40.

[156] *Id.*

[157] S.B. S.2800 § 65(b), (c) (Mass. 2020).

potentially ban, law enforcement use of FRT.[158] After months of debate and hearings, however, Massachusetts lawmakers compromised on a police reform bill that did not ban use of facial recognition but instead imposed limitations on how the police may use the technology.[159] For example, Massachusetts police are now required to submit a written request to the appropriate authority before conducting facial recognition searches, document each individual search, and publish data regarding the total number of searches.[160]

Similar to Massachusetts, some jurisdictions have permitted use of FRT but implemented guidelines or restrictions for law enforcement to navigate.[161] The Board of Police Commissioners in Detroit, for example, heard months of testimony from the community before endorsing police use of FRT, subject to numerous guidelines.[162] One such guideline requires the appointment of a Local Agency Security Officer ("LASO") working within the law enforcement's Technical Services department to "[o]versee[] and administer[] the facial recognition program to ensure compliance with applicable laws, regulations, standards, and policy."[163] In addition, the Detroit Police Department is prohibited from using FRT on any type of video, cannot use the technology to identify individuals at protected First Amendment events, like protests, and is limited to using FRT only for violent crime or home invasion investigations.[164] By limiting FRT to still images, Detroit police no

---

[158] Adrianna Appel, *Massachusetts Could Become First State to Ban Facial Recognition*, BLOOMBERG L. (July 8, 2020, 3:05 PM), https://news.bloomberglaw.com/tech-and-telecom-law/facial-recognition-ban-in-massachusetts-set-for-senate-approval [https://perma.cc/PFV2-DKNV].

[159] *See* S.B. 2963, 191st Gen. Ct. § 26 (Mass. 2020).

[160] *Id.* at §§ 220(b), (c), (d) (2020).

[161] *See* Erin Einhorn, *Detroit Police Can Keep Using Facial Recognition – With Limits*, NBC NEWS (Sept. 19, 2019, 7:24 PM), https://www.nbcnews.com/news/us-news/detroit-police-can-keep-using-facial-recognition-limits-n1056706 [https://perma.cc/YH8U-X8AY].

[162] *Id.*

[163] DET. POLICE DEP'T, PLAN., RSCH. & DEPLOYMENT DEP'T., REVISED FACIAL RECOGNITION DIRECTIVE 5 (Sept. 12, 2019).

[164] *Id.*

longer have access to real time video streams previously available under the city's PGL program.[165]

Similarly, in June of 2020, Governor Jay Inslee of Washington state signed a bill regulating police use of FRT.[166] The law requires the police to first secure a warrant before using facial recognition for "ongoing surveillance or real-time identification," and requires government agencies who wish to use FRT to first give public notice followed by a published report "outlining the technology's potential impact on civil liberties."[167] Washington's policy is widely regarded as "one of the most comprehensive laws governing the use of facial recognition by government" to date.[168]

B. Proposed Federal Legislation

Despite the exceptions above, most states and local governments have been slow to enact guidelines regarding the use of FRT, leaving police use of the technology largely unregulated in most of the country.[169] While a total ban or moratorium on FRT is not necessary to combat its current flaws, Congress must implement specific regulations governing law enforcement's use of FRT at the federal level. In the absence of such a law right now, law enforcement agencies currently remain free to "police" themselves with minimal accountability, and the individual protections afforded to citizens are ultimately determined by the area in which they reside.[170] A comprehensive law regulating FRT will provide guidance to police

---

[165] Einhorn, *supra* note 161.

[166] S.B. 6280, 66th Leg., Reg. Sess. (Wash. 2020).

[167] Sascha Matuszak, *Washington State Enacts Regulations on Facial Recognition Technology*, JD SUPRA (June 12, 2020), https://www.jdsupra.com/legalnews/washington-state-enacts-regulations-on-67156/ [https://perma.cc/5USW-CLFA].

