RACIAL RECOGNITION

Eldar Haber†

TABLE OF CONTENTS

† Associate Professor, Faculty of Law, University of Haifa; Faculty Member, Center for Cyber, Law and Policy (CCLP) and Haifa Center for Law and Technology (HCLT), University of Haifa. I thank Michael Birnhack, Olga Frishman, Einav Hadas Tamir, Rotem Kadosh Nussbaum, and Jill Presser for their insightful suggestions and comments. I am also grateful to Tomer Antshel, Gabriel Focshaner, Hadar Gilboa, Idan Mor, and Aviv Toby for their excellent assistance in research.

INTRODUCTION

Every human is unique. We all look, sound, and walk differently from one another. These unique physiological and behavioral characteristics could be translated into biometric identifiers. With developments in the intersection between biometric identification and Artificial Intelligence (AI), algorithms are now capable of measuring and analyzing unique human characteristics, such as fingerprints, palm prints, irises, faces, voices, gaits and gestures, typing patterns, and handwriting, for verification and identification purposes.[1] With the rise in computational capabilities, such recognition technology is increasingly used by interested parties to combat terrorism, authenticate flight passengers or identify undocumented migrants at airports, or by the market for various consumer-related purposes, like increasing security or simply making products and services more accessible or enjoyable.[2]

The use of recognition technology for purposes of identification, perhaps most notably facial recognition, has now entered the realm of criminal enforcement. Within their efforts in the prevention, investigation, detection, and prosecution of crimes, law enforcement agencies on both the federal and state levels began using facial recognition technology early in the twenty-first century.[3] With further advancements in the field of AI, such use has quickly spread across police departments in America.[4] When attempting to identify culprits, police officers, including federal agents, are now positioned to feed an algorithm with a suspect's image, which can be matched against databases containing images of individuals and would then produce a list of potential matches.[5]

While the use of recognition technology by law enforcement agencies is likely an important tool for maintaining public safety and

---

1 It is important to differentiate between verification and identification. While *verification* is used to confirm one's claimed identity (one-to-one comparison), *identification* refers to identifying an unknown individual (one-to-many comparison). Some might also use biometrics for purposes of *detection*, e.g., to detect if there is a face within an image. *See* CLARE GARVIE, ALVARO M. BEDOYA & JONATHAN FRANKLE, GEO. L. CTR. ON PRIV. & TECH., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 10–11 (2016). In addition, there could also be differences between physiological and behavioral biometrics. Whereas physiological biometrics are difficult to change, behavioral biometrics could be controlled or manipulated, at least to some extent.

2 *See infra* Section I.B.

3 *See infra* Section I.B.

4 *See infra* Section I.B.

5 *See infra* Section I.B.

security, it is also highly troubling from human rights and liberties perspectives.[6] This technology, most notably facial recognition, is constantly and systematically proven to be erroneous—making many inaccurate identifications (false positives).[7] Such inaccuracy, as researchers continuously prove, is not equally spread between cohorts, making dramatically more false identifications for women than for men and, in the context of this Article, for Black people than for white people.[8] While such use of recognition technology digitally places nearly half of Americans, along other foreigners, in a perpetual lineup,[9] it more dramatically affects those who systematically tend to suffer from racially biased enforcement within the realm of criminal law, duplicating and potentially amplifying these mistreatments.

This Article examines the effects of combining recognition technology with criminal enforcement—tainted with racist algorithms, datasets, and decision-making—defining it as *racial recognition*. As further discussed, racial recognition might stem from biased and often homogenous developers of recognition algorithms and services,[10] tainted training data and datasets,[11] and both institutional and individual police racism evident throughout history and ongoing in current American society.[12]

As this Article further suggests, a biased system combined with institutional or personal racism within police work might not only perpetuate racial bias, but rather it is likely to increase mistreatment of marginalized communities, often Black people, legitimizing legal action against them, thus increasing racial disparities and social control over these communities. While there are some recent initiatives to place moratoriums on the use of facial recognition by law enforcement agencies,[13] and by both private entities and a few state legislatures,[14]

---

6 As further discussed throughout this Article, recognition technology might impact many human rights, such as privacy, free speech, free association, free movement, and due process. Notably, however, while this Article sometimes points to the potential violations of these human rights and liberties in the context of surveillance, it focuses on recognition technology as a form of identification.

7 *See infra* Section II.A.

8 *See infra* Section II.A.

9 *See generally* GARVIE, BEDOYA & FRANKLE, *supra* note 1; Clare Garvie, *You're in a Police Lineup, Right Now*, N.Y. TIMES (Oct. 15, 2019), https://www.nytimes.com/2019/10/15/opinion/facial-recognition-police.html [https://perma.cc/57TK-LYEZ].

10 *See infra* Section II.A.

11 *See infra* Section II.A.

12 *See infra* Section II.B.

13 *See infra* Sections III.A–III.B.

14 *See infra* Sections III.A–III.B.

such legal intervention is currently insufficient in regulating racial recognition, whereas this technology might soon be normalized and structured within daily police work.

The time is ripe to directly address the concerns of racial recognition on the federal level before it becomes too late. This Article thus analyzes how to properly regulate the use of recognition technology, most dominantly facial recognition, for purposes of suspect identification by criminal law enforcement agents, while focusing on the racial aspects that unregulated use of this technology will perpetuate and amplify. This analysis is composed of three main Parts.

Part I provides a general taxonomy of criminal enforcement, further divided into five eras—locating the use of recognition technology within the fourth era of *digital policing*. This Part further explores developments in the field of biometrics and recognition technology to set grounds for discussing the racial aspects of recognition technology within the context of criminal enforcement.

Part II introduces the rise of *racial recognition*—how recognition technology and its use by enforcement agents could be embedded with racism. It begins by scrutinizing the general racial aspects of recognition technology as they currently unfold and continues by zooming out to the realm of criminal law to examine how the combination of recognition technology and racism becomes highly troubling within the realm of criminal law enforcement.

Part III turns to discuss and analyze the regulation of racial recognition and offers viable solutions to this conundrum. It begins by providing an analysis of the legality of using recognition technology within criminal law, while considering its proven racism. It does so by dividing the discussion between constitutional protections and other laws and regulations that are prime candidates to either directly or indirectly regulate police work, algorithms, and datasets in the context of racial recognition. Upon concluding that the current legal landscape is insufficient in regulating racial recognition properly, Section III.B discusses the inevitable entrance of recognition technology for purposes of identification in the future and how to slow it down, further dividing the discussion between legal and non-legal modalities. This Section then offers a conceptual blueprint for policymakers, which details the three stages and steps that policymakers must follow to properly legalize the use of recognition technology in the near and inevitable future, while focusing on human rights and liberties in general and of those affected by this technology—mostly marginalized and over-policed communities.

I. TECHNOLOGY'S GROWING ROLE IN CRIMINAL ENFORCEMENT

Criminal enforcement and technology share a meaningful history. With new technological developments, it became natural for law enforcement agencies to seek ways to implement and use these innovations to aid in performing their legal mandates of maintaining public safety. Naturally, equipping enforcement agents with new tools to combat crime has had many benefits but has also raised concerns of misuse. To better understand how recent developments within the intersection of AI and biometrics could be misused against some cohorts, this Part discusses the growing role of technology in criminal enforcement generally and then turns to further explore biometric developments, as well as recognition technology, in order to set the grounds for discussing their racial aspects and potential misuse.

A. *Criminal Enforcement and Technological Innovation*

Technology began to assume a role in criminal enforcement roughly two centuries ago. It began in what some termed as the *Political Era*,[15] lasting from 1840 to 1920, during which the state granted the police access to new weapons: along with inventions like the nightstick, police officers began using more sophisticated weapons, like Colt's first multi-shot pistol.[16] New developments in communication technologies also joined the array of tools used in criminal investigations, and enforcement agents in many states were technically, and often legally, positioned to wiretap telegraphs and telephones to obtain data on what individuals were writing or saying.[17]

Then came the *Professional Model Era*, roughly lasting from 1920 to 1970, in which inventions like the polygraph and fingerprint and handwriting classification systems revolutionized criminal investigations.[18] This era saw many developments. In its early days,

---

15 Notably, the terminology of these eras, along with the exact timelines, could be challenged, and they are merely used to exemplify the development of police use of technology throughout history.

16 *See* SEASKATE, INC., THE EVOLUTION AND DEVELOPMENT OF POLICE TECHNOLOGY 2, 22 (1998), https://www.ncjrs.gov/pdffiles1/Digitization/173179NCJRS.pdf [https://perma.cc/2TQR-PKA4].

17 *See* Eldar Haber, *The Wiretapping of Things*, 53 U.C. DAVIS L. REV. 733, 737–40 (2019). Notably, at that time, the state also initiated police callboxes to offer direct communication with them. *See* SEASKATE, INC., *supra* note 16, at 2.

18 *See* SEASKATE, INC., *supra* note 16, at 22.

crime laboratories arrived to America.[19] In the mid-1930s, American police began using automobiles and two-way radios.[20] In the late 1940s, traffic law agents began using radar speed guns.[21] And finally, beginning in the 1960s, computers assumed a more significant role within police efforts to combat crime, as exemplified in the formation of the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC), which enabled many police departments across America to connect to a computer for the first time.[22]

Many consider the 1970s as the beginning of a third era in criminal enforcement—some have dubbed it the *Community Policing Era*.[23] At that time, American police departments entered a large-scale computerization phase, which included computer-assisted dispatch management information systems and a nationwide centralized call collection (the famous "911" system).[24] Technology also made it possible for enforcement agencies to use new innovations, like soft body armor, night-vision devices, pepper spray (as a force alternative), and tasers, among other inventions made readily available and legal for police use.[25]

While current police practices could be located somewhere in the midst of this third era, this Article frames new technological developments within a fourth one—that of big data, hyper-connectivity, and AI. This era, dubbed here as *Digital Policing*, continues the role that technology played within law enforcement agencies, but its growth might be exponential.[26] The starting point of *Digital Policing* could be

---

19 The first police crime laboratory is attributed to the French criminologist Edmund Locard in Lyon, France, in 1910. The first American crime laboratory was established by the Los Angeles Police Department in 1923. *See id.*

20 *Id.* at 2, 22.

21 *Id.* at 2, 22, 27.

22 The NCIC is an electronic clearinghouse of crime data that can be tapped into by virtually every criminal justice agency nationwide, 24 hours a day, 365 days a year. It helps criminal justice professionals apprehend fugitives, locate missing persons, recover stolen property, and identify terrorists. It also assists law enforcement officers in performing their duties more safely and provides information necessary to protect the public. *National Crime Information Center (NCIC)*, FBI SERVS., https://www.fbi.gov/services/cjis/ncic [https://perma.cc/43H4-ZVWQ]; *see also* SEASKATE, INC., *supra* note 16, at 23.

23 SEASKATE, INC., *supra* note 16, at 5, 23, 32.

24 *Id.*

25 *Id.* at 23.

26 This is due partially to what is termed as "Moore's law," arguing that the number of transistors in a dense integrated circuit will double roughly every two years. *See* Gordon E. Moore, *Cramming More Components onto Integrated Circuits*, 38 ELECS. 114 (1965), http://eletel.p.lodz.pl/sm/materialy/ext/cramming.pdf [https://perma.cc/6MRZ-8ASL]. Many, however, argue that Moore's law will reach its limits soon. *See, e.g.*, M. Mitchell Waldrop, *The*

traced to the early 1990s, with the invention of the public internet.[27] Since making its debut, the internet has developed into a communication tool for many individuals. In a relatively brief time, data storage has become accessible and cheaper, while computers have become more mobile and affordable for almost anyone to use.[28] With the rise in connectivity and storage, and along with other technological developments, the growing field of AI has enabled individuals to go online in new and exciting ways, which in turn has paved new pathways for enforcement agencies to locate and investigate crimes.[29]

Public infrastructure has also become more connected. The public sphere has gradually become awash with sensors of various kinds—more cameras and other sensors that could be used for investigating crimes or enforcement in real time.[30] For example, these sensors and cameras aid enforcement agencies in detecting license plates to obtain timestamps and locations of cars;[31] body-worn cameras (BWCs) can aid law enforcement investigations by capturing both video and audio of those in the vicinity of an agent;[32] drones are used to obtain an aerial view of a crime scene or in real time to locate suspects;[33] gunshot detection technologies are deployed for detecting, recording, and

Chips Are Down for Moore's Law, NATURE (Feb. 9, 2016), https://www.nature.com/news/the-chips-are-down-for-moore-s-law-1.19338 [https://perma.cc/3RD9-47QX].

27 *See* Evan Andrews, *Who Invented the Internet?*, HISTORY (Oct. 28, 2019), https://www.history.com/news/who-invented-the-internet [https://perma.cc/F8GW-4CX8].

28 *See, e.g.*, William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1197–99 (2010) (describing how storage costs dropped).

29 The use of AI by enforcement agencies is not only inevitable, as this Article further suggests in Section III.B, but it is already on the move. One example is Internet of Things (IoT) devices equipped with microphones and cameras that could be turned into wiretapping devices. *See generally* Haber, *supra* note 17.

30 *See* Andrew Guthrie Ferguson, *Illuminating Black Data Policing*, 15 OHIO ST. J. CRIM. L. 503, 506–07 (2018); Irina Ivanova, *Video Surveillance in U.S. Described as on Par with China*, CBS NEWS (Dec. 10, 2019, 6:36 PM), https://www.cbsnews.com/news/the-u-s-uses-surveillance-cameras-just-as-much-as-china [https://perma.cc/LV2A-L4QK].

31 *See Street-Level Surveillance: Automated License Plate Readers (ALPRs)*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/automated-license-plate-readers-alpr [https://perma.cc/U6LJ-AH7S].

32 *See Street-Level Surveillance: Body-Worn Cameras*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/body-worn-cameras [https://perma.cc/4FLB-WSDT].

33 *See Street-Level Surveillance: Drones/Unmanned Aerial Vehicles*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/dronesunmanned-aerial-vehicles [https://perma.cc/E8CE-WSA3].

locating the sound of gunfire;[34] and, as a final example, predictive policing uses AI to work more efficiently and proactively in policing.[35]

The combination of these and other technological developments are likely to substantially impact how criminal enforcement is reshaped and, one might suggest, eventually lead to a fifth conceptual era of enforcement: that of *Autonomous Policing*. One day, maybe even during our lifetimes, the unfolding of the so-called Industrial Revolution 4.0 might, in turn, make enforcement autonomous and machine-reliant.[36] Autonomous policing robots might one day partially or fully enforce the law. The field of warfare is already showing evidence of heading in this direction, as we begin to witness the automation of militaries in some parts of the world.[37] Criminal enforcement might thus follow suit.

Currently, however, while some autonomous security robots already exist,[38] we are not yet within the era of *Autonomous Policing*. We might witness the partial or even full automation of many instruments, including perhaps vehicles or other "things" that shape

---

34 *See Street-Level Surveillance: Acoustic Gunshot Detection*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/gunshot-detection [https://perma.cc/J9XY-L5ST].

35 Predictive policing refers to using analytical techniques "to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions." *See* WALTER L. PERRY, BRIAN MCINNIS, CARTER C. PRICE, SUSAN C. SMITH & JOHN S. HOLLYWOOD, RAND CORP., PREDICTIVE POLICING: THE ROLE OF CRIME FORECASTING IN LAW ENFORCEMENT OPERATIONS 1–2 (2013). *See generally* Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259, 265 (2012) ("[P]redictive policing involves computer models that predict areas of future crime locations from past crime statistics and other data."); Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109, 1112 (2017) ("[P]olice are adopting predictive policing strategies that promise the holy grail of policing—stopping crime before it happens."); Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 GA. L. REV. 109, 114 (2017) (explaining how predictive policing uses "data and analytics to predict crime" (quoting JENNIFER BACHNER, IBM CTR. FOR THE BUS. OF GOV'T, PREDICTIVE POLICING: PREVENTING CRIME WITH DATA AND ANALYTICS 6 (2013))); Aziz Z. Huq, *Racial Equity in Algorithmic Criminal Justice*, 68 DUKE L.J. 1043, 1045 (2019) (discussing the "effect of algorithmic criminal justice tools on *racial equity*").

36 *See generally* KLAUS SCHWAB, THE FOURTH INDUSTRIAL REVOLUTION (2016).

37 *See, e.g.*, Rebecca Crootof, *The Killer Robots Are Here: Legal and Policy Implications*, 36 CARDOZO L. REV. 1837 (2015); Rebecca Crootof, *War Torts: Accountability for Autonomous Weapons*, 164 U. PA. L. REV. 1347 (2016).