[168] Pam Greenberg, *Facial Recognition Gaining Measured Acceptance*, NAT'L CONF. OF STATE LEG. (Sept. 18, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/facial-recognition-gaining-measuredacceptancemagazine2020.aspx [https://perma.cc/7J9A-DV8S].

[169] *See* Susan Crawford, *Facial Recognition Laws Are (Literally) All Over the Map*, WIRED (Dec. 16, 2019, 8:00 AM), https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/ [https://perma.cc/PZ3D-AEBW].

[170] *See id.*

departments while protecting citizens' privacy and liberties.[171] Such a law should require increased transparency, address racial biases, prohibit long-term surveillance without a warrant, and limit the databases from which law enforcement can run facial recognition searches.

1. Transparency

As previously discussed, police use of FRT suffers from a lack of transparency, both in the algorithms that comprise the technology and how it is deployed.[172] Insufficient transparency consequently sows distrust in members of the public and supports the narrative that FRT is creating a surveillance state with no discernable protections for individual privacy.[173] Any legislation Congress passes should require law enforcement agencies to make available to the public the specific ways in which FRT is being implemented, including where the images come from, how the images are found, which databases are used, and how frequently FRT is employed. "Citizens do not necessarily need information about the mathematical formula underlying the algorithm but do need explanation about why the algorithm is being used and what mechanisms exist to hold the creators accountable."[174]

Similar to Washington's policy, federal legislation should require notice to the public regarding law enforcement's intent to use FRT, community meetings allowing for public input, and published reports outlining potential impacts. Since police are currently not required to disclose their use of this technology, and often do not make such disclosures, many suspects arrested are not even aware that FRT was used in their apprehension.[175] Although

---

[171] *Id.*

[172] FERGUSON, *supra* note 54, at 136–37.

[173] Mazin Hussain, *Facial Recognition & The Surveillance State. Big Tech's New Export.*, MEDIUM (June 14, 2020), https://medium.com/digital-diplomacy/facial-recognition-the-surveillance-state-big-techs-new-export-ebcdc50d5e95 [https://perma.cc/YGC5-4668].

[174] FERGUSON, *supra* note 54, at 137.

[175] *See, e.g.*, Ng, *supra* note 18 ("[Robert] Williams didn't know that Detroit police used facial recognition to find him, until an investigator mentioned the detail during their conversation. Attorneys representing protesters in Miami didn't know that police used facial recognition in their arrests, according to an NBC

expectations of privacy are reduced in public, knowledge that police are actually using FRT as an investigative method allows for more cautious consideration of one's actions and may allow for individuals to change their behavior accordingly.

Moreover, if police are aware that information regarding the frequency and extent to which FRT is used will be publicly available, they might be more careful before misusing or abusing such technology. Public pressure has been the impetus for much police reform. For example, public outrage in 2014 following the death of Michael Brown at the hands of the police in Ferguson, Missouri convinced many law enforcement agencies to adopt body cameras as a means of rebuilding public trust, promoting accountability, and minimizing the risk of deadly police encounters.[176] Research on the benefits of body cameras worn by law enforcement established some success in achieving these objectives, finding that incidents of excessive force and complaints against police departments both decreased significantly after installing body cameras on officers.[177]

While heightened disclosure and transparency will not completely eradicate police misconduct, these principles can illuminate the horrific actions of some officers and provide a measure of greater accountability.[178] In some cases, officers have been fired or indicted for their misconduct, and the disclosure of

---

Miami report. Police used facial recognition software in a $50 drug dealing case in Florida in 2016 but made no mention of it in the arrest report.").

[176] Mary D. Fan, *Privacy, Public Disclosure, Police Body Cameras: Policy Splits*, 68 ALA. L. REV. 395, 409–10 (2016).

[177] *Id.* at 410–11. The research here is from select police departments. There is much disagreement about whether disclosure of body camera footage has made any significant impact on reducing police brutality. *See* Cynthia Lum et al., *Body-worn Cameras' Effects on Police Officers and Citizen Behavior: A Systematic Review*, 16 CAMPBELL SYSTEMATIC REVS. 1, 21 (2020) (discussing a metanalysis on the effects of body cameras on police officer behavior, ultimately finding "substantial uncertainty regarding the effectiveness of [body worn cameras] in reducing [police] use of force").

[178] *See, e.g.*, Kate Brumback, *Body-camera Review Leads to Firing of 2 Atlanta Officers*, DETROIT NEWS (June 1, 2020, 3:57 PM), https://www.detroitnews.com/story/news/nation/2020/06/01/body-camera-review-leads-firing-atlanta-officers/111893092/ [https://perma.cc/9HS5-63TB].

body camera footage was instrumental in achieving that outcome.[179] So, even if increased transparency will not entirely eliminate police misuse of FRT, it may keep officers honest in the way they employ the technology and facilitate accountability if officers continue to abuse the technology.

2. Address Racial Biases

Any meaningful legislation governing FRT must address the racial biases that currently plague the technology.[180] In order to address algorithmic bias, the training data that FRTs learn from must include a more diverse set of faces that are representative of Americans.[181] Along these lines, training data sets should reflect an intersectional approach–that is, not only include faces consisting of different races, but also take into consideration various ages and genders.[182] To ensure compliance from law enforcement, federal legislation "should establish testing requirements, standard-setting, and certification mechanisms [which would serve] to prevent the deployment of biased facial recognition systems."[183] Such minimum standards might be established by a neutral agency such as the NIST, which could review facial recognition systems and test them for accuracy and propensity for bias.[184] Any proposed legislation should require approval from a neutral, independent agency before a law enforcement agency could deploy FRT.

---

[179] *See, e.g.*, *id.* ("Mayor Keisha Lance Bottoms . . . decided to fire two officers and place three others on desk duty pending further investigation after reviewing body-camera footage . . . . [that] showed a clear use of force.").

[180] Najibi, *supra* note 64.

[181] Isabella Garcia, *Can Facial Recognition Overcome Its Racial Bias?*, YES! MAG. (Apr. 16, 2020), https://www.yesmagazine.org/social-justice/2020/04/16/privacy-facial-recognition/ [https://perma.cc/M6YH-C49J].

[182] *See* Najibi, *supra* note 64.

[183] Sam duPont, *Facial Recognition Is Here but We Have No Laws*, NEXTGOV (July 8, 2020), https://www.nextgov.com/ideas/2020/07/facial-recognition-here-we-have-no-laws/166711/ [https://perma.cc/D4TD-DVRJ].

[184] *Standardization Coordination*, NAT'L. INST. OF STANDARDS & TECH., (Nov. 15, 2019), https://www.nist.gov/standardsgov/what-we-do/standardization-coordination [https://perma.cc/6YME-R66F]. The NIST assists federal agencies by "identif[ing] relevant standards development organizations, catalyz[ing] or foster[ing] development of needed standards, and driv[ing] the development of technical standards critical to national goals." *Id.*

Congressional legislation should also require human review and several layers of approval within each police department to ensure that there is adequate justification for the use of FRT. Additionally, police departments should be required to appoint an individual responsible for maintaining compliance with the aforementioned standards, similar to the appointment of a LASO in Detroit.[185] Doing so provides a measure of internal oversight within police departments, and adds a layer of accountability if the standards and guidelines are not being followed.

Federal legislation should also prohibit police surveillance cameras from being installed only in communities comprised mainly of minorities, like PGL in Detroit. For too long, continuous monitoring has been directed primarily at Black communities and as such, FRT surveillance and data collection must be applied equally throughout a police department's jurisdiction or not at all. Part V(B)(4), *infra*, will discuss in more detail how the problem of overrepresentation in mugshot databases can be mitigated, which is crucial to addressing the racial bias that accompanies FRT in the law enforcement context.