38 Autonomous policing robots are increasingly becoming a reality in some parts of the world, including Dubai. *See* Thomas Page, *The Inevitable Rise of the Robocops*, CNN BUS. (May 22, 2017, 11:04 AM), https://edition.cnn.com/2017/05/22/tech/robot-police-officer-future-dubai/index.html [https://perma.cc/ULV8-GZMJ]; Reuters Staff, *Robocop Joins Dubai Police to Fight Real Life Crime*, REUTERS (June 1, 2017, 6:02 AM), https://www.reuters.com/article/us-emirates-robocop-idUSKBN18S4K8 [https://perma.cc/NHU2-9D6B]. Autonomous security robots, however, are already in use by some U.S. states. *See* Katie Flaherty, *A RoboCop, a Park and a Fight: How Expectations About Robots Are Clashing with Reality*, NBC NEWS (Oct. 4, 2019, 9:04 AM), https://www.nbcnews.com/tech/tech-news/robocop-park-fight-how-expectations-about-robots-are-clashing-reality-n1059671 [https://perma.cc/5RKW-C8NT].

our lives. But these developments have not yet been directly translated into the American criminal realm—not fully at least. Automation is relatively still in its infancy, with the example of the promised driverless or autonomous car that currently seems far from reaching its goals or fulfilling its potential.[39]

Still, there are vast differences in policing within the fourth era. Policing in 2021 is different from policing in 1990. Policing, for one, has expanded far beyond the kinetic world, as cyberspace has become a playing field for criminals to act in.[40] But aside from such moves that necessitated institutional changes in police practices, new technological advancements that are intertwined with biometric analysis are becoming valuable new tools in policing. As Section I.B further shows, somewhere within the curve of *Digital Policing*, the combination of biometrics and the wide spread of data and advancements in AI are already beginning to reshape criminal law enforcement.

B. *Biometrics, Recognition Technology, and Criminal Enforcement*

Identifying suspects and locating witnesses to crimes is integral to criminal enforcement. Criminals are likely to flee the crime scene, often leaving law enforcement agents with few or no clues as to their identity. Identification efforts could be directed, inter alia, toward gathering forensic evidence, like that of deoxyribonucleic acid (DNA)[41] or fingerprints.[42] Other efforts will likely be directed toward the

---

39 Take, for example, the "conservative" prediction made in 2017 that by 2020 there will be ten million self-driving cars on the road. Olivier Garret, *10 Million Self-Driving Cars Will Hit the Road by 2020–Here's How to Profit*, FORBES (Mar. 3, 2017, 9:00 AM), https://www.forbes.com/sites/oliviergarret/2017/03/03/10-million-self-driving-cars-will-hit-the-road-by-2020-heres-how-to-profit/?_sh=493fea0d7e50 [https://perma.cc/HJ4C-2QRF]. The reality is far from it. Daniel Gessner, *Experts Say We're Decades from Fully Autonomous Cars. Here's Why.*, BUS. INSIDER (July 22, 2020, 10:30 AM), https://www.businessinsider.com/self-driving-cars-fully-autonomous-vehicles-future-prediction-timeline-2019-8 [https://perma.cc/A23V-TK3J].

40 For more on the growth of crime rates within the digital world, see Ronald Deibert, *The Growing Dark Side of Cyberspace (. . . and What to Do About It)*, 1 PA. ST. J.L. & INT'L AFFS. 260, 265–66 (2012); Elena Anatolyevna Kirillova, Rashad Afatovich Kurbanov, Natalia Viktorovna Svechnikova, Teymur El'darovich Zul'fugarzade & Sergey Sergeevich Zenin, *Problems of Fighting Crimes on the Internet*, 8 J. ADVANCED RSCH. L. & ECON. 849 (2017).

41 The DNA was first discovered in the early 1980s and was first used in a criminal proceeding in 1988. *See* Andrews v. State, 533 So. 2d 841 (Fla. Dist. Ct. App. 1988); Ronald J. Rychlak, *DNA Fingerprinting, Genetic Information, and Privacy Interests*, 48 TEX. TECH L. REV. 245, 245–46 (2015).

42 The first known criminal trial in the United States that used fingerprint evidence dates to 1910. *See* Francine Uenuma, *The First Criminal Trial that Used Fingerprints as Evidence*, SMITHSONIAN MAG. (Dec. 5, 2018), https://www.smithsonianmag.com/history/first-case-where-

questioning of victims or eyewitnesses, if any exist and are able to assist. These victims or eyewitnesses might be able to, inter alia, describe the culprit, sometimes to a composite sketch artist, for the police to publish the sketch or use in another way to aid in solving the crime.[43] When attempting to visually pick a culprit from a police lineup, enforcement agents might not merely rely on people's memories and identification of faces but also on identification of other biometric features, like voices or even body gestures.[44]

Biometrics entered criminal investigations prior to digital technology. Even within the *Political Era* of policing, and as early as 1888, the police used various methods, such as anthropological classification, to identify culprits.[45] Fingerprinting, now an indispensable part of policing, was used in American criminal investigations as early as the early twentieth century.[46] Almost three-quarters of a century later, computers entered the world of biometric identification, and in 1975, the FBI began using fingerprint readers.[47] Realizing the potential of computerized biometrics, the FBI's Criminal Justice Information Services Division initiated the Integrated Automated Fingerprint Identification System (IAFIS) in 1999, which provided, inter alia, digital tenprint and latent fingerprint searches.[48] These, along with other forensic and investigative techniques, began to assume integral roles within the criminal justice system.[49]

---

fingerprints-were-used-evidence-180970883 [https://perma.cc/SE98-H77V]. *See generally* SIMON A. COLE, SUSPECT IDENTITIES: A HISTORY OF FINGERPRINTING AND CRIMINAL IDENTIFICATION (2002).

43 *See generally* STEPHEN MANCUSI, THE POLICE COMPOSITE SKETCH (2010).

44 *See, e.g.*, Ryan J. Fitzgerald, Heather L. Price & Tim Valentine, *Eyewitness Identification: Live, Photo, and Video Lineups*, 24 PSYCH., PUB. POL'Y & L. 307 (2018).

45 Anthropological classification methods, invented by Alphonse Bertillon in 1879, were first used to identify criminals in 1888 with the adoption of the Bertillon system of identification. Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 19 & n.25 (2016) (citing COLE, *supra* note 42, at 32–59); SEASKATE, INC., *supra* note 16, at 22.

46 Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 418–19 (2012) (describing the history of fingerprinting).

47 SEASKATE, INC., *supra* note 16, at 23.

48 *Next Generation Identification (NGI)*, FBI SERVS., https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi [https://perma.cc/Y99H-GHES].

49 Jessica D. Gabel & Margaret D. Wilkinson, *"Good" Science Gone Bad: How the Criminal Justice System Can Redress the Impact of Flawed Forensics*, 59 HASTINGS L.J. 1001, 1002 (2008). *See generally* Jessica Gabel Cino, *Deploying the Secret Police: The Use of Algorithms in the Criminal Justice System*, 34 GA. ST. U. L. REV. 1073, 1074 (2018) ("[S]cience (in particular, forensic science) has become a mainstay in the criminal justice system.").

Perhaps the biggest leap in biometric identification, the one that is at the heart of this Article, is that of *recognition technology*. Biometric features of people's faces, voices, or bodily gestures (often gait), among other biometric features, can now be analyzed not simply by humans but by computers to match them with potential culprits.[50] Such practices of *verification* or *identification*[51] can even include searching for non-biometric features linked to suspects, such as tattoos, clothing, shoes, or any other identifying characteristics relevant for investigation. The imperfect memory of humans can now be replaced with the allegedly exact—and almost endless—memory and capabilities of computers[52] for detecting and analyzing both physiological and behavioral characteristics.

Recognition technology can apply to many bodily and non-bodily features. One current dominant technology is that of facial recognition, focusing on various facial features, like eyes or nose, measuring the distance between them; using various datapoints within one's face, such as skin, shadows, or other attributes; or matching faces as a whole.[53] Other notable forms of recognition technology consist of iris recognition,[54] voice recognition,[55] and gesture recognition.[56] Recognition technology can also extend beyond classical biometric identification to include the use of physiometrics, like the measurement of heart rate or blood pressure; the use of anthropometrics;[57] and the recognition of tattoos.[58] To use recognition technology for purposes of

---

50 *See* Timothy Williams, *Facial Recognition Software Moves from Overseas Wars to Local Police*, N.Y. TIMES (Aug. 12, 2015), https://www.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local-police.html [https://perma.cc/VVS9-ZGRG].

51 *See* GARVIE, BEDOYA & FRANKLE, *supra* note 1.

52 *See* Robison, *supra* note 28, at 1197–99.

53 Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1107 (2021).

54 *Street-Level Surveillance: Iris Recognition*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/iris-recognition [https://perma.cc/6945-ZB3A].

55 Voice recognition is not to be confused with speech recognition—"a capability which enables a program to process human speech into a written format." IBM Cloud Education, *Speech Recognition*, IBM (Sept. 2, 2020), https://www.ibm.com/cloud/learn/speech-recognition [https://perma.cc/P7SW-BFNH].

56 Sushmita Mitra & Tinku Acharya, *Gesture Recognition: A Survey*, 37 IEEE TRANSACTIONS ON SYS., MAN & CYBERNETICS 311, 311 (2007) ("Gesture recognition pertains to recognizing meaningful expressions of motion by a human, involving the hands, arms, face, head, and/or body.").

57 Malkia Devich-Cyril, *Defund Facial Recognition*, ATLANTIC (July 5, 2020), https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771 [https://perma.cc/F4H4-K8QA].

58 Tattoo recognition technology examines images of tattoos to identify suspects. *Street-Level Surveillance: Tattoo Recognition*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/tattoo-

identification, one must obtain a sample of the target's recognizable feature, a database that contains identification features of the population, and an algorithm that produces potential matches between the created template of the target's recognizable feature and the stored identification features present within the database.[59]

The promises of recognition technology for identification and verification, perhaps most dominantly these days that of facial recognition, are already implemented and affect many areas of our lives. The military and intelligence agencies reportedly use facial recognition tools to identify possible terrorist suspects, especially overseas.[60] The Transportation Security Administration (TSA) uses it in airports as a more efficient form of checking and verifying travel documents, e.g., for verifying overstayed visas,[61] or simply for passenger identification purposes.[62] Immigration and Customs Enforcement (ICE) agents use it

---

recognition [https://perma.cc/6KKS-DUEA]. For an empirical evaluation of tattoo recognition algorithms, see MEI NGAN, PATRICK GROTHER & KAYEE HANAOKA, NAT'L INST. OF STANDARDS & TECH., TATTOO RECOGNITION TECHNOLOGY - EVALUATION (TATT-E) PERFORMANCE OF TATTOO IDENTIFICATION ALGORITHMS (2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8232.pdf [https://perma.cc/V5GX-9WF6].

59 U.S. GOV'T. ACCOUNTABILITY OFF., GAO-20-522, FACIAL RECOGNITION TECHNOLOGY: PRIVACY AND ACCURACY ISSUES RELATED TO COMMERCIAL USES 6 (2020) [hereinafter PRIVACY AND ACCURACY ISSUES] (exemplifying how a facial recognition technology system works).

60 Nick Wingfield, *Amazon Pushes Facial Recognition to Police. Critics See Surveillance Risk.*, N.Y. TIMES (May 22, 2018), https://www.nytimes.com/2018/05/22/technology/amazon-facial-recognition.html [https://perma.cc/R9L5-JSNC]. American military and intelligence agencies were reported to use facial recognition technology in Iraq and Afghanistan. Williams, *supra* note 50; Bobby Allyn, *Amazon Halts Police Use of Its Facial Recognition Technology*, NPR (June 12, 2020, 12:55 PM), https://www.npr.org/2020/06/10/874418013/amazon-halts-police-use-of-its-facial-recognition-technology [https://perma.cc/9UF3-JFA6] ("American intelligence and military officials have long used facial recognition software in overseas anti-terrorist operations . . . .").

61 Ron Nixon, *Facial Scans at U.S. Airports Violate Americans' Privacy, Report Says*, N.Y. TIMES (Dec. 21, 2017), https://www.nytimes.com/2017/12/21/us/politics/facial-scans-airports-security-privacy.html [https://perma.cc/G8ZD-M2NM]; *see* Francesca Street, *How Facial Recognition Is Taking Over Airports*, CNN TRAVEL (Oct. 8, 2019), https://edition.cnn.com/travel/article/airports-facial-recognition/index.html [https://perma.cc/R9NG-RXZM].

62 The TSA identified passengers under a U.S. Customs and Border Protection program called "Biometric Exit." *See* Laura Hautala, *Facial Recognition Can Speed You Through Airport Security, But There's a Cost*, CNET (Mar. 21, 2019, 1:45 PM), https://www.cnet.com/news/facial-recognition-can-speed-you-through-airport-security-but-theres-a-cost [https://perma.cc/Y7WS-M3FM]. As for now, however, the U.S. Customs and Border Protection dropped its plans "to require that US citizens go through a biometric face scan when entering or exiting the country." Laura Hautala, *Proposal to Require Facial Recognition for US Citizens at Airports Dropped*, CNET (Dec. 5, 2019, 3:37 PM), https://www.cnet.com/news/proposal-to-require-facial-recognition-for-us-citizens-at-airports-dropped [https://perma.cc/Q8J9-RMZK].

to target undocumented immigrants.[63] And most likely, its primary use in terms of quantity comes from the market, sometimes within surveillance capitalism,[64] but also within its efforts to increase security[65] or to make products and services more convenient and enjoyable for consumers.[66]

Within the realm of criminal enforcement, it is hardly surprising that recognition technology is already deployed in totalitarian

---

63 Bill Chappell, *ICE Uses Facial Recognition to Sift State Driver's License Records, Researchers Say*, NPR (July 8, 2019, 4:23 PM), https://www.npr.org/2019/07/08/739491857/ice-uses-facial-recognition-to-sift-state-drivers-license-records-researchers-sa [https://perma.cc/D8XA-37B2].

64 *See* Sharon Nakar & Dov Greenbaum, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, 23 B.U. J. SCI. & TECH. L. 88, 97 (2017) (listing uses of facial recognition technology). With variations, surveillance capitalism means the commodification of personal data for profit. In this context, it refers to profiting from biometric features. *See generally* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

65 Madison Square Garden was reported using facial recognition technology "to bolster security and identify those entering the building." Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, N.Y. TIMES (Mar. 13, 2018), https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html [https://perma.cc/NPH7-NCFH]. Walmart was reported using facial recognition technology to identify shoplifters since 2015. *See* Jeff John Roberts, *Walmart's Use of Sci-Fi Tech to Spot Shoplifters Raises Privacy Questions*, FORTUNE (Nov. 9, 2015, 7:30 AM), https://fortune.com/2015/11/09/wal-mart-facial-recognition [https://perma.cc/9H37-Z993]. *See generally* Robert H. Thornburg, *Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses Under the Fourth Amendment*, 20 J. MARSHALL J. COMPUT. & INFO. L. 321, 326–29 (2002) (detailing various uses of facial recognition as a security measure).

66 For example, recognition technology can replace humans in verification tasks. Faceprints are already used in some places as a payment method. For groups, recognition technology might be used to adapt electronic advertising. *See* Adrienne LaFrance, *Who Owns Your Face?*, ATLANTIC (Mar. 24, 2017), https://www.theatlantic.com/technology/archive/2017/03/who-owns-your-face/520731 [https://perma.cc/R79G-V4C2]. Aside from using facial recognition to unlock phones or other devices, or instant tagging within social media, there could be many uses of this technology that could aid humans in performing various tasks. To exemplify, a Sky News broadcaster used Amazon's "Rekognition" technology to identify celebrities during the royal wedding of Prince Harry and Meghan Markle. Ryan Suppe, *Orlando Police Decide to Keep Testing Controversial Amazon Facial Recognition Program*, USA TODAY (July 10, 2019, 6:44 PM), https://www.usatoday.com/story/tech/2018/07/09/orlando-police-decide-keep-testing-amazon-facial-recognition-program/768507002 [https://perma.cc/9K4D-FFBY].

regimes.[67] But it is not merely reserved for these regimes.[68] Facial recognition technology is known to have been used by many enforcement agencies worldwide at least since the beginning of the twenty-first century.[69] Such use is also becoming more integral in the international criminal domain, in which Interpol operates and maintains a facial recognition system (known as IFRS) that contains facial images from most parts of the world.[70] And America is no exception. During the 2001 Superbowl in Tampa, Florida, the police admittedly used facial recognition tools to locate subjects of outstanding warrants, in perhaps the first reported event in America.[71] At roughly the same time, police departments across America were reported to have begun using facial recognition technology.[72] Officially, the New York Police Department (NYPD) reported its use of facial

67 For more on the wide use of advanced technologies like phone scanners, facial recognition cameras, and glasses in China, see Paul Mozur & Aaron Krolik, *A Surveillance Net Blankets China's Cities, Giving Police Vast Powers*, N.Y. TIMES (Dec. 17, 2019), https://www.nytimes.com/2019/12/17/technology/china-surveillance.html [https://perma.cc/J3WK-PVZJ]; Josh Chin, *Chinese Police Add Facial-Recognition Glasses to Surveillance Arsenal,* WALL ST. J. (Feb. 7, 2018, 6:52 AM), https://www.wsj.com/articles/chinese-police-go-robocop-with-facial-recognition-glasses-1518004353 [https://perma.cc/W8LZ-N4KH].