No single law passed by Congress can address and completely resolve the history and impact of discriminatory policing in the United States. Laws that are facially neutral operate on the mistaken assumption of racial neutrality, forgetting that "contemporary color barriers are less visible but neither less real nor less oppressive."[186] Discriminatory policing is a systemic problem, and one that will require immense effort to unravel and meaningfully change. However, federal legislation that addresses the main areas where bias currently creeps into law enforcement use of FRT is an important step in the right direction.

3. Prohibit Long-Term Surveillance Without a Warrant

Although it is currently unclear whether law enforcement's use of FRT raises Fourth Amendment protections, Congress has the ability to enact legislation that offers more protection to individuals

[185] Einhorn, *supra* note 161.
[186] Derrick Bell, *Racial Realism*, 24 CONN. L. REV. 363, 374 (1992).

than does the Constitution.[187] Federal legislation governing law enforcement's use of FRT should include a warrant requirement for long-term surveillance to address the current gray area in facial recognition jurisprudence. Senators Chris Coons and Mike Lee tried to limit the use of FRT by federal agencies in 2019 by introducing the Facial Recognition Technology Warrant Act.[188] The bipartisan bill would have "require[d] federal law enforcement to obtain a warrant based upon a showing of probable cause . . . in order to utilize facial recognition technology for the purpose of ongoing public surveillance of an individual" or group of individuals in a public space.[189] The proposed bill further limited surveillance to a period of thirty days and required reports disclosing to the public the nature and frequency of warrant applications made by law enforcement.[190] The bill ultimately died in Congress and did not receive a vote before the end of the session.[191]

In addition, there should also be an exhaustion provision which would require the government to demonstrate that other less intrusive means of surveillance have already failed, are likely to fail,

---

[187] *See* RICHARD M. THOMPSON II & JARED P. COLE, CONG. RSCH. SERV., R44036, STORED COMMUNICATIONS ACT: REFORM OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 1 (2015). *See also* 18 U.S.C. §§ 2703(1)(3), 2703(a) (2018). In 1986, for example, Congress noticed that applicable Fourth Amendment jurisprudence did not adequately protect individuals who entrusted the security of their online information to Internet Service Providers ("ISPs"). THOMPSON & COLE, *supra* note 187, at 1. Congress combatted this issue by passing the Stored Communications Act, which prohibited ISPs from voluntarily disclosing electronic communications to the government or other entities, and additionally permitted the government to require disclosure from ISPs only pursuant to a warrant. *Id.* By legislative action, Congress essentially created additional Fourth Amendment protections for individuals regarding their electronic communications that did not exist prior. *Id.*

[188] S. 2878, 116th Cong. § 4(a), (b) (2019).

[189] Press Release, Chris Coons, Facial Recognition Tech: Sens. Coons, Lee Bill Requires Court Orders for Law Enforcement use of Facial Recognition Technology (Nov. 14, 2019), https://www.coons.senate.gov/news/press-releases/facial-recognition-tech-sens-coons-lee-bill-requires-court-orders-for-law-enforcement-use-of-facial-recognition-technology [https://perma.cc/REQ6-N4GH].

[190] S. 2878 § 4(a), (b).

[191] Facial Recognition Technology Warrant Act of 2019, S. 2878, 116th Cong. (2019).

or are too dangerous to attempt.[192] Implementing such a requirement would provide a measure of restraint for law enforcement and ensures that continuous monitoring of civilians does not become routine. As such, using FRT for ongoing surveillance would become a method of last resort rather than the first action taken.

Federal legislation should also carve out specific prohibitions on FRT use. For instance, the law should prohibit the use of FRT at protected First Amendment events, irrespective of any applications for a warrant. Amid the social justice movement that erupted throughout the country in the summer of 2020, it was revealed that the NYPD used facial recognition software to track down Black Lives Matter activists participating in the protests.[193] The Federal Bureau of Investigation ("FBI") has a long history of surveilling Black activists and has used this tactic to disrupt the civil rights movement and discredit its leaders.[194] "Awareness that the Government may be watching chills associational and expressive freedoms," and law enforcement should not be permitted to use FRT to identify individuals at protests or religious events.[195] Implementing a warrant requirement for long-term surveillance provides meaningful judicial supervision to a questionable police practice and can, at the very least, serve as a limitation to continuous police surveillance.

4. Redefine Searchable Databases

Finally, Congressional legislation must limit the databases from which law enforcement run can facial recognition searches.

---

[192] *See, e.g.*, 18 U.S.C. § 2518(1)(c) (2019) (requiring the government to include a statement detailing other investigative procedures tried first before the court will authorize a wiretap of electronic communication).

[193] James Vincent, *NYPD Used Facial Recognition to Track Down Black Lives Matter Activist*, THE VERGE (Aug. 18, 2020, 5:26 AM), https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram [https://perma.cc/CK2B-9U8U].

[194] Michael German, *The FBI Targets a New Generation of Black Activists*, BRENNAN CTR. FOR JUST. (June 26, 2020), https://www.brennancenter.org/our-work/analysis-opinion/fbi-targets-new-generation-black-activists [https://perma.cc/GX4A-LNRN].

[195] United States v. Jones, 556 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

Currently, twenty-one states allow law enforcement access to driver's license databases, and over 2,400 law enforcement agencies use Clearview AI's facial recognition software.[196] These databases grant police access to billions of images of individuals, the majority of whom have never committed a crime nor consented to being included in such a database.[197] As such, federal legislation should limit police access to mugshot databases only and prohibit access to databases of DMV records or private facial recognition companies.

Moreover, any individual who was found innocent or whose charges were dropped should be excluded from mugshot databases. An estimated seventy million Americans have a criminal record, however only about twenty million of those Americans were actually convicted of felonies.[198] The remaining individuals were either convicted of a misdemeanor, never charged, had their charges dismissed, or were not convicted.[199] "Even the briefest minor interaction with the justice system can leave someone with a criminal record" and consequently, included in police records for life.[200] Congressional legislation should require law enforcement to update their databases every month, purging the criminal records of those who have been acquitted or exonerated. This requirement minimizes the chance that a law-abiding citizen will become entangled in a police investigation or wrongfully arrested due to a faulty facial recognition match.

Further, legislation should also prohibit law enforcement from including individuals who were convicted of minor misdemeanors in the mugshot database for FRT searches. It is important to note that Black people are still significantly overrepresented in mugshot databases, and the requirements in the proposed law will not change this fact. However, misdemeanors represent eighty percent of all arrests, and these minor criminal offenses are how a vast majority

---

[196] Miller, *supra* note 40; Lyons, *supra* note 47.

[197] Elinson, *supra* note 38.

[198] Tina Rosenberg, *Have You Ever Been Arrested? Check Here*, N.Y. TIMES (May 24, 2016), https://www.nytimes.com/2016/05/24/opinion/have-you-ever-been-arrested-check-here.html [https://perma.cc/5RJ2-Q6WS].

[199] *Id.*

[200] *Id.*

Black people become involved with the criminal justice system.[201] By excluding low-level misdemeanor convictions and individuals acquitted or exonerated from mugshot databases, the disproportionate impact on people of color can begin to be mitigated, even if not wholly corrected.

5. Enforcement at the State and Local Level

Initially, congressional legislation that encompasses these suggestions would only be binding on federal law enforcement agencies (e.g., FBI, ICE, DEA) but not on state and local agencies.[202] One way to apply federal regulation to states and municipalities would be to withhold federal grant funding.[203] In *South Dakota v. Dole*,[204] the Supreme Court upheld a statute under Congress' spending power that withheld federal highway funds from states that did not raise the minimum age to purchase alcohol to twenty-one years old.[205] As such, under the Spending Clause, Congress has the authority to condition the receipt of federal funding on compliance with specified conditions or restrictions that "encourage a State to regulate in a particular way and influence a State's policy choices."[206]

The Congressional spending power is not unlimited, however, and any conditions or restrictions imposed must be (1) in pursuit of the general welfare, (2) unambiguous, (3) related to a federal interest, and (4) in compliance with other Constitutional

---

[201] Christianna Silva, *Law Professor on Misdemeanor Offenses and Racism in the Criminal Justice System*, NPR (June 12, 2020, 7:19 PM), https://www.npr.org/sections/live-updates-protests-for-racial-justice/2020/06/12/876221163/law-professor-on-how-misdemeanors-sweep-blacks-into-the-criminal-system [https://perma.cc/VB8H-BY3H].