68 Aside from China, facial recognition technology is used for law enforcement purposes in the United Kingdom, Russia, Singapore, and the United States, to name a few examples. *See* Matthew Keegan, *Big Brother Is Watching: Chinese City with 2.6m Cameras Is World's Most Heavily Surveilled*, GUARDIAN (Dec. 2, 2019, 1:00 PM), https://www.theguardian.com/cities/2019/dec/02/big-brother-is-watching-chinese-city-with-26m-cameras-is-worlds-most-heavily-surveilled [https://perma.cc/9FZL-49XB].

69 See, for instance, the United Kingdom, where the Metropolitan Police tested "[t]he Face Examiner"—a facial recognition system that automatically scans faces in crowds and compares them, inter alia, against a database of known criminals. Darren Boyle, *Police to Scan 1 Million People with New Automatic Facial Recognition Software in Bid to Beat Crime at Notting Hill Carnival*, DAILY MAIL (Aug. 27, 2016, 7:44 AM), https://www.dailymail.co.uk/news/article-3761236/Police-scan-1million-people-new-automatic-facial-recognition-software-bid-beat-crime-Notting-Hill-Carnival.html [https://perma.cc/U2N5-TNS7].

70 *See Facial Recognition*, INTERPOL, https://www.interpol.int/How-we-work/Forensics/Facial-Recognition [https://perma.cc/VU84-27PN].

71 The system identified nineteen subjects of outstanding warrants, but they were not arrested at that time. Niraj Chokshi, *Facial Recognition's Many Controversies, From Stadium Surveillance to Racist Software*, N.Y. TIMES (May 15, 2019), https://www.nytimes.com/2019/05/15/business/facial-recognition-software-controversy.html [https://perma.cc/5ESH-JJ73].

72 Seemingly, the largest facial recognition program is based in Pinellas County, Florida. The program is almost twenty years old. 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?auth=login-google [https://perma.cc/93M4-BS2R]; *see also* Williams, *supra* note 50.

recognition since 2011,[73] while the Detroit Police Department has been using it since at least 2017.[74]

On the federal level, the United States maintains and operates various biometric identification systems and programs.[75] In 2011, the FBI began using the Next Generation Identification (NGI) system, which replaced the previously mentioned fingerprint system (IAFIS).[76] NGI includes a facial recognition search in which an authorized law enforcement official can submit a "probe" photo to be matched against mostly federally generated images, like mugshot repositories (accompanying criminal tenprint fingerprints and a criminal history record).[77] The FBI also operates a facial recognition unit named Facial Analysis, Comparison, and Evaluation Services, or simply FACE, which can compare a facial image (probe photo) to a database comprising driver's licenses and other ID photos,[78] along with other state photo repositories, such as criminal mugshots or corrections photos, obtained from databases of several U.S. states.[79]

Enforcement agencies have become eager to use recognition technology and, perhaps more commonly for now, facial recognition.[80]

---

73 *NYPD Questions and Answers: Facial Recognition*, NYPD, https://www1.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page [https://perma.cc/HYE5-HKXW]; *see* GARVIE, BEDOYA & FRANKLE, *supra* note 1, at 13.

74 Tawana Petty, *Defending Black Lives Means Banning Facial Recognition*, WIRED (July 10, 2020, 8:00 AM), https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition [https://perma.cc/4M9K-TQJ8].

75 Such would include the Department of Defense's (DoD) Automated Biometric Identification System (ABIS), the Department of Homeland Security (DHS), and the State Department biometric databases and watchlists. Donohue, *supra* note 46, at 413–14.

76 The NGI system maintains a photograph repository titled the Interstate Photo System (IPS), allowing automated facial recognition "searches by authorized local, state, tribal, and federal law enforcement agencies." Kimberly J. Del Greco, Deputy Assistant Dir., Crim. Just. Info. Servs. Div., FBI, Statement Before the House Oversight and Reform Committee: Facial Recognition Technology: Ensuring Transparency in Government Use (June 4, 2019), https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use [https://perma.cc/7PNR-287J].

77 *See Next Generation Identification (NGI)*, *supra* note 48; GARVIE, BEDOYA & FRANKLE, *supra* note 1, at 14. Notably, the FBI claims that such search will return "a gallery of 'candidate' photos of 2–50 individuals," whereas in the second step, the agent will "manually review the candidate photos and perform further investigation to determine if any of the candidate photos are the same person as the probe photo." Del Greco, *supra* note 76. *See generally* Donohue, *supra* note 46, at 443–48.

78 These might include, inter alia, the Department of State's Visa and Passport Photo Files. *See* Del Greco, *supra* note 76.

79 *See* GARVIE, BEDOYA & FRANKLE, *supra* note 1, at 14–15; Del Greco, *supra* note 76.

80 The NYPD claims that any matches from facial recognition technology do not establish probable cause to arrest or obtain a search warrant but rather serve as leads. *NYPD Questions and Answers: Facial Recognition*, *supra* note 73. A similar approach is taken by ICE's Homeland

To run a search, other than obtaining the suspect's identifier and the technological tool that enables identification, there must be a database within which to search a suspect's identifier. The FBI's NGI system contains an electronic repository of biometrics along with criminal history information.[81] Similar systems can also be found on the state level.[82] And by 2016, police facial recognition databases were reported to have the photos of roughly half of the adult population in America,[83] while various reports indicate that enforcement agencies are continuously building enormous databases with millions of individuals' photos.[84] Enforcement agencies often share data between various state and federal departments and agencies, and such sharing might eventually increase the already large datasets of biometric data accessible to police officers.[85] These internal biometric databases, the legality of which will be further discussed in Part III, might thus be composed of various sources most notably from arrest photos and criminal-related activities.[86]

Within their efforts to improve their abilities, law enforcement agencies also turned to the private market's power. Already heavily invested in the technology, the market was ready to provide identification tools for anyone to use, including law enforcement

---

Security Investigations. *See* Aaron Boyd, *ICE Outlines How Investigators Rely on Third-Party Facial Recognition Services*, NEXTGOV (June 2, 2020), https://www.nextgov.com/emerging-tech/2020/06/ice-outlines-how-investigators-rely-third-party-facial-recognition-services/165846 [https://perma.cc/M682-BAKA].

81 *See Next Generation Identification (NGI)*, *supra* note 48. This database "combines data such as fingerprints, iris scans, photographs, and voice data into a searchable platform used by both federal and state agencies." Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. MARSHALL L. REV. 589, 596 (2018).

82 *See* Donohue, *supra* note 46, at 459–62.

83 *See* GARVIE, BEDOYA & FRANKLE, *supra* note 1, at 2; Lily Hay Newman, *Cops Have a Database of 117M Faces. You're Probably in It*, WIRED (Oct. 18, 2016, 2:19 PM), https://www.wired.com/2016/10/cops-database-117m-faces-youre-probably [https://perma.cc/5WCY-25A8].

84 To exemplify, *The New York Times* reported that in San Diego County "beat cops, detectives and even school police officers have been using hand-held devices to create a vast database of tens of thousands of photos of people . . . —some suspected of committing crimes, others not—usually without the person's consent." Williams, *supra* note 50.

85 One example is that of the Law Enforcement National Data Exchange (N-DEx)—a national data-sharing system that aids agencies across the country to "search, link, analyze, and share local, state, tribal, and federal records." *National Data Exchange (N-DEx) System*, FBI SERVS., https://www.fbi.gov/services/cjis/ndex [https://perma.cc/L4UU-667Q].

86 The NYPD, for example, argues that it only uses facial recognition when comparing images that are obtained during a criminal investigation, with "lawfully possessed arrest photos." *NYPD Questions and Answers: Facial Recognition*, *supra* note 73.

agencies.[87] Some market players directly targeted law enforcement agencies as customers, offering them biometric or biological identification tools services. Amazon, for instance, pushed its face identification system (Rekognition) to enforcement agencies,[88] emphasizing that it "could aid criminal investigations by recognizing suspects in photos and videos."[89] And such private technology is not a rare exception. Many federal and state law enforcement officers reportedly used private facial recognition apps or services in their efforts to identify suspects.[90]

The market soon expanded to include not only the technology but also the database. Companies like Clearview AI began offering enforcement agencies services of comparing probe photos submitted by the police—not only against limited state-owned databases but also against billions of images scraped from Facebook, YouTube, Venmo, and other online sources.[91] Until recently at least, Clearview AI worked closely with thousands of police agencies across the United States alone,[92] while other foreign companies in this field had also been reported to work closely with American law enforcement agencies.[93]

While outside this Article's main focus, what already came into play in some areas, and could likely expand without regulatory barriers, is the police use of recognition technology in real time. If the public sphere becomes awash with sensors, then it might also be intertwined with real-time recognition technology, e.g., identifying the faces or other features of those in the public sphere.[94] Such live facial recognition is already used in China and by enforcement agents in London, United

---

87 For more on the increase in the facial recognition market, see PRIVACY AND ACCURACY ISSUES, *supra* note 59, at 8–10.

88 *See Amazon Rekognition*, AMAZON WEB SERVS., https://aws.amazon.com/rekognition/?blog-cards.sort-by=item.additionalFields.createdDate&blog-cards.sort-order=desca [https://perma.cc/A9FQ-67WE].

89 Wingfield, *supra* note 60.

90 *See* Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. TIMES (Mar. 18, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/5FPJ-3TNC].

91 *Id.*

92 *See* Elizabeth Lopatto, *Clearview AI CEO Says 'Over 2,400 Police Agencies' Are Using Its Facial Recognition Software*, VERGE (Aug. 26, 2020, 4:40 PM), https://www.theverge.com/2020/8/26/21402978/clearview-ai-ceo-interview-2400-police-agencies-facial-recognition [https://perma.cc/MBT7-NNTY].

93 Reportedly, these include NEC and Ayonix (Japan); Cognitec (Germany); and iOmniscient (Australia). *See* Julia Horowitz, *Tech Companies Are Still Helping Police Scan Your Face*, CNN BUS. (July 3, 2020, 12:36 PM), https://edition.cnn.com/2020/07/03/tech/facial-recognition-police/index.html [https://perma.cc/QTK4-T4Z9].

94 *See* Newman, *supra* note 83.

Kingdom.[95] While it is unclear how many American jurisdictions have incorporated live facial recognition in public places,[96] Detroit is reported to use such recognition technology in conjunction with its $8 million Project Green Light that includes more than seven hundred high-definition cameras scattered across the city.[97] This Article, however, focuses mainly on proactive recognition rather than real-time recognition. And while a glimpse into the near future suggests that recognition technology could be much broader,[98] facial recognition is the most dominant for now.

Surely, the use of biometric identification might always sound troubling, but when it comes to criminal enforcement, it could carry dire consequences for people's rights and liberties. And as Part II shows, the use of recognition technology, especially facial recognition, dramatically affects some cohorts more than others. The next Part thus discusses the threats that recognition technology raises in the context of criminal enforcement, which has been systematically proven to be flawed and, more specifically, biased toward misidentifying some cohorts, most notably in the United States, Black people.

---

95 *See* Jason Douglas & Parmy Olson, *London Police to Start Using Facial-Recognition Cameras*, WALL ST. J. (Jan. 24, 2020, 2:49 PM), https://www.wsj.com/articles/london-police-to-start-using-facial-recognition-cameras-11579895367 [https://perma.cc/DQ4C-MVG7].

96 Currently, in New York City, the NYPD does not use facial recognition technology to identify people recorded on the city's network of security cameras, that is, "unless it is relevant to a crime that has been committed." *NYPD Questions and Answers: Facial Recognition*, *supra* note 73.

97 *See* Alfred Ng, *In the 'Blackest City in America,' a Fight to End Facial Recognition*, CNET (July 2, 2020, 3:04 PM), https://www.cnet.com/news/in-the-blackest-city-in-america-a-fight-to-end-facial-recognition [https://perma.cc/TE7S-EPTC]; Teresa Wiltz, *Facial Recognition Software Prompts Privacy, Racism Concerns in Cities and States*, PEW STATELINE (Aug. 9, 2019), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2019/08/09/facial-recognition-software-prompts-privacy-racism-concerns-in-cities-and-states [https://perma.cc/29MB-FY42].

98 For instance, police can scan t-shirts, watches, and shoes, and track potential suspects in photos uploaded to social media, and they will likely use tattoo, voice, and gait recognition, if they are not already doing so. *See* 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/Z4NL-2N44]; Aaron Mackey, Dave Maass & Soraya Okuda, *5 Ways Law Enforcement Will Use Tattoo Recognition Technology*, ELEC. FRONTIER FOUND. (May 5, 2015), https://www.eff.org/deeplinks/2016/05/5-ways-law-enforcement-will-use-tattoo-recognition-technology [https://perma.cc/9MDC-DTMF].

II. RACIAL RECOGNITION THREATS

Due to various legal instruments that prohibit or limit the use of recognition technology, limited governmental funding for using these technologies, or other market-related reasons, recognition technology is not yet fully implemented within the American criminal system. But where in use, and with a glimpse to the near future, it has many negative consequences on the rights and liberties of individuals and, specifically in the context of this Article, is a tool that might be used disproportionally for targeting specific cohorts, most profoundly Black people, who have historically been treated differently by enforcement agencies.[99] The use of recognition technology by enforcement agencies thus raises fears of mistreatment and increasing social control on marginalized communities.

This Part introduces the rise of what this Article calls *racial recognition*—that is, how the combination of law enforcement and recognition technology is likely tainted with racism. This term broadly incorporates the use of race, ethnicity, or national origin as a factor used by enforcement agents within any police practice relating to recognition technology. To do so, Section II.A scrutinizes the general racial aspects of recognition technology as they currently unfold, while Section II.B focuses on the realm of criminal law to show how the combination of recognition technology and racism becomes more than highly troubling within the realm of criminal law enforcement.

A. *Bias and Racism Within Recognition Technology*

Technology by itself is neither inherently biased nor racist. But it is hardly neutral either.[100] Algorithms and software are still mainly constructed and programed by humans. Under the AI branch of machine learning,[101] computational outcomes depend on their algorithms, the data that they are trained on, and the data fed into the system. This is where potential bias enters first: data and algorithms

---

99 *See, e.g.*, Rachel Moran, *In Police We Trust*, 62 VILL. L. REV. 953, 986 (2017) ("As long as police misconduct has existed in this country, its victims have been primarily people of color.").

100 *See generally* Batya Friedman & Helen Nissenbaum, *Bias in Computer Systems*, 14 ACM TRANSACTIONS ON INFO. SYS. 330 (1996).

101 Simply stated, machine-learning algorithms "use statistics to find patterns in massive amounts of data." Karen Hao, *What Is Machine Learning?*, MIT TECH. REV. (Nov. 17, 2018) (footnote omitted), https://www.technologyreview.com/2018/11/17/103781/what-is-machine-learning-we-drew-you-another-flowchart [https://perma.cc/TED2-9G8M].

often reflect choices about connections, inferences, and interpretations.[102] If the coder, the training dataset, or the data used contains some forms of explicit or implicit bias, then the output of the software will likely replicate or amplify this bias.[103] Bias in often means bias out.[104]

As machines are not inherently biased, it is humans that form such bias. Unfortunately, humans are probably the most biased organisms on this planet.[105] Computer bias begins with the architecture of systems. When coding, humans are likely to reflect their own priorities, preferences, and prejudices.[106] Adding to this conundrum, algorithms are often written by homogeneous developers.[107] Namely, American, white men, benevolent and without explicit bias as they may be, will often be influenced by cognitive shortcomings, like a tendency to recognize faces more easily within their racial group, also known as a *cross-race effect*.[108] Simply put, algorithms and codes might reflect both explicit and implicit biases and cognitive failures stemming from their developers, often linked to their own race or ethnicity. Human bias in recognition technology continues with the datasets used to train the

---

102 *See* Cynthia Dwork & Deirdre K. Mulligan, *It's Not Privacy, and It's Not Fair*, 66 STAN. L. REV. ONLINE 35, 35 (2013).

103 *See, e.g.*, Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 674 (2016) ("[D]ata mining can reproduce existing patterns of discrimination, inherit the prejudice of prior decision makers, or simply reflect the widespread biases that persist in society.").

104 *See* Sandra G. Mayson, *Bias In, Bias Out*, 128 YALE L.J. 2218, 2224 (2019) ("[I]f the thing that we undertake to predict—say arrest—happened more frequently to black people than to white people in the past data, then a predictive analysis will project it to happen more frequently to black people than to white people in the future.").

105 *See* Khari Johnson, *AI Weekly: Facial Recognition Policy Makers Debate Temporary Moratorium vs. Permanent Ban*, VENTUREBEAT (May 17, 2019, 2:01 PM), https://venturebeat.com/2019/05/17/ai-weekly-facial-recognition-policy-makers-debate-temporary-moratorium-vs-permanent-ban [https://perma.cc/7KES-7ZGL] (quoting Veritone CEO Chad Steelberg explaining that "[t]he most biased systems on this planet are humans").

106 *See* Katelyn Ringrose, *Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns*, 105 VA. L. REV. ONLINE 57, 62 (2019) ("These automated systems reflect the priorities, preferences, and prejudices of their coders . . . .").

107 *See* Nina Massey, *Biased AI Could Worsen Racial Inequality, Researchers Say*, INDEPENDENT (Aug. 6, 2020, 9:50 AM), https://www.independent.co.uk/news/uk/home-news/ai-bias-whiteness-racial-inequality-researchers-a9656546.html [https://perma.cc/FJQ5-3XVB] (quoting Dr. Kanta Dihal concluding that "[i]f the developer demographic does not diversify, AI stands to exacerbate racial inequality").

108 *See* Queenie Wong, *Why Facial Recognition's Racial Bias Problem Is So Hard to Crack*, CNET (Mar. 27, 2019, 5:00 AM), https://www.cnet.com/news/why-facial-recognitions-racial-bias-problem-is-so-hard-to-crack [https://perma.cc/G5FW-QDJ2] ("Engineers at tech companies, which are made up of mostly white men, might also be unwittingly designing the facial recognition systems to work better at identifying certain races . . . .").

system. AI-based algorithms learn from data and compute results accordingly. If the dataset is already tainted with bias or otherwise fails to accurately represent cohorts in society, then the algorithm will likely produce inaccurate or biased outcomes.[109]

With its promises, inaccuracy is still a major problem in recognition technology.[110] The American Civil Liberties Union (ACLU), for instance, proved that Amazon's Rekognition was so inaccurate that comparing twenty-five thousand public mugshots to Congressmembers resulted in falsely identifying twenty-eight of them as having previously been arrested by the police.[111] London Metropolitan's automated facial recognition system was proven to be wrong most of the time.[112] Adding to this problem, while some of these findings were performed under a closed environment in which the photos used were clear and well lit, poor-quality photos, which might be prevalent in criminal investigations, were proven to increase inaccuracies.[113]

---

109 *See, e.g.*, Harry Surden, *Machine Learning and Law*, 89 WASH. L. REV. 87, 106 (2014) ("In general, machine learning algorithms are only as good as the data that they are given to analyze.").

110 The accuracy of biometric identification has attracted much scholarly attention. *See, e.g.*, P. JONATHON PHILLIPS ET AL., PROC. OF THE NAT'L ACAD. OF SCIS. OF THE U.S., FACE RECOGNITION ACCURACY OF FORENSIC EXAMINERS, SUPERRECOGNIZERS, AND FACE RECOGNITION ALGORITHMS (Thomas D. Albright ed., 2018), https://obj.umiacs.umd.edu/papers_for_stories/chellappa_facial_recognition.pdf [https://perma.cc/QEB9-PBS8].

111 *See* Geoffrey A. Fowler, *Black Lives Matter Could Change Facial Recognition Forever—If Big Tech Doesn't Stand in the Way*, WASH. POST (June 12, 2020, 11:13 AM), https://www.washingtonpost.com/technology/2020/06/12/facial-recognition-ban [https://perma.cc/23JV-J83U]. Amazon claimed it was due to poor calibration. Russell Brandom, *Amazon's Facial Recognition Matched 28 Members of Congress to Criminal Mugshots*, VERGE (July 26, 2018, 8:02 AM), https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition [https://perma.cc/P3MG-L8HS].

112 One study showed a ninety-eight percent error rate in London. *See* James Vincent, *London Police Chief 'Completely Comfortable' Using Facial Recognition with 98 Percent Error Rate*, VERGE (July 5, 2018, 5:49 AM), https://www.theverge.com/2018/7/5/17535814/uk-face-recognition-police-london-accuracy-completely-comfortable [https://perma.cc/8S78-KGZE]. Another study in London showed an eighty-one percent error rate. *See* Charlotte Jee, *London Police's Face Recognition System Gets It Wrong 81% of the Time*, MIT TECH. REV. (July 4, 2019) https://www.technologyreview.com/f/613922/london-polices-face-recognition-system-gets-it-wrong-81-of-the-time [https://perma.cc/9MSH-E3SE]. Detroit's police chief said that the facial recognition technology used by the department "misidentifies suspects about 96 percent of the time." Timothy B. Lee, *Detroit Police Chief Cops to 96-Percent Facial Recognition Error Rate*, ARSTECHNICA (June 30, 2020, 12:12 PM), https://arstechnica.com/tech-policy/2020/06/detroit-police-chief-admits-facial-recognition-is-wrong-96-of-the-time [https://perma.cc/7R3L-7KHQ].

113 *See, e.g.*, DANIEL E. HO, EMILY BLACK, MANEESH AGRAWALA & LI FEI-FEI, STAN. INST. FOR HUM.-CENTERED A.I., EVALUATING FACIAL RECOGNITION TECHNOLOGY: A PROTOCOL FOR PERFORMANCE ASSESSMENT IN NEW DOMAINS 7 (2020) [hereinafter EVALUATING FACIAL

And the problem is not merely inaccuracy. Studies continuously prove that facial recognition discriminates based on classes like age, race, and gender.[114] And while bias could exist for various cohorts, facial recognition software has been proven to be systemically biased against those with darker skin, providing more false positives than for others.[115] Such bias forms partially due to lack of diversity,[116] as datasets have an over-representation of white men.[117] When white men's data comes in, the computation of white men's data comes out.[118] Another reason is that Black people's images in databases are often of lower quality than those of white people.[119] To put things more simply, facial recognition was proven prone to make more misidentifications—false positives—when applied to Black people.[120]

RECOGNITION TECHNOLOGY], https://hai.stanford.edu/sites/default/files/2020-11/HAI_FacialRecognitionWhitePaper.pdf [https://perma.cc/7A8B-6AV9].

114 *See, e.g.*, Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 1 (2018); Jon Porter, *Federal Study of Top Facial Recognition Algorithms Finds 'Empirical Evidence' of Bias*, VERGE (Dec. 20, 2019, 9:27 AM), https://www.theverge.com/2019/12/20/21031255/facial-recognition-algorithm-bias-gender-race-age-federal-nest-investigation-analysis-amazon (last visited Sept. 11, 2021); Tom Simonite, *When AI Sees a Man, It Thinks 'Official.' A Woman? 'Smile*,*'* WIRED (Nov. 19, 2020, 7:00 AM), https://www.wired.com/story/ai-sees-man-thinks-official-woman-smile [https://perma.cc/ES2B-FVE8] (discussing gender bias in AI).

115 *See* 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/X48D-4L9A].

116 Research on facial recognition algorithms in Asia proved that algorithmic bias can be reduced by using diverse sets of training data. *See* Porter, *supra* note 114.

117 *See* Lohr, *supra* note 115 ("One widely used facial-recognition data set was estimated to be more than 75 percent male and more than 80 percent white, according to another research study."); ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 3–4, 131–42 (2017) (discussing the "black data" problem). For one-to-one matching, an NIST study found "higher rates of false positives for Asian and African American faces relative to images of Caucasians." *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NAT'L INST. OF STANDARDS & TECH. (May 18, 2020), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software [https://perma.cc/WDG4-Q9HY]. For one-to-many matching, the study found "higher rates of false positives for African American females." *Id.*

118 *See* Cino, *supra* note 49, at 1079 ("[T]he result coming out is only as good as the data that went in.").

119 *See* KRISHNAPRIYA K. S, KUSHAL VANGARA, MICHAEL C. KING, VÍTOR ALBIERO & KEVIN BOWYER, CHARACTERIZING THE VARIABILITY IN FACE RECOGNITION ACCURACY RELATIVE TO RACE (2019).

120 *See Facial Recognition Technology: (Part 1): Its Impact on Our Civil Rights and Liberties: Hearing Before the H. Oversight & Reform Comm.*, 116th Cong. 5 (2019) (statement of Neema S. Guliani, Senior Legislative Counsel, ACLU); Hill, *supra* note 90 ("[Facial recognition] has a tendency to deliver false matches for certain groups, like people of color."); Newman, *supra* note 83.

And it is not just false positives but also systematic biases embedded within some of these systems, often caused by developers. For example, some early versions of face-tracking web cameras by Hewlett-Packard were found not to detect Black people.[121] Google's facial recognition software was notoriously known for categorizing two Black men as gorillas.[122] Twitter's neural network was proven racially biased when prioritizing those with lighter skin within cropped preview timelines.[123] This bias applied not only to humans but also cartoon characters and even dogs, preferring the light-colored over the dark-furred.[124]

Racial bias exists in other recognition technology as well. Researchers recently proved similar misidentifications with voice recognition technology,[125] better understanding white males than

---

121 *See* Christian Sandvig, Kevin Hamilton, Karrie Karahalios & Cedric Langbort, *When the Algorithm Itself Is a Racist: Diagnosing Ethical Harm in the Basic Components of Software*, 10 INT'L J. COMMC'N 4972, 4973 (2016).

122 Google's mis-tagging of users as gorillas was not racist per se but rather due to its object recognition algorithm's mode of operation. Google in response blocked words like gorilla from searches and image tags. *See* Alex Hern, *Google's Solution to Accidental Algorithmic Racism: Ban Gorillas*, GUARDIAN (Jan. 12, 2018, 11:04 AM), https://www.theguardian.com/technology/2018/jan/12/google-racism-ban-gorilla-black-people [https://perma.cc/P78M-HP28]; Omer Tene & Jules Polonetsky, *Taming the Golem: Challenges of Ethical Algorithmic Decision-Making*, 19 N.C. J.L. & TECH. 125, 154–55 (2017). Notably, Yonatan Zunger, Google's chief architect of social, said that Google Photos was also "confusing white faces with dogs and seals." Maggie Zhang, *Google Photos Tags Two African-Americans as Gorillas Through Facial Recognition Software*, FORBES (July 1, 2015, 1:42 PM), https://www.forbes.com/sites/mzhang/2015/07/01/google-photos-tags-two-african-americans-as-gorillas-through-facial-recognition-software/#3347aded713d [https://perma.cc/DG87-YDFB].

123 *See* Adam Smith, *Twitter's Photo Algorithm Prioritised White Faces Over Black Ones, Company Says It's 'Got More Analysis to Do*,' INDEPENDENT (Sept. 21, 2020, 2:42 PM), https://www.independent.co.uk/life-style/gadgets-and-tech/twitter-facial-recognition-bias-race-algorithm-photos-b511827.html [https://perma.cc/V3NP-RXG7]. Notably, Twitter's chief design officer argued this was "not a scientific test as it's an isolated example." *Id.*

124 *Id. See generally* Megan Rose Dickey, *Twitter and Zoom's Algorithmic Bias Issues*, TECHCRUNCH (Sept. 21, 2020, 2:58 PM), https://techcrunch.com/2020/09/21/twitter-and-zoom-algorithmic-bias-issues [https://perma.cc/Z24V-BEXY] (discussing algorithmic bias issues on Twitter and Zoom platforms). To be fair, the fact that an algorithm picks white people over Black people is not necessarily tainted trained data or anything necessarily linked to racism. It might be simply that these algorithms are constructed for market purposes, thus choosing to focus on attributions that might draw people's attention more, i.e., shiny white objects. *See* Lucas Theis & Zehan Wang, *Speedy Neural Networks for Smart Auto-Cropping of Images*, TWITTER ENG'G: INFRASTRUCTURE (Jan. 24, 2018), https://blog.twitter.com/engineering/en_us/topics/infrastructure/2018/Smart-Auto-Cropping-of-Images.html [https://perma.cc/ACK2-YJBC] ("[P]eople tend to pay more attention to faces, text, animals, but also other objects and regions of high contrast.").

125 *See* Allison Koenecke et al., *Racial Disparities in Automated Speech Recognition*, 117 PNAS 7684 (2020), https://www.pnas.org/content/117/14/7684 [https://perma.cc/98JH-5WQU]; Cade

others.[126] Gesture recognition technology—identifying bodily movements—was also found to better compute the gestures of males than of women and children, primarily because these systems were trained on men aged eighteen to thirty-five.[127]

While there is much promise in these technologies, they do not yet live up to their promises.[128] Aside from general accuracy and misidentification problems, the use of recognition technology might perpetuate racial bias that already exists in the real world. Applying this fear to the realm of criminal enforcement, in which racial bias and misuse are inherent within the American system, will make enforcement even more flawed and increase means of social control over marginalized communities. To better understand the optimal tradeoff between law enforcement needs and the implications of the error-prone recognition technology, Section II.B turns to discuss why recognition technology is highly risky within the context of law enforcement.

B. *Racial Recognition Within Criminal Enforcement*

The perpetuation and potential enhancement of racial bias becomes more evident within the use of recognition technology. Either programmed with inherent biases or trained or fed with biased data, the use of recognition technology is troubling not only in its commercial aspects but more so in the context of criminal law—the most coercive and liberty-limiting instrument of the law.[129] If we rely on biased systems in the criminal justice system, then crucial decisions on who should be suspected, arrested, indicted, incarcerated, or paroled will be discriminatory.

Metz, *There Is a Racial Divide in Speech-Recognition Systems, Researchers Say*, N.Y. TIMES (Mar. 23, 2020), https://www.nytimes.com/2020/03/23/technology/speech-recognition-bias-apple-amazon-google.html [https://perma.cc/2Z9R-5QAR].

126 Joan Palmiter Bajorek, *Voice Recognition Still Has Significant Race and Gender Biases*, HARV. BUS. REV. (May 10, 2019), https://hbr.org/2019/05/voice-recognition-still-has-significant-race-and-gender-biases [https://perma.cc/XBP3-HJL4].

127 *See* Alina Tugend, *Exposing the Bias Embedded in Tech*, N.Y. TIMES (June 17, 2019), https://www.nytimes.com/2019/06/17/business/artificial-intelligence-bias-tech.html [https://perma.cc/8UB2-82CH].

128 *See* Valentino-DeVries, *supra* note 72 (quoting Clare Garvie suggesting, "It's really being sold as this tool accurate enough to do all sorts of crazy stuff. . . . It's not there yet.").

129 While some individuals might view civil penalties more aversively than criminal sanctions, criminal law is generally considered the most coercive legal instrument that is used as an *ultima ratio*—a last resort. *See* Nils Jareborg, *Criminalization as Last Resort (Ultima Ratio)*, 2 OHIO ST. J. CRIM. L. 521, 526 (2005).

The discussion on using recognition technology in criminal enforcement thus begins with misidentification in general—creating false positives—meaning that the algorithm matching the suspect's image, voice, or gesture with a dataset produces incorrect outcomes. While these mistakes might not sound dramatic in commercial applications, say if a browser or social media account misidentifies a turtle as a rifle,[130] it becomes highly troubling when someone is arrested simply because technology misidentified him or her.[131]

The fear of misidentification increases when error rates are higher for some cohorts, like Black people. To be fair, as the National Institute of Standards and Technology (NIST) demonstrated, it is not only Black people that produce higher error rates in comparison to white people within recognition technology but also Asians and Native Americans, women more than men, and older adults more than middle-aged ones.[132] While issues like gender bias are no less important to research and fight against,[133] racial errors have higher implications in the context of criminal law, as Black people tend to suffer more from biased enforcement, thus forming the focus of this Article.

As established, racial recognition begins with homogeneous developers (mostly white men). It continues with racial bias from flawed datasets. Here is where the source of the *training* data will highly impact the inherent bias of the system.[134] The system will likely be fed with trained data that might cause systematic misidentification for Black individuals more than for white individuals. Next comes the dataset used to identify the suspect. Here is where it would highly depend on whether the police are using their own internal databases or if they are using an external database, often scraped from the internet.

---

130 *See* James Vincent, *Google's AI Thinks This Turtle Looks Like a Gun, Which Is a Problem*, VERGE (Nov. 2, 2017, 8:19 AM), https://www.theverge.com/2017/11/2/16597276/google-ai-image-attacks-adversarial-turtle-rifle-3d-printed [https://perma.cc/7JHY-G46S].

131 As an Amazon spokesperson replied on the use of Amazon's Rekognition, "When using facial recognition for law enforcement activities, we guide customers to set a threshold of at least 95 percent or higher." Sean Hollister, *Amazon Facial Recognition Mistakenly Confused 28 Congressmen with Known Criminals*, CNET (July 26, 2018, 12:45 PM), https://www.cnet.com/news/amazon-facial-recognition-thinks-28-congressmen-look-like-known-criminals-at-default-settings [https://perma.cc/VX8E-UH7U].

132 *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/CR6G-K8EJ].

133 *See* Carsten Schwemmer et al., *Diagnosing Gender Bias in Image Recognition Systems*, 6 SOCIUS: SOCIO. RSCH. DYNAMIC WORLD 1 (2020).

134 *See* Anupam Chander, *The Racist Algorithm?*, 115 MICH. L. REV. 1023, 1036 (2017) ("Even facially neutral algorithms will produce discriminatory results because they train and operate on the real world of pervasive discrimination.").

If the police use their own datasets, then some cohorts, like Black men, might be at a severe disadvantage, as these datasets are often compiled from arrest records and police-generated images, like mugshots, that initially contain higher rates of Black people compared to the rest of the general population,[135] thus making them more susceptible to the use of these biometric systems, and thereby, also more prone to mistakes in identification.[136] Thus, Black people are more likely than others to be in the compared dataset, meaning that they have higher chances of being identified from this database.[137] Using the internet as a source for the dataset will have to be examined specifically in light of potential biases within it. In that instance, the internet might be advantageous for identification purposes (unlike for data-training purposes) for Black people, as they are generally less represented online.[138]

Adding to this alarming list of biases are institutional and individual police racism. Criminal enforcement is often prone to target communities of color, and along with various unlawful misconduct,[139] racial disparities in policing have been statistically proven in many police practices.[140] Race and ethnicity, for that matter, play an unfortunate and historic role within the criminal justice system, as

---

135 *See* Mayson, *supra* note 104, at 2229–30.

136 *See* Newman, *supra* note 83; Lohr, *supra* note 115.

137 *See* James Vincent, *IBM Hopes to Fight Bias in Facial Recognition with New Diverse Dataset*, VERGE (June 27, 2018, 10:22 AM), https://www.theverge.com/2018/6/27/17509400/facial-recognition-bias-ibm-data-training (last visited Sept. 12, 2021).

138 *See, e.g.*, Sarah Kaufman, *White People Are the Default for Google Images*, VOCATIV (May 26, 2015, 12:26 PM), https://www.vocativ.com/195780/white-people-are-the-default-for-google-images/index.html [https://perma.cc/TS9K-HPNU].

139 *See generally* Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. REV. ONLINE 192 (2019) (discussing "dirty data" as data derived or influenced by corrupt, biased, and unlawful practices, focusing on the way the data affects predictive policing systems).

140 *See, e.g.*, Emma Pierson et al., *A Large-Scale Analysis of Racial Disparities in Police Stops Across the United States*, 4 NATURE HUM. BEHAV. 736 (2020), https://5harad.com/papers/100M-stops.pdf [https://perma.cc/3SX6-C6YY]; Barry Friedman, *Disaggregating the Police Function*, 169 U. PA. L. REV. 925, 928 (2021); Mark Berman & Wesley Lowery, *The 12 Key Highlights from the DOJ's Scathing Ferguson Report*, WASH. POST (Mar. 4, 2015, 3:11 PM), https://www.washingtonpost.com/news/post-nation/wp/2015/03/04/the-12-key-highlights-from-the-dojs-scathing-ferguson-report [https://perma.cc/5YQD-NNAR] (highlighting and exemplifying racist police practices as indicated within a searing DOJ report into policing and court practices in the Missouri city); Alisa Tiwari, *Disparate-Impact Liability for Policing*, 129 YALE L.J. 252, 256 (2019) ("[R]acial disparities often result from institutionalized police practices . . . .").

many researchers have proven.[141] Predictive policing, the application of analytical techniques to predict crimes and identify targets, was also found to be used disproportionally against historically over-policed communities.[142] Simply put, when it comes to policing, some groups, most notably Black people, receive dissimilar treatment.[143]

Such dissimilar treatment is another factor that must be considered within the notion of *racial recognition* on both institutional and individual levels. The institutional level mainly represents how racism on the individual level was historically translated into police practices that generally mistreat minorities and communities of color.[144] For example, such institutional bias could stem from general police practices or guidelines affected by individual bias. Specifically in the context of recognition technology, institutional decisions on where to place cameras (to obtain probe images of suspects) or where police officers equipped with BWCs patrol (regardless of individual bias) could highly impact what data enters the system to begin with.

From an individual perspective, the fact that, statistically, there are other biased humans in the system—police officers—will increase the likelihood for racism. While surely not every police officer is racist, the history of racial policing raises a substantial fear. This fear not only represents another factor that could increase chances of racism and dissimilar treatment between cohorts but also implies that the use of recognition technology within the realm of criminal enforcement is risky regardless of whether the technology yields inaccurate or biased results.

---

141 *See generally* DAVID A. HARRIS, PROFILES IN INJUSTICE: WHY RACIAL PROFILING CANNOT WORK (2003) (demonstrating that racial profiling is not only morally or legally wrong but also ineffectual at preventing crime); MARC MAUER, RACE TO INCARCERATE (rev. ed. 2006) (detailing the overreliance on imprisonment to stem economic and social problems); Tracey Maclin, *Race and the Fourth Amendment*, 51 VAND. L. REV. 333, 333 (1998) ("In America, police targeting of black people for excessive and disproportionate search and seizure is a practice older than the Republic itself.").

142 *See* Kristian Lum & William Isaac, *To Predict and Serve?*, SIGNIFICANCE MAG. (Oct. 2016), https://rss.onlinelibrary.wiley.com/doi/epdf/10.1111/j.1740-9713.2016.00960.x [https://perma.cc/5XC8-MB7Z].

143 *See* Kia Makarechi, *What the Data Really Says About Police and Racial Bias*, VANITY FAIR (July 14, 2016), http://www.vanityfair.com/news/2016/07/data-police-racial-bias [https://perma.cc/AP8Y-F9SB]. *See generally* MICHELLE ALEXANDER, THE NEW JIM CROW: MASS INCARCERATION IN THE AGE OF COLORBLINDNESS 2 (10th anniversary ed. 2020) ("We have not ended racial caste in America; we have merely redesigned it."). In the context of traffic offenses, see David A. Harris, "*Driving While Black" and All Other Traffic Offenses: The Supreme Court and Pretextual Traffic Stops*, 87 J. CRIM. L. & CRIMINOLOGY 544 (1997); Tiwari, *supra* note 140, at 254–56.

144 *See* Makarechi, *supra* note 143.

In other words, accuracy is only one problem within racial recognition. Even if the algorithm learns how to "de-bias" its results, it does not "de-bias" humans. The combination is alarming, as a biased system combined with a racist law enforcement agent or institutional racism might not only perpetuate racial bias and increase social inequalities but might even become a tool for legitimizing legal action against some people—all within what might appear as a justified and legitimate cause of action.

These technologies might thus be misused to violate human rights and, most notably, target minorities and communities of color.[145] Consider the broad implications of misusing a technology that could specifically target individuals based on their age, gender, and skin tone.[146] China was reported to use facial recognition technology for racial profiling against the Uighur Muslim minority,[147] while reporters indicate that the private sector is developing a technology that would enable the government to receive alerts when detecting individuals from this group.[148] A substantial fear is that enforcement agencies will digitally point their efforts within minority neighborhoods and equip them with more cameras to be used and misused.[149]

And this misuse could extend far beyond the realm of criminal law. The use of recognition technology in the public sphere might impact many constitutional or basic human rights, such as privacy, free speech, free association, free movement, and due process.[150] Abusing the power

---

145 *See* Letter from the ACLU to Jeffrey P. Bezos, Founder & Chief Exec. Officer, Amazon.com, Inc. (May 22, 2018), https://www.aclunc.org/docs/20180522_AR_Coalition_Letter.pdf [https://perma.cc/8TG3-DRFT].

146 IBM was reported to use footage from NYPD CCTV cameras to develop technology that identifies individuals based on bodily characteristics. *See* James Vincent, *IBM Secretly Used New York's CCTV Cameras to Train Its Surveillance Software*, VERGE (Sept. 6, 2018, 10:24 AM), https://www.theverge.com/2018/9/6/17826446/ibm-video-surveillance-nypd-cctv-cameras-search-skin-tone [https://perma.cc/D5HK-H6TH].

147 *See* Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. TIMES (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html [https://perma.cc/U8NC-KX55].

148 *See* Drew Harwell & Eva Dou, *Huawei Tested AI Software that Could Recognize Uighur Minorities and Alert Police, Report Says*, WASH. POST (Dec. 8, 2020, 10:30 AM), https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says [https://perma.cc/M3FV-QQAF] (reporting that Huawei tested an AI facial recognition technology that could send automated "Uighur alarms" to government authorities).

149 *See* Fowler, *supra* note 111 ("[M]ore cameras could be pointed at minority neighborhoods, used to target immigrants or even people who join protests about police brutality.").

150 *See* Garvie, *supra* note 9; Evan Selinger & Woodrow Hartzog, *What Happens When Employers Can Read Your Facial Expressions?*, N.Y. TIMES (Oct. 17, 2019),

afforded by this technology could potentially lead to identifying public protesters or people at rallies in general,[151] which are probably at unprecedented levels these days.

Thus, racial recognition affects much more than selective enforcement of Black people. It might be misused as a powerful tool for social control over anyone, but most likely marginalized communities and perhaps those supporting them in pursuing their causes. Think of protesters that are targeted by these technologies.[152] This becomes frightening especially when these protests are exactly due to police racism, such as those that arose from the killing of George Floyd in 2020.[153] Not surprisingly then, minorities are less trusting than the general public of police use of facial recognition technology.[154]

One of the fears of using this technology under the umbrella of public safety is that of becoming a surveillance state. Suppose, arguendo, that the police use recognition software to obtain full surveillance on individuals.[155] In its examples of its Rekognition software, Amazon demonstrated how the input photograph could come

---

https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html [https://perma.cc/8TTW-MS8H].

151 NYPD claims that it does not use facial recognition to monitor and identify people in crowds or at rallies. *NYPD Questions and Answers: Facial Recognition*, *supra* note 73.

152 New York City Mayor, Bill de Blasio, said that the NYPD never uses facial recognition to "undermine or affect public expression or public protest." James Vincent, *NYPD Used Facial Recognition to Track Down Black Lives Matter Activist*, VERGE (Aug. 18, 2020, 5:26 AM), https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram (last visited Sept. 12, 2021).

153 George Floyd was an unarmed Black man that was killed on May 25, 2020, by a white officer that knelt on his neck in Minneapolis. *See* Derrick Bryson Taylor, *George Floyd Protests: A Timeline*, N.Y. TIMES (Mar. 28, 2021), https://www.nytimes.com/article/george-floyd-protests-timeline.html [https://perma.cc/DL4Q-GBEJ]. Notably, following the death of George Floyd, Congress proposed a bill to reduce racist policing practices while increasing law enforcement accountability. *See* George Floyd Justice in Policing Act of 2020, H.R. 7120, 116th Cong. (2020).

154 AARON SMITH, PEW RSCH. CTR., MORE THAN HALF OF U.S. ADULTS TRUST LAW ENFORCEMENT TO USE FACIAL RECOGNITION RESPONSIBLY (2019).

155 Upon introducing its Rekognition software, Amazon specifically noted that Amazon Rekognition Video also allows you "to easily and quickly review hours of video footage to search for persons of interest, track their movement and detect their activities." Elizabeth Weise, *Amazon Should Stop Selling Facial Recognition Software to Police, ACLU and Other Rights Groups Say*, USA TODAY (May 25, 2018, 12:42 PM), https://www.usatoday.com/story/tech/2018/05/22/aclu-wants-amazon-stop-selling-facial-recognition-police/633094002 [https://perma.cc/4FTK-Y2R4]; *see* Neema Singh Guliani, *The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database*, ACLU (June 7, 2019, 3:15 PM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through [https://perma.cc/7TAC-C2WN] ("[Facial recognition] gives government agencies the unprecedented power to track who we are, where we go, and who we know.").

from a body camera worn by a police officer.[156] The state might thus use an array of available technological tools like BWCs,[157] which were adopted in part to reduce discrimination,[158] or drones equipped with technology like portable spying devices.[159]

And this is where undocumented immigrants or Black activists might again be at a severe disadvantage compared to the general population.[160] In practice, both Miami police and the NYPD used facial recognition to track down Black Lives Matter activists.[161] Baltimore police were reported to use facial recognition to identify protesters by linking their images to their social media profiles.[162] In a weekly public report, the Detroit Police Department admitted using its facial recognition software against Black people in ninety-seven percent of its facial recognition requests.[163]

---

156 *See* Julia Carrie Wong, *'Recipe for Authoritarianism': Amazon Under Fire for Selling Face-Recognition Software to Police*, GUARDIAN (May 22, 2018, 7:55 PM), https://www.theguardian.com/technology/2018/may/22/amazon-rekognition-facial-recognition-police [https://perma.cc/PY8M-FTUW].

157 *See generally* Ringrose, *supra* note 106; Mary D. Fan, *Privacy, Public Disclosure, Police Body Cameras: Policy Splits*, 68 ALA. L. REV. 395, 407–09 (2016); Karson Kampfe, Note, *Police-Worn Body Cameras: Balancing Privacy and Accountability Through State and Police Department Action*, 76 OHIO ST. L.J. 1153 (2015).

158 The use of BWCs was adopted due to the shooting of unarmed Black men by police and the ruling of a federal court to reduce discrimination. *See* Floyd v. City of New York, 959 F. Supp. 2d 668, 685 (S.D.N.Y. 2013); Kelly Blount, *Body Worn Cameras with Facial Recognition Technology: When It Constitutes a Search*, 3 CRIM. L. PRAC. 61, 63 (2017).

159 *See* Ringrose, *supra* note 106, at 61; Ian Wren & Scott Simon, *Body Camera Maker Weighs Adding Facial Recognition Technology*, NPR (May 12, 2018, 8:07 AM), https://www.npr.org/2018/05/12/610632088/what-artificial-intelligence-can-do-for-local-cops [https://perma.cc/P843-CBW2]; Zolan Kanno-Youngs, *U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance*, N.Y. TIMES (June 19, 2020), https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html [https://perma.cc/LBF3-SVS9].

160 *See* ACLU, *supra* note 145.

161 *See* Vincent, *supra* note 152; Kate Cox, *Cops in Miami, NYC Arrest Protesters from Facial Recognition Matches*, ARSTECHNICA, (Aug. 19, 2020, 4:45 PM), https://arstechnica.com/tech-policy/2020/08/cops-in-miami-nyc-arrest-protesters-from-facial-recognition-matches [https://perma.cc/TY79-KR59]; *Facial Recognition Technology: (Part 1): Its Impact on Our Civil Rights and Liberties: Hearing Before the H. Oversight & Reform Comm.*, 116th Cong. 20–21, 21 n.71 (2019) [hereinafter *Ferguson Testimony*] (written testimony of Professor Andrew Guthrie Ferguson).

162 This was reported to be used against protesters of the mistreatment and death of Freddie Gray—a twenty-five-year-old Black man who died from a spinal cord injury he allegedly sustained while in police custody. *See* Shira Ovide, *A Case for Banning Facial Recognition*, N.Y. TIMES (Jan. 31, 2021), https://www.nytimes.com/2020/06/09/technology/facial-recognition-software.html [https://perma.cc/U56D-TAVK].

163 *See* DETROIT POLICE DEP'T, DETROIT POLICE DEPARTMENT: WEEKLY REPORT ON FACIAL RECOGNITION (2020), https://detroitmi.gov/sites/detroitmi.localhost/files/2020-06/DPD%20

Notably, the fear of racist algorithms in criminal law enforcement was raised in the context of risk assessments, well before the advent of recognition technology.[164] The proprietary risk assessment AI system known as COMPAS, a tool designed to assess recidivism that is often used in sentencing by some courts and affirmed by the Wisconsin Supreme Court,[165] was proven to yield biased results against Black people,[166] among other problems.[167]

In the context of recognition technology, while enforcement agencies including the NYPD claim there were no false arrests due to facial recognition misidentification,[168] there is already proof in other departments. In June 2020, a Black male was falsely arrested in Detroit due to facial recognition.[169] Only upon spending thirty hours in custody was the suspect released on bail, with the charges eventually being

---

Report%20on%20Facial%20Recognition%20Usage%20%20061520%20-%20062120.pdf [https://perma.cc/S2KR-Q7KP] (reporting facial recognition use for the week of June 22, 2020).

164 *See, e.g.*, FILIPPO RASO, HANNAH HILLIGOSS, VIVEK KRISHNAMURTHY, CHRISTOPHER BAVITZ & LEVIN KIM, ARTIFICIAL INTELLIGENCE & HUMAN RIGHTS: OPPORTUNITIES & RISKS 22–24 (2018). *See generally* Mayson, *supra* note 104 (arguing that the source of racial inequality in risk assessment lies in the nature of prediction itself).

165 *See* State v. Loomis, 881 N.W.2d 749 (Wis. 2016); Adam Liptak, *Sent to Prison by a Software Program's Secret Algorithms*, N.Y. TIMES (May 1, 2017), https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html [https://perma.cc/4GCF-DACP].

166 COMPAS, an acronym for Correctional Offender Management Profiling for Alternative Sanctions, is used in many U.S. jurisdictions for recidivism assessments. *See* Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks.*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/KX6U-447H]. Melissa Hamilton also proved that COMPAS "is not well calibrated for Hispanics." Melissa Hamilton, *The Biased Algorithm: Evidence of Disparate Impact on Hispanics*, 56 AM. CRIM L. REV. 1553, 1577 (2019).

167 Some scholars, for instance, have criticized the accuracy of COMPAS, suggesting that it was "no more accurate or fair than predictions of people with little to no criminal justice expertise." *See* Julia Dressel & Hany Farid, *The Accuracy, Fairness, and Limits of Predicting Recidivism*, 4 SCI. ADVANCES 1, 3 (2018), https://www.researchgate.net/publication/322573250_The_accuracy_fairness_and_limits_of_predicting_recidivism (last visited Sept. 13, 2021). *See generally* Huq, *supra* note 35, at 1080–82.

168 *NYPD Questions and Answers: Facial Recognition*, *supra* note 73 ("The NYPD knows of no case in New York City in which a person was falsely arrested on the basis of a facial recognition match.").

169 *See* 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/Q2G4-GRJS]; Bobby Allyn, *'The Computer Got It Wrong': How Facial Recognition Led to False Arrest of Black Man*, NPR (June 24, 2020, 8:00 AM), https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig [https://perma.cc/4UQR-6VQV].

dropped.[170] Only a few days later, another Black man was misidentified.[171]

Thus, the use of recognition technology, primarily facial recognition, could lead to discrimination against some people and, perhaps most profoundly, Black people. When racial disparities already exist in policing, and when technology and data are tainted with racism, crucial decisions become even more discriminatory than within traditional policing. Even if we eliminate any embedded biases within the system—something currently highly improbable—there are still checks and balances to be set when using this technology to ensure it is not misused against some groups or individuals.[172] In other words, algorithmic recognition technology in use of law enforcement might become racial profiling tools. They might operate to identify race, not face, thereby improperly correlating race to criminality, and they might replicate and exacerbate systemic inequalities and discrimination against individuals on the basis of race. Part III focuses on the current legal regime that governs racial recognition and then turns to discuss how to properly regulate it.

III. REGULATING RECOGNITION TECHNOLOGY IN LAW ENFORCEMENT

Police use of recognition technology raises a host of legal questions, with emphasis on its negative impact on human rights and liberties. While recognition technology could aid police officers in performing their legal mandates, the risks of errors and misuse might halt the use of recognition technology for criminal enforcement purposes, at least until its perceived shortcomings can be substantially reduced. But as the future, in this respect, is just around the corner, the use of recognition technology for identification necessitates rethinking the permissible framework that law enforcement must act within, including the problems that stem from the use of this technology, even if it becomes "neutral" or otherwise unbiased per se.

---

170 Sidney Fussell, *A Flawed Facial-Recognition System Sent This Man to Jail*, WIRED (June 24, 2020, 7:30 PM), https://www.wired.com/story/flawed-facial-recognition-system-sent-man-jail [https://perma.cc/87WN-5MVL].

171 *See* Press Release, ACLU, ACLU Statement on Second Wrongful Arrest Due to Face Recognition Technology (July 10, 2020).

172 *See* Ovide, *supra* note 162 ("There's also an imbalance of power. Facial recognition can be completely accurate, but it can still be used in a way that is detrimental to certain groups of people.").

A. *The Legality of Recognition Technology Within Criminal Enforcement*

There are many benefits of data-driven police practices in general and of recognition technology specifically.[173] If it functions properly, recognition technology could aid law enforcement agents in identifying suspects and subsequently in the investigation and prosecution of crimes.[174] It could also aid the police in identifying suspects of crimes when victims are unable to do so, e.g., Alzheimer's patients.[175] Recognition technology could even aid in rescuing human trafficking victims, finding missing children, or aiding disoriented individuals.[176] Recognition technology could also aid in reducing concerns about bias, as these systems often perform automated tasks based on numeric analysis of features and patterns, regardless of race.[177] In a utopian future, recognition technology could aid in increasing public safety

---

173 *See, e.g.*, Ferguson, *supra* note 30, at 503 (listing benefits of "Big Data" policing).

174 *See, e.g.*, *NYPD Questions and Answers: Facial Recognition*, *supra* note 73 ("In 2019, the Facial Identification Section received 9,850 requests for comparison and identified 2,510 possible matches, including possible matches in 68 murders, 66 rapes, 277 felony assaults, 386 robberies, and 525 grand larcenies."). In the United Kingdom it was reported that facial recognition technology aided in the identification of Russian assassins that poisoned a spy on UK soil. *See* Hollister, *supra* note 131. As reported by at least one private company, the use of facial recognition technology, combined with images from the internet, led to the arrest and charging of a man that did not appear in any government database, and it also aided in identifying many suspects of crimes. The company also claims that:

> the app helped identify a range of individuals: a person who was accused of sexually abusing a child whose face appeared in the mirror of someone's else gym photo; the person behind a string of mailbox thefts in Atlanta; a John Doe found dead on an Alabama sidewalk; and suspects in multiple identity-fraud cases at banks.

See Hill, *supra* note 90. For more examples of facial recognition use by enforcement agencies, see Julie Bosman & Serge F. Kovaleski, *Facial Recognition: Dawn of Dystopia, or Just the New Fingerprint?*, N.Y. TIMES (May 18, 2019), https://www.nytimes.com/2019/05/18/us/facial-recognition-police.html [https://perma.cc/APW4-NKWJ].

175 Consider that Alzheimer's patients might be incapable of identifying crime victims (and perhaps themselves), along with other individuals that might be unable to identify suspects for various reasons. *See* Valentino-DeVries, *supra* note 72.

176 Even upon announcing that it will stop providing law enforcement agencies with their facial recognition tool, as further mentioned, Amazon keeps providing this technology "to help rescue human trafficking victims and reunite missing children with their families." Allyn, *supra* note 60; *see* Tom Simonite, *How Facial Recognition Is Fighting Child Sex Trafficking*, WIRED (June 19, 2019, 7:00 AM), https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/amp [https://perma.cc/LLE2-QL7R]; *Facial Recognition: Top 7 Trends (Tech, Vendors, Markets, Use Cases & Latest News)*, THALES (June 24, 2021), https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition [https://perma.cc/HAA4-YDN6].

177 *See* Newman, *supra* note 83.

while potentially reducing the effects of inherent human biases and prejudices in enforcement.

To some extent, it might sound farfetched that the police would be denied the possibility of identifying suspects or finding missing individuals.[178] But while denying the police from using any technology that would aid them in identifying suspects might strike some as unnecessarily raising barriers for proper police work, the drawbacks of racial recognition, along with other human rights and liberties that might be violated, are too significant. To understand what regulatory gaps need to be filled in the legal regime that governs racial recognition, the following Section discusses constitutional protection on the one hand and federal and state laws on the other.

1. Constitutional Aspects

The legal analysis of racial recognition begins with the Constitution or, more precisely, with some of its amendments. The use of recognition technology in criminal enforcement raises constitutional concerns around the rights granted under the First, Fourth, Fifth, and Fourteenth Amendments.[179] Unfortunately, as further discussed, these amendments are currently highly limited, mostly inapplicable, in regulating racial recognition.

The first candidate for governing racial recognition is the First Amendment. Depending on how recognition technology is deployed, one concern regarding law enforcement's use of recognition technology for purposes of identification is that it will create a chilling effect on freedom of speech and association as protected by the First Amendment.[180] When the police use such technology, it might infringe upon individuals' First Amendment rights to anonymous speech,[181] as

---

178 Whether police officers are barred from generally demanding identity information from individuals is questionable regardless of technology. While the Supreme Court previously held that seizing individuals simply to ascertain identity is prohibited, other cases left this somewhat unclear. *See* Brown v. Texas, 443 U.S. 47, 52 (1979); Wayne A. Logan, *Policing Police Access to Criminal Justice Data*, 104 IOWA L. REV. 619, 635–39 (2019) (discussing the "identity exception").

179 U.S. CONST. amends. I, IV, V, XIV; *see* ERIK LEARNED-MILLER, VICENTE ORDÓÑEZ, JAMIE MORGENSTERN & JOY BUOLAMWINI, FACIAL RECOGNITION TECHNOLOGIES IN THE WILD: A CALL FOR A FEDERAL OFFICE 11–12 (2020) [hereinafter FACIAL RECOGNITION TECHNOLOGIES IN THE WILD].

180 *See* U.S. CONST. amend. I.

181 *See, e.g.*, Talley v. California, 362 U.S. 60 (1960) (explaining that compelling identification of anonymous speech might deter peaceful discussions of important matters); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995); Ringrose, *supra* note 106, at 62–63.

individuals might refrain from engaging in expressive action or association out of fear of being associated and identified within a specific context—often political or religious.[182]

As this Article focuses on identification, when it comes to merely identifying individuals with recognition technology, it is not clear if the First Amendment could be invoked. Merely identifying individuals is not a First Amendment violation per se, and even surveillance of speech might not violate the First Amendment.[183] Moreover, even if the use of this technology will lead to retaliatory arrests, as one might fear within the context of racial recognition, it would be highly difficult for plaintiffs to prevail on a First Amendment claim, as the existence of probable cause would defeat such a claim.[184] Thus, without using live facial recognition to locate individuals in the public sphere, the First Amendment would be rather limited to regulating racial recognition in the context of identification.

The second candidate is the Fourth Amendment, which protects against unreasonable searches and seizures—often a primary tool to regulate police conduct.[185] As the Supreme Court ruled in *Katz v. United States*, violating a reasonable expectation of privacy constitutes a search, which then requires a warrant,[186] unless an exception exists.[187] The reasonable expectation of privacy test is both subjective, i.e., whether an

---

182 *See* Julian R. Murphy, *Chilling: The Constitutional Implications of Body-Worn Cameras and Facial Recognition Technology at Public Protests*, 75 WASH. & LEE L. REV. ONLINE 1, 25–27 (2018); Memorandum from Majority Staff to Members of the Comm. on Oversight & Reform 5 (May 20, 2019), https://docs.house.gov/meetings/go/go00/20190522/109521/hhrg-116-go00-20190522-sd002.pdf [https://perma.cc/TU2J-PKQR].

183 *See* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 466 (1958); Donohue, *supra* note 46, at 543–51; GARVIE, BEDOYA & FRANKLE, *supra* note 1, at 41–44 (summarizing the First Amendment implications of facial recognition technology use).

184 The existence of probable cause would defeat such claims, that is, unless plaintiffs can prove the "atypical-arrest exception." *First Amendment—Freedom of Speech—Retaliatory Arrest*—Nieves v. Bartlett, 133 HARV. L. REV. 272 (2019); *see* Nieves v. Bartlett, 139 S. Ct. 1715, 1722, 1725, 1727 (2019). *See generally* John S. Clayton, Note, *Policing the Press: Retaliatory Arrests of Newsgatherers After* Nieves v. Bartlett, 120 COLUM. L. REV. 2275 (2020).

185 For more on the Fourth Amendment in the context of criminal law, see generally Richard M. Leagre, *The Fourth Amendment and the Law of Arrest*, 54 J. CRIM. L. & CRIMINOLOGY 393 (1963).

186 *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

187 Perhaps most relevant in recognition technology and criminal enforcement would be either the exigent circumstances exception or the special needs exception. For a discussion on the potential exceptions to the warrant requirements in the context of facial recognition technology, see Murphy, *supra* note 182, at 17–22.

actual expectation of privacy exists, and objective, i.e., whether society recognizes the expectation as "reasonable."[188]

Subsequent case law has clarified when a search is considered reasonable. After *Katz*, the Supreme Court began widening the scope of the Fourth Amendment to digital technology.[189] In the context of criminal law, police officers are allowed to stop suspects and frisk them when they have a "reasonable suspicion" (a lower standard than probable cause) that the person has committed, is committing, or is about to commit a crime.[190] When making decisions, police officers must "point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion."[191] They must have an individualized suspicion; otherwise, there is no probable cause for the search.[192] Police officers can also make mistakes in identification, especially if the decision is "an objectively 'reasonable good-faith belief' that their conduct is lawful" or when it is an isolated event of negligence.[193] They cannot, however, make intentional or systemic errors.[194]

When not taking technology into account, recognizing one's face, voice, or gestures does not constitute a Fourth Amendment search.[195] When no physical invasion occurs, inspection by the naked eye is

---

188 *See Katz*, 389 U.S. at 361 (Harlan, J., concurring); Smith v. Maryland, 442 U.S. 735, 740 (1979).

189 *See* United States v. Jones, 565 U.S. 400 (2012) (holding that the installation and use of a GPS device constitutes a Fourth Amendment search). Movements revealed by third-party cell-site records had been held as constituting a search, and "the Government must generally obtain a warrant supported by probable cause before acquiring such records." *See* Carpenter v. United States, 138 S. Ct. 2206, 2220–21 (2018) ("[T]he fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection."); *see also* Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205 (2018).

190 *See* Terry v. Ohio, 392 U.S. 1, 19–21 (1968); Heien v. North Carolina, 574 U.S. 54 (2014). *See generally* Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 338–40 (2015).

191 *Terry*, 392 U.S. at 21; Ferguson, *supra* note 53, at 1174.

192 *See* Chandler v. Miller, 520 U.S. 305, 308 (1997); Selbst, *supra* note 35, at 154 ("Individualized suspicion is at the core of the Fourth Amendment's probable cause requirement.").

193 Davis v. United States, 564 U.S. 229, 238 (2011) (quoting United States v. Leon, 468 U.S. 897, 909 (1984)); Ferguson, *supra* note 53, at 1169–70.

194 *See* Ferguson, *supra* note 53, at 1169–70.

195 *See* United States v. Dionisio, 410 U.S. 1, 14 (1973) ("Like a man's facial characteristics, or handwriting, his voice is repeatedly produced for others to hear. No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world."); Ferguson, *supra* note 53, at 1123–24.

generally permissible.[196] In addition, subjective racial discrimination in conducting a search has been held irrelevant to the Fourth Amendment, especially when the search was otherwise lawful.[197] Generally speaking, race is considered outside the scope of the Fourth Amendment.[198]

Still, the main question within the analysis is that of privacy expectations in the context of identification when taking technology into account. This analysis begins with the probe photo of the suspect as technologically captured.[199] Even lacking suspicion, the mere capturing of such information is reasonable when obtained from a public place, which has traditionally afforded fewer privacy protections than the private sphere.[200] While the Supreme Court famously noted that the Fourth Amendment "protects people [and] not places,"[201] there is little expectation of privacy when individuals go out to a public place to begin with,[202] that is, unless they make efforts to shield such information from public view.[203] It is generally also legal for anyone, including law enforcement agents, to photograph people in public.[204]

---

196 Some have dubbed this the "naked eye doctrine." For a discussion on this doctrine, see Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo's *Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393 (2002); Florida v. Riley, 488 U.S. 445, 450–52 (1989).

197 *See* Whren v. United States, 517 U.S. 806, 811 (1996) (holding that the motivation for stopping two men for involvement in illegal drug-dealing activity was immaterial due to a traffic violation); Selbst, *supra* note 35, at 145; Maclin, *supra* note 141, at 336–38. For criticism of *Whren v. United States*, see Kevin R. Johnson, *How Racial Profiling in America Became the Law of the Land*: United States v. Brignoni-Ponce *and* Whren v. United States *and the Need for Truly Rebellious Lawyering*, 98 GEO. L.J. 1005, 1007 (2010).

198 *See, e.g.*, Devon W. Carbado, *(E)racing the Fourth Amendment*, 100 MICH. L. REV. 946, 1033 (2002) ("[F]or purposes of Fourth Amendment law, race does not matter.").

199 Notably, in other recognition technology, the input could also be voice or gesture.

200 *See, e.g.*, Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 495–96 (2006) ("The law often recognizes surveillance as a harm in private places but rarely in public places.").

201 Katz v. United States, 389 U.S. 347, 351 (1967).

202 *See* United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."); Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 529 (2017) ("[T]here is no reasonable expectation of privacy in one's movements in public space."). *See generally* Joel R. Reidenberg, *Privacy in Public*, 69 U. MIA. L. REV. 141 (2014).

203 *See* Murphy, *supra* note 182, at 14–15. Notably, however, hiding your face in public, and even within the private property of another, might even be illegal in some states. *See, e.g.*, GA. CODE ANN. § 16-11-38 (2010).

204 *See* United States v. Farias-Gonzalez, 556 F.3d 1181, 1188 (11th Cir. 2009) ("The police can obtain both photographs and fingerprints without conducting a search under the Fourth Amendment."); Megan Behrman, Note, *When Gangs Go Viral: Using Social Media and Surveillance Cameras to Enhance Gang Databases*, 29 HARV. J.L. & TECH. 315, 318 (2015) ("[S]urveillance cameras set up by the state that only record people in the public sphere also do

Perhaps the smartification of the public sphere will lead to different conclusions in the future; as articulated by Chief Justice John Roberts, "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere."[205] Currently, we generally surrender our faces, voices, and other biometric features when going out.

Second is the question of searching within databases. If the police use their own databases, whether composed of mugshots, driver's license photos, passport photos, or otherwise legally obtained photos from investigations, such use is unlikely to constitute a Fourth Amendment violation.[206] Unless otherwise barred by state law, law enforcement agents can legally use Department of Motor Vehicles photos.[207] If the police legally obtain publicly available online information, as they often do, then searching within such a database is generally permissible.[208]

Other databases might be privately owned. Under current Supreme Court jurisprudence, it is not a Fourth Amendment violation when the data held by third parties is voluntarily shared with them.

---

not infringe on any Fourth Amendment rights."). Photographing people in public is generally legal, unless someone knowingly and intentionally captures a person's "private area" ("the naked or undergarment clad genitals, pubic area, buttocks, or female breast") without consent. *See* 18 U.S.C. § 1801 (2004).

205 Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018); *see also* Levinson-Waldman, *supra* note 202 (suggesting a blueprint comprising six factors to consider when applying the Fourth Amendment to public surveillance technologies in the digital age).

206 *See* Ferguson, *supra* note 53, at 1151 ("As a general matter, there does not appear to be a strong claim that photographs taken by police or the government infringe on an expectation of privacy.").

207 *See* 18 U.S.C. § 2721(b)(1) (2000); Phillips v. Bailey, 337 F. Supp. 2d 804, 806 (W.D. Va. 2004); KELSEY Y. SANTAMARIA, CONG. RSCH. SERV., R46541, FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT: SELECT CONSTITUTIONAL CONSIDERATIONS 15 (2020) [hereinafter SELECT CONSTITUTIONAL CONSIDERATIONS]. Some pointed out an ethical dilemma in using these photos, as they are not considered public records and there was no consent of citizens that it will be used in this manner. *See* Bosman & Kovaleski, *supra* note 174.

208 Police officers routinely collect and analyze data that was obtained from social media accounts. *See* Joh, *supra* note 45, at 24. Even when internal policies guide police officers to abstain from using images from social media accounts, it was difficult for some to comply with these policies. While a spokesperson for the NYPD said that "[t]he NYPD uses facial recognition as a limited investigative tool, comparing a still image from a surveillance video to a pool of lawfully possessed arrest photos," they had likely used a photo taken from the Instagram account of an individual for purposes of identification, found within a document titled "Facial Identification Section Informational Lead Report." Considering this discovery, New York City Mayor Bill de Blasio announced that "his office would reexamine the standards for police use of facial recognition." *See* Vincent, *supra* note 152. Other online police practices were also held lawful. *See, e.g.*, People v. Pride, 242 Cal. Rptr. 3d 297 (Ct. App. 2019) (holding that there was no Fourth Amendment violation when undercover police officers pose as a false friend and obtain incriminating information from a social media page).

Under this so-called third-party doctrine, there is no reasonable expectation of privacy within these images, which in turn are exempt from the protections afforded by the Fourth Amendment.[209] This analysis might change if the algorithm produces more than mere identification, i.e., reveals metadata and information about suspects that is embedded within the media (such as location details or other contextual information about them).[210] Here, the public might be unaware of such metadata and might not expect that it would be divulged to third parties. In the case of mere identification, this becomes less relevant, however.

Finally comes the algorithm used by the police. As these technologies are often offered by the market, a valid Fourth Amendment claim might arise if such "sense-enhancing" technology is not provided to the public.[211] On the one hand, the public can use various recognition services.[212] One such example is PimEyes, a website that grants anyone the opportunity to upload a probe photo and search within its own database that is composed of people's faces scraped from the internet.[213] Truly, if functioning properly, websites like PimEyes pose difficult Fourth Amendment questions. If they are widely available, barring the police from using such websites seems not only impractical in the sense that it would be highly difficult to prove such use, but also unreasonable, as such use would be expected by the public. It would be difficult to argue that such a search is unreasonable, considering the availability of the service. Still, websites like PimEyes must be compared to the use of more sophisticated technologies to examine if the public has access to similar tools.

---

209 *See* United States v. Miller, 425 U.S. 435, 442–43 (1976); Smith v. Maryland, 442 U.S. 735, 743–44 (1979); *see also* SELECT CONSTITUTIONAL CONSIDERATIONS, *supra* note 207, at 15–16. Also, depending on the classification as either an electronic communication service or a remote computing service, these photographs or voices might also fall under the protection that is afforded by the Stored Communications Act, thus barring voluntarily sharing data. *See* 18 U.S.C. § 2703(b)(2) (2019); Kirill Levashov, Note, *The Rise of a New Type of Surveillance for Which the Law Wasn't Ready*, 15 COLUM. SCI. & TECH. L. REV. 164, 178–85 (2013) (discussing the application of the Stored Communications Act for faceprints within photographs).

210 *See Ferguson Testimony*, *supra* note 161, at 19.

211 *See* Kyllo v. United States, 533 U.S. 27, 34–35 (2001) (holding that "the [thermal imaging] technology in question is not in general public use"); Murphy, *supra* note 182, at 12–13.

212 *See* Donohue, *supra* note 46, at 511–13 (exemplifying private use of facial recognition technology that was already available in 2012).

213 *See* Daniel Laufer & Sebastian Meineck, *A Polish Company Is Abolishing Our Anonymity*, NETZPOLITIK.ORG (July 10, 2020, 10: 30 AM), https://netzpolitik.org/2020/pimeyes-face-search-company-is-abolishing-our-anonymity [https://perma.cc/WCK3-Y6LU] ("[E]very day more than 1 terabyte of photos are analysed and . . . the database contains the biometric data of more than 100 million faces.").

A final query lies within partnerships with companies like Clearview AI. While the third-party doctrine would invalidate a Fourth Amendment claim against such a practice, the difference here would be that Clearview AI scraped the internet for the photos likely in violation of the terms and services of such websites. In other words, while users likely consented to some third-party use of these photos, they did so under these terms and services. Still, it seems that, here as well, it would be the role of other laws, like contract law, to regulate such misuse of biometrics. Overall, the Fourth Amendment is highly limited in regulating racial recognition.[214]

The next candidate for constitutional protection could be equal protection rights granted under either the Due Process Clause of the Fifth Amendment[215] or, more likely, under the Equal Protection Clause of the Fourteenth Amendment.[216] The Fourteenth Amendment grants equal protection under the law, and due process might be violated in the context of racial recognition when it is biased and used in a discriminatory way or when recognition technology is incorporated into decisions without an individual's knowledge that it is being used.[217] But suing might be challenging, as one will need to prove a discriminatory *effect* and *purpose*.[218]

Discriminatory effect is allegedly easier to prove in this context. As this Article argues, the statistical or otherwise aggregated data for accuracy rates of the technology and, more specifically, against some minorities could aid in proving discriminatory effect.[219] But

---

214 *See Ferguson Testimony*, *supra* note 161, at 2 ("[T]he Fourth Amendment will not save us from the privacy threat posed by facial recognition technology.").

215 *See, e.g.*, Kenji Yoshino, *The New Equal Protection*, 124 HARV. L. REV. 747, 748 n.10 (2011).

216 U.S. CONST. amend. XIV, § 1 ("No State shall . . . deny to any person within its jurisdiction the equal protection of the laws."); *see* SELECT CONSTITUTIONAL CONSIDERATIONS, *supra* note 207, at 23–24.

217 *See* FACIAL RECOGNITION TECHNOLOGIES IN THE WILD, *supra* note 179, at 12; Floyd v. City of New York, 959 F. Supp. 2d 540, 562 (S.D.N.Y. 2013) (finding that a program of routine stops and frisks performed mainly in minority neighborhoods was racially biased under the Equal Protection Clause of the Fourteenth Amendment); Valentino-DeVries, *supra* note 72; Donohue, *supra* note 46, at 551–56.

218 *See* 42 U.S.C. § 1983 (1996); Tiwari, *supra* note 140, at 256. In *Washington v. Davis*, the Supreme Court held that a racially discriminatory impact was insufficient, on its own, to constitute racial discrimination under the Equal Protection Clause. *See* Washington v. Davis, 426 U.S. 229, 239–41 (1976); *see also* Hunter v. Underwood, 471 U.S. 222, 227–28 (1985) (inquiring whether a law passed with discriminatory purpose); SELECT CONSTITUTIONAL CONSIDERATIONS, *supra* note 207, at 24. *Washington v. Davis* was further confirmed in key decisions, perhaps most notably in *Pers. Adm'r of Mass. v. Feeney*, 442 U.S. 256 (1979) and (the much-criticized) *McCleskey v. Kemp*, 481 U.S. 279 (1987).

219 *See* SELECT CONSTITUTIONAL CONSIDERATIONS, *supra* note 207, at 25.

discriminatory purpose is a different story and is highly difficult to prove.[220] Plaintiffs will have to prove that the decision against them, or their cohort, was intentional and personal.[221] Institutional racism or any racism embedded within the technology or the dataset is insufficient for discriminatory purpose, as it does not directly target individuals. Statistical discrimination might not be sufficient either.[222] Even awareness by the enforcement agent to the consequences of using a provenly biased technology will not suffice to prove discriminatory purpose.[223]

To prove discriminatory purpose, plaintiffs will have to focus on at least one of the two human decisions in the process—whom to use this technology on and what to make of the outcome. That would be highly difficult to prove, as a racist police officer will not likely reveal that his decision was based on racism, masking it behind other rationales that invoked the use of the recognition technology.[224]

The second hurdle is that of the human mind. Many people might act in discriminatory ways without knowing so, due to cognitive shortcomings and biases.[225] While some might act on what they think is a reasonable good-faith belief, unconsciously it might not be.[226] For example, people tend to categorize and stereotype to make quick (and efficient) decisions—including racial stereotypes.[227] Moreover, even unbiased police officers might suffer from automation bias, in which they will over-rely on (statistically flawed) outcomes of such searches.[228]

---

220 The Court articulated several factors to be considered when determining whether a certain law has a discriminatory purpose. *See* Vill. of Arlington Heights v. Metro. Hous. Dev. Corp., 429 U.S. 252, 266 (1977); SELECT CONSTITUTIONAL CONSIDERATIONS, *supra* note 207, at 25.

221 *See* Whren v. United States, 517 U.S. 806, 813 (1996).

222 *See* Huq, *supra* note 35, at 1086.

223 *See Feeney*, 442 U.S. at 279; SELECT CONSTITUTIONAL CONSIDERATIONS, *supra* note 207, at 26. Even upon proving such purpose, it will only shift the burden to the State to prove that the agent would have acted similarly even without the discriminatory motivation. *See Hunter*, 471 U.S. at 228; SELECT CONSTITUTIONAL CONSIDERATIONS, *supra* note 207, at 24.

224 *See* Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 682 (2017) (discussing the practice of "masking").

225 *See* Ferguson, *supra* note 53, at 1170.

226 *See, e.g.*, Adam Benforado, *Frames of Injustice: The Bias We Overlook*, 85 IND. L.J. 1333, 1367 (2010); L. Song Richardson, *Arrest Efficiency and the Fourth Amendment*, 95 MINN. L. REV. 2035, 2039–40 (2011). *See generally* Charles R. Lawrence III, *The Id, the Ego, and Equal Protection: Reckoning with Unconscious Racism*, 39 STAN. L. REV. 317 (1987); Charles R. Lawrence III, *Unconscious Racism Revisited: Reflections on the Impact and Origins of "The Id, the Ego, and Equal Protection*," 40 CONN. L. REV. 931 (2008).

227 Anthony C. Thompson, *Stopping the Usual Suspects: Race and the Fourth Amendment*, 74 N.Y.U. L. REV. 956, 983 (1999); Selbst, *supra* note 35, at 147.

228 *See* Linda J. Skitka, Kathleen L. Mosier & Mark Burdick, *Does Automation Bias Decision-Making?*, 51 INT'L J. HUM.-COMPUT. STUD. 991 (1999); EVALUATING FACIAL RECOGNITION

Overall, whether consciously or not, it would be highly difficult to prove discriminatory purpose.[229] Adding to this conundrum, it will be challenging for individuals to seek civil damages of an alleged constitutional rights violation under the qualified immunity doctrine, especially when it relies on human error.[230] Thus, equal protection as a constitutional remedy currently offers little protection against misuse by officers or the algorithm, thus failing to protect against racial recognition.

The Constitution is thus limited in governing racial recognition.[231] Perhaps it is not even within its mandate, as police work is often largely governed by statutes that regulate specific technology-related aspects of policing, like wiretapping or access to stored wire and electronic communications,[232] or by internal rules and guidelines.[233]

2. Laws and Regulations

While several congressional initiatives were proposed in the past and some are still ongoing, federal law currently lacks direct rules or regulations for the use of recognition technology.[234] States and several municipalities recently became more active in this sense. While not

---

TECHNOLOGY, *supra* note 113, at 14. Notably, there might also be "algorithm aversion," whereas people tend to under-rely on machine output, as well as selective bias. *See id.* at 14–15.

229 Ferguson, *supra* note 53, at 1188 ("At an officer level, one cannot see into the human brain to understand why an officer acted the way they did.").

230 *See id.* at 1176.

231 To be clear, I am not arguing that constitutional litigation in the field of AI will always prove to be unhelpful or unfruitful. Litigation can, in fact, be a valuable tool in the project of defending legal, human, and constitutional rights, including facial recognition. I merely point to the current interpretation of the Court in this respect, which might change in the future. *See generally* JILL PRESSER, JESSE BEATSON & GERALD CHAN, LITIGATING ARTIFICIAL INTELLIGENCE (2021).

232 *See* Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1844 (2015).

233 *Id.* at 1845.

234 *See, e.g.*, Facial Recognition Technology Warrant Act, S. 2878, 116th Cong. (2019); Ethical Use of Facial Recognition Act, S. 3284, 116th Cong. (2020); An Act Establishing a Moratorium on Face Recognition and Other Remote Biometric Surveillance Systems, S. 1385, 119th Gen. Ct. (Mass. 2019). For other propositions, see Jennifer Lee, *We Need a Face Surveillance Moratorium, Not Weak Regulations: Concerns About SB 6280*, ACLU WASH. (Mar. 31, 2020), https://www.aclu-wa.org/story/we-need-face-surveillance-moratorium-not-weak-regulations-concerns-about-sb-6280 [https://perma.cc/87JJ-G8QP]; Ringrose, *supra* note 106, at 63. A moratorium on federal government use of facial recognition technology is still being considered. *See* Chris Mills Rodrigo, *Booker, Merkley Propose Federal Facial Recognition Moratorium*, HILL (Feb. 12, 2020, 3:48 PM), https://thehill.com/policy/technology/482815-booker-merkley-propose-facial-recognition-moratorium [https://perma.cc/YH7E-7NGD].

necessarily applicable to all recognition technology, some states regulated the use of facial recognition technology by government entities;[235] some cities banned facial recognition within specific technologies, like BWCs;[236] and others banned governmental use of face surveillance or facial recognition technology by non-governmental entities more broadly.[237] It remains to be seen if other states will follow this line, but notably, these laws are directed mostly at facial recognition, leaving other potential recognition technology aside for now. Still, directly banning the use of recognition technology by enforcement agencies becomes the most efficient way to tackle its threats, even if only temporarily, as Section III.B will argue.

Other than specifically targeting facial recognition, a few potential federal and state laws might regulate racial recognition as well. Prime candidates are antidiscrimination statutes, which exist in many fields, e.g., housing and employment laws restricting the use of factors like race, gender, disability, or age within decision-making.[238] On the federal level, the Civil Rights Act of 1964, which applies to police departments receiving federal funds,[239] prohibits discrimination based on race, color, religion, national origin, or sex.[240] Another candidate is the Safe Streets Act, which prohibits the police from acting with a racially disparate

---

235 Washington, for example, limits the use of facial recognition technology when it is used "in ongoing surveillance, conduct real-time or near real-time identification." WASH. REV. CODE § 43.386.080 (2021). This law was highly criticized by the ACLU as it does not place a moratorium on facial recognition use and because it lacks meaningful accountability and enforcement measures for violation. *See* Lee, *supra* note 234. Oregon regulated the use of facial recognition technology in the context of BWCs. OR. REV. STAT. § 133.741 (2015). New Hampshire regulated the use of facial recognition within the Department of Motor Vehicles. N.H. REV. STAT. ANN. § 263:40-b (2014); *see also* SELECT CONSTITUTIONAL CONSIDERATIONS, *supra* note 207, at 9.

236 *See* OR. REV. STAT. § 133.741(1)(b)(D) (2015); N.H. REV. STAT. ANN. § 105-D:2(XII) (2017).

237 These include, inter alia, Somerville, Cambridge, Brookline, and Springfield, Massachusetts; San Francisco, Oakland, and Berkeley, California; Portland, Maine; and New York City. *See* Matthew Guariglia, *Victory! Berkeley City Council Unanimously Votes to Ban Face Recognition*, ELEC. FRONTIER FOUND. (Oct. 16, 2019), https://www.eff.org/deeplinks/2019/10/victory-berkeley-city-council-unanimously-votes-ban-face-recognition [https://perma.cc/L8BK-MU9B]; Tom Simonite, *Portland's Face-Recognition Ban Is a New Twist on 'Smart Cities*,' WIRED (Sept. 21, 2020, 9:00 AM), https://www.wired.com/story/portlands-face-recognition-ban-twist-smart-cities [https://perma.cc/MAZ7-F4H8]; N.Y.C., N.Y., ADMIN. CODE, ch. 1, tit. 14, § 188 (2020), https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0 [https://perma.cc/T7VZ-KR8Y] (scroll down to the "Attachments" section; then click "20. Local Law 65"); FACIAL RECOGNITION TECHNOLOGIES IN THE WILD, *supra* note 179, at 13.

238 *See, e.g.*, 42 U.S.C. § 2000e–2(a) (in employment); Tene & Polonetsky, *supra* note 122, at 166.

239 *See* 42 U.S.C. § 2000d.

240 *See id.*

impact.[241] There are also some antidiscrimination laws on the state level that might regulate racially disparate impact within police work.[242] Unfortunately, antidiscrimination laws are rarely used to create any systematic change within already discriminatory and racist police practices.[243] While some argue that disparate impact laws must apply to criminal enforcement,[244] the disparate impact doctrine is not yet considered part of criminal enforcement.[245]

In addition, these laws only regulate parts of the bias problem and do not address the technological black box of the process—that is, the regulation of algorithms and trained data. Thus, another regulation pertains to databases, and even more directly, to those containing biometric data. The collection of biometric data from foreign nationals in airports, when they depart or enter the country, was legalized over time,[246] and the state is also not directly prohibited from collecting and storing biometric information.[247] Unauthorized collection, use, and disclosure of information (including biometric data) could fall under the Privacy Act of 1974,[248] or other privacy-related state-enacted laws or constitutions.[249]

The 1974 Act has many limits within the regulation of recognition technology. First, it applies only to federal entities, exempting state and local governments along with private entities.[250] Even for federal

---

241 *See* Omnibus Crime Control and Safe Streets Act of 1968, 34 U.S.C § 10228.

242 Notably, such laws exist in Illinois and California. *See* 740 ILL. COMP. STAT. 23/5 (2008); CAL. CODE REGS. tit. 2, § 11154(h)–(i) (2017); *see* Aziz Z. Huq, *The Consequences of Disparate Policing: Evaluating Stop and Frisk as a Modality of Urban Policing*, 101 MINN. L. REV. 2397, 2404–05, 2459–60 (2017).

243 *See* Tiwari, *supra* note 140, at 256 ("[T]here is almost no use of antidiscrimination law—let alone discussion of disparate-impact law—in creating systemic change.").

244 *See generally id.* (arguing that disparate impact liability should be part of the Safe Street Act's prohibition of discrimination in law enforcement agencies).

245 *See* Owen Fiss, *The Accumulation of Disadvantages*, 106 CALIF. L. REV. 1945, 1974–75 (2018); Tiwari, *supra* note 140, at 261.

246 *See* 8 U.S.C. § 1365b; Omnibus Consolidated Appropriations Act, 1997, Pub. L. No. 104-208, § 104(a), 110 Stat. 3009-555–56 (1996) (codified as amended at 8 U.S.C. § 1103 note); Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, 116 Stat. 543 (2002); *see also* Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2242 (2015) (funding the biometric program).

247 *See* Donohue, *supra* note 46, at 463–67 (summarizing why many state departments have "broad authority to collect personally identifiable information on U.S. citizens").

248 *See* Privacy Act of 1974, 5 U.S.C. § 552(a); Donohue, *supra* note 46, at 468.

249 Every state has some form of statutory provision regarding the collection, maintenance, accuracy, use, and disclosure of personal information. *See* E. Casey Lide, *Balancing the Benefits and Privacy Concerns of Municipal Broadband Applications*, 11 N.Y.U. J. LEGIS. & PUB. POL'Y 467, 487 (2008).

250 *See* 5 U.S.C. § 552a(b); Donohue, *supra* note 46, at 468, 471.

entities, the FBI has issued a final rule implementing an exemption from the Act for its NGI biometric database.[251] Second, the 1974 Act applies only to American citizens, excluding companies, non-resident aliens, and other foreigners.[252] Finally, it sets many exemptions that might include recognition data.[253]

The E-Government Act of 2002 is another potential candidate within this realm, requiring federal agencies to conduct Privacy Impact Assessments (PIAs) when running programs or information technology systems that collect, maintain, or disseminate personal information.[254] These PIAs should aid the agencies in evaluating the privacy risks to individuals, while offering potential protections to them, and it should be updated when new privacy risks arise.[255] The problem, however, is that these PIAs are not updated as frequently as they should be, and the public is still largely unaware of the use of recognition technology by enforcement agencies.[256] While important, such assessments must have regulatory teeth to succeed and can only lightly regulate racial recognition.

The relevant datasets are also not merely state owned, as the police might use privately owned datasets, whether by voluntarily asking for aid from companies or by using targeted recognition services offered by the market, e.g., Clearview AI. Generally, from the aspect of private companies' collection, while some federal laws might be somewhat applicable to biometric data,[257] such data is mainly regulated on the state level.[258] Companies will often adhere to privacy-related laws and

---

251 *See* 5 U.S.C. § 552a(j)(2); 28 C.F.R. pt. 16 (2020); *see also* Jay Stanley, *FBI Wants to Exempt Biometric Mega-Database from Privacy and Accuracy Rules*, ACLU (May 31, 2016, 5:15 PM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-wants-exempt-biometric-mega-database-privacy [https://perma.cc/VZ3S-YW5U].

252 *See* 5 U.S.C. § 552a(a)(2); Donohue, *supra* note 46, at 471–72.

253 *See* Donohue, *supra* note 46, at 472–76 (listing and discussing exemptions to the 1974 Act).

254 *See* 44 U.S.C. § 3501; SELECT CONSTITUTIONAL CONSIDERATIONS, *supra* note 207, at 8.

255 *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-579T, FACE RECOGNITION TECHNOLOGY: DOJ AND FBI HAVE TAKEN SOME ACTIONS IN RESPONSE TO GAO RECOMMENDATIONS TO ENSURE PRIVACY AND ACCURACY, BUT ADDITIONAL WORK REMAINS 8–10 (2019), https://www.gao.gov/assets/gao-19-579t.pdf [https://perma.cc/F7AH-YYC5].

256 *Id.*

257 The Government Accountability Office found that several federal laws address private companies' collection, use, and storage of biometric data, e.g., the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721–2725 (limiting the use of driver's license photographs for commercial purposes). For a full list, see PRIVACY AND ACCURACY ISSUES, *supra* note 59, at 38–39.

258 Notably, biometric information could also be somewhat regulated within data breach notification laws that, in some states, must be reported upon a breach. To exemplify, the New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act imposes data security requirements on companies collecting and using the biometric data of New York residents. *See*

regulations that might specifically relate to the use of biometric data and even facial recognition.[259] The most notable example is Illinois's Biometric Information Privacy Act (BIPA), which requires private companies, inter alia, to inform and obtain written consent from those whose biometric identifiers are collected or stored,[260] while also prohibiting profiting from such biometric data.[261] Texas,[262] Arkansas,[263] and Washington[264] also have specific biometric laws, and there are other state privacy laws that might regulate biometric data to some extent, the most comprehensive of which are those of California.[265]

Aside from datasets, it remains to be seen how courts view partnerships between enforcement agencies and private companies that offer recognition services. Vermont filed a lawsuit against Clearview AI for, inter alia, unlawfully acquiring data from consumers and businesses, thus violating Vermont's Data Broker Law.[266] There are also

---

Stop Hacks and Improve Electronic Data Security Act, N.Y. GEN. BUS. LAW §§ 899-aa, -bb (McKinney 2019).

259 *See* Jay Peters, *Facebook to Pay $550 Million to Settle Privacy Lawsuit Over Facial Recognition Tech*, VERGE (Jan. 29, 2020, 7:17 PM), https://www.theverge.com/2020/1/29/21114358/facebook-550-million-settle-lawsuit-facial-recognition-technology-illinois [https://perma.cc/2MSH-GGLY].

260 *See* Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/1 (2008); Nick Statt, *ACLU Sues Facial Recognition Firm Clearview AI, Calling It a 'Nightmare Scenario' for Privacy*, VERGE (May 28, 2020, 1:13 PM), https://www.theverge.com/2020/5/28/21273388/aclu-clearview-ai-lawsuit-facial-recognition-database-illinois-biometric-laws (last visited Sept. 14, 2021). Notably, BIPA exempts "a State or local government agency," thus it does not cover enforcement agencies. *See* 740 ILL. COMP. STAT. § 14/10.

261 *See* 740 ILL. COMP. STAT. § 14/15(b).

262 TEX. BUS. & COM. CODE ANN. § 503.001 (2017). *See generally* Carra Pope, Note, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J.L. & POL'Y 769, 791–92 (2018).

263 ARK. CODE ANN. § 4-110-103(7) (2019).

264 WASH. REV. CODE § 19.375.020 (2017). This law, however, does not apply to local police departments, exempting all "general authority Washington law enforcement agencies." *See* Ira S. Rubinstein, *Privacy Localism*, 93 WASH. L. REV. 1961, 2041 (2018); *see also* Pope, *supra* note 262, at 792–93.

265 The California Consumer Privacy Act includes biometric data as protected by the law and grants various rights to consumers, e.g., to access and delete the information and request that it will not be sold to third parties. *See* CAL. CIV. CODE §§ 1798.100–.199 (2020); Matthew Guariglia, *Victory! California Governor Signs A.B. 1215*, ELEC. FRONTIER FOUND. (Oct. 9, 2019), https://www.eff.org/deeplinks/2019/10/victory-california-governor-signs-ab-1215 [https://perma.cc/5AC4-ZM4Z]. *See generally* Rubinstein, *supra* note 264.

266 *See* Kate Cox, *Vermont Sues Clearview, Alleging "Oppressive, Unscrupulous" Practices*, ARSTECHNICA (Mar. 11, 2020, 4:09 PM), https://arstechnica.com/tech-policy/2020/03/vermont-sues-clearview-alleging-oppressive-unscrupulous-practices [https://perma.cc/L3QP-VBWH].

class action lawsuits against Clearview in various states,[267] and some states, including New Jersey, barred police officers from using its services.[268]

Current law is thus limited in properly regulating recognition technology in the context of law enforcement—that is, without resorting to a complete ban on its use like some jurisdictions have begun to do.[269] But as Section III.B argues, while such moratoriums are important, they are also temporary solutions. Properly setting the legality of recognition use requires a more holistic and realistic view of the benefits of this technology and, more specifically, directly targeting the main problems of racism embedded within the identification process. This Article discusses such solutions in Section III.B.

B. *Slowing Down the Inevitable Future of Criminal Recognition*

"Laws have to determine what's legal, but you can't ban technology. Sure, that might lead to a dystopian future or something, but you can't ban it."[270]

The deployment of AI will likely change and reshape many aspects of our lives, and criminal enforcement is unlikely to remain in the stone age of AI.[271] It would be somewhat inevitable for the police to use these new technologies in light of the history of law enforcement's adoption and use of novel technological policing tools.[272] The question is *how*. How should policymakers craft proper rules for the use of AI by law enforcement agents? As this field advances quickly, should democracies in general, and the United States specifically, place a moratorium on any use of recognition technology by enforcement agents, at least until proper barriers are in place? Can the State properly regulate

---

267 *See* Erin Shaak, *Clearview AI Hit with Class Action Lawsuit Over Controversial Data Collection Practices*, CLASSACTION.ORG (Apr. 16, 2020), https://www.classaction.org/blog/clearview-ai-hit-with-class-action-lawsuit-over-controversial-data-collection-practices [https://perma.cc/BU5P-WPPR]; Cox, *supra* note 266; Mutnick v. Clearview A.I., Inc., No. 20-CV-00512, 2020 WL 4676667 (N.D. Ill. Aug. 12, 2020).

268 *See* Kashmir Hill, *New Jersey Bars Police from Using Clearview Facial Recognition App*, N.Y. TIMES (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/technology/clearview-ai-new-jersey.html [https://perma.cc/CBR9-4MTG].

269 *See, e.g.*, sources cited *supra* note 237.

270 *See* Hill, *supra* note 90 (quoting David Scalzo, founder of Kirenaga Partner, interviewing with *The New York Times*).

271 For more on the use of AI in policing, see Selbst, *supra* note 35, at 113–15.

272 *See supra* Part I.

identification by recognition technology, and, if so, how? This Section provides a conceptual blueprint for policymakers and discusses how the market and society might be part of the equation.

1. The Direct Roles of the Law in Regulating Racial Recognition

Much like some state or municipal initiatives, the most straightforward regulatory response to regulate racial recognition would be placing a ban or at least a moratorium on its development or use. Many opine that this option is a just and feasible way to handle the potential drawbacks of recognition technology within the realm of the State.[273] Selinger and Hartzog took such an approach further, proposing a ban on facial recognition in the private sector as well.[274] And as this Article has argued, there are many good reasons to do so, as the potential harms of using recognition technology within the realm of law enforcement might currently outweigh its benefits.

But it is highly difficult, if not impossible, to stop an innovative technology once it is already deployed. Once the cat is out of the bag, there is little governments can pragmatically do to put it back in, especially with the significant economic values and other benefits that this technology provides. It should not be all or nothing in this respect.

---

273 The Facial Recognition and Biometric Technology Moratorium Act was introduced "[t]o prohibit biometric surveillance by the Federal Government without explicit statutory authorization and to withhold certain Federal public safety grants from State and local governments that engage in biometric surveillance." Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084, 116th Cong. (2020); *see* Charlotte Jee, *A New US Bill Would Ban the Police Use of Facial Recognition*, MIT TECH. REV. (June 26, 2020), https://www.technologyreview.com/2020/06/26/1004500/a-new-us-bill-would-ban-the-police-use-of-facial-recognition [https://perma.cc/LQC3-PY9A]. In New York, State Senator Brad Hoylman (D/WF-Manhattan) introduced legislation that would ban the use of facial recognition technology by law enforcement. *See* Press Release, Brad Hoylman, N.Y. State Sen., Senator Brad Hoylman Announces New Legislation to Protect Civil Liberties by Banning the Use of Facial Recognition Technology by Law Enforcement (Jan. 27, 2020), https://www.nysenate.gov/newsroom/press-releases/brad-hoylman/senator-brad-hoylman-announces-new-legislation-protect-civil [https://perma.cc/7GWM-ZA94]. Nicole Ozer, technology and civil liberties director with the ACLU of Northern California, argued that "a blanket ban on the technology is needed" and that facial recognition technology must be stopped. *See* Allyn, *supra* note 60. Many organizations and individuals around the world have signed a declaration for suspending the use of facial recognition technology. *See Declaration: A Moratorium on Facial Recognition