[202] NATHAN JAMES & BEN HARRINGTON, CONG. RSCH. SERV., IF10572, WHAT ROLE MIGHT THE FEDERAL GOVERNMENT PLAY IN LAW ENFORCEMENT REFORM? 1 (2020) ("The U.S. Constitution established a federal government of limited powers. A general police power is not among them. That authority is largely reserved for the states.").

[203] FINKLEA ET AL., *supra* note 1, at 12.

[204] 483 U.S. 203 (1987).

[205] *Id.* at 205.

[206] *See* U.S. CONST., art. I, § 8, cl. 1; Nat'l Fed'n of Indep. Bus. v. Sebelius, 567 U.S. 519, 576, (2012).

provisions.[207] Moreover, the financial inducement offered by Congress must not be "so coercive as to pass the point at which 'pressure turns into compulsion.'"[208] Spending Clause programs do not run the risk of impermissible coercion "when a State has a legitimate choice whether to accept the federal conditions in exchange for federal funds."[209]

There are two major federal programs that currently provide federal funding to the states for a variety of police initiatives. The Edward Byrne Memorial Justice Assistance Grant ("JAG") Program allocates federal funding to all fifty states for a "variety of state and local criminal justice initiatives."[210] Similarly, the Community Oriented Policing Services ("COPS") program provides federal grant funding and resources to the states to hire new law enforcement officers and procure new equipment and technology."[211] The JAG program allocates an estimated $435 million and the COPS program allocates around $304 million to state and local law enforcement agencies each year.[212] Leveraging its spending power, Congress could condition the receipt of such funding on compliance with the guidelines and regulations described in the proposed legislation.[213] The funding condition must be clear and unambiguous, would certainly be for the general welfare and related to a federal interest, and likely would not violate any other Constitutional provisions, therefore not exceeding of the limitations of the Spending Clause.

Moreover, the inducement here could be crafted in a way to avoid impermissible coercion that would exceed Congress'

---

[207] Dole, 483 U.S. at 207–08.

[208] *Id.* at 211 (quoting Charles C. Steward Mach. Co. v. Davis, 301 U.S. 548, 590 (1937)).

[209] Sebelius, 567 U.S. at 578.

[210] NATHAN JAMES, CONG. RSCH. SERV., IF 10691, THE EDWARD BYRNE MEMORIAL JUSTICE ASSISTANCE GRANT (JAG) PROGRAM (2021).

[211] NATHAN JAMES, CONG. RSCH. SERV., IF 10922, COMMUNITY ORIENTED POLICING SERVICES (COPS) PROGRAM (2021).

[212] Nathaniel Lee, *Here's How Two Federal Programs Helped Expand Police Funding by Over 200% Since 1980*, CNBC (June 25, 2020, 11:16 AM), https://www.cnbc.com/2020/06/25/two-federal-programs-helped-expand-police-funding-by-over-200percent.html [https://perma.cc/EL7X-UUSS].

[213] Sebelius, 567 U.S. at 537.

spending power. The Supreme Court has not specified an exact threshold as to when pressure turns into compulsion, but has generally been reluctant to a find a condition unconstitutionally coercive.[214] In *Dole*, withholding five percent of federal highway funds, which represented less than half of one percent of South Dakota's budget at the time, was considered to be a "relatively mild encouragement" and an acceptable use of the spending power.[215] In *N.F.I.B. v. Sebelius*,[216] however, Congress threatened to withhold over ten percent of a state's overall budget if they failed to participate in the Medicaid expansion, "leav[ing] the States with no real option but to acquiesce."[217] The financial inducement in *Sebelius*, the Court said, was not a mild encouragement but instead a "gun to the head."[218]

Police budgets vary in size across states, however police spending represents approximately four to six percent of state and local budgets on average across the nation.[219] Despite a significant increase in federal funding for police over the last three decades, policing still comprises a relatively small portion of a typical city's budget.[220] Indeed, "[n]early all state and local spending on police, corrections, and courts was funded by state and local governments because federal grants account for a very small share of these expenditures."[221] As such, it is unlikely that conditioning receipt of JAG or COP funding on compliance with FRT guidelines would constitute a "gun to the head," thereby leaving states without a

---

[214] Patrick Haney, *Coercion by the Numbers: Conditional Spending Doctrine and the Future of Federal Education Spending*, 64 CASE W. RSRV. L. R. 557, 578 (2013). *See* Sebelius, 567 U.S. at 581.

[215] South Dakota v. Dole, 483 U.S. 203, 211 (1987).

[216] 567 U.S. 519 (2012).

[217] *Id.* at 582.

[218] *Id.* at 581.

[219] Tara O'Neill Hays, *Assessing Calls to Defund the Police: Police Budgets and Employment Levels*, AM. ACTION F. (Sept. 29, 2020), https://www.americanactionforum.org/research/assessing-calls-to-defund-the-police-police-budgets-and-employment-levels/ [https://perma.cc/3L3P-JTFH].

[220] *Id.*; Lee, *supra* note 212.

[221] *Criminal Justice Expenditures: Police, Corrections and Courts*, URB. INST. https://www.urban.org/policy-centers/cross-center-initiatives/state-and-local-finance-initiative/state-and-local-backgrounders/criminal-justice-police-corrections-courts-expenditures [https://perma.cc/UZ6P-LRAR].

meaningful choice whether to accept the conditions in exchange for federal funding. The financial pressure from withholding such funds may be persuasive enough to ensure federal regulations are followed at the state and local levels as well.

VI. CONCLUSION

FRT has been around for decades, and there is no indication that it will be disappearing any time soon. While law enforcement agencies use FRT for a variety of investigatory purposes, some of which are legitimate and protect society, police are not transparent in how they currently use this technology. What is more, recent research has established that many FRTs currently used by law enforcement display a demonstrated bias toward people of color, especially women. As such, people of color are at a significant risk of being targeted and negatively impacted by use of facial recognition. Compounding the issue is the fact that police have access to databases containing billions of images of law-abiding citizens, which allows police to keep tabs on millions of people in a way that would have previously been unthinkable, leaving individuals' safety, privacy, and constitutional protections uncertain and at risk. The lack of federal guidelines for police use of FRT ultimately passes the buck to state and local agencies to regulate themselves, which has proved insufficient to protect all citizens.

A comprehensive law must be passed by Congress that addresses the current flaws with FRT and its use by police departments. First, such a law should increase transparency and mandate disclosure to the public as to how FRT is being deployed by the police. Second, the law must address racial biases by requiring independent review of FRTs to ensure the training data sets are representative of Americans, and preventing discriminatory deployment in majority Black communities. Third, the law should impose a warrant requirement for long-term surveillance, addressing the current gray area in Fourth Amendment jurisprudence concerning FRT and providing judicial supervision to a police practice that is of major concern to many citizens right now.

Lastly, the law should severely restrict the databases law enforcement can run facial recognition searches on, allowing access

only to mugshot databases and completely excluding those exonerated or convicted of minor misdemeanors. This law could be enforced at the state and local levels by conditioning the receipt of federal police funding on compliance with the stated guidelines of the legislation. Ultimately, this law will provide guidance to law enforcement agencies, protect civil liberties generally, and reduce FRT's disparate impact on people of color. Facial recognition remains a powerful technology that can have numerous advantages when deployed properly. It is time that Congress establishes standards and guidelines for law enforcement agencies around the country to follow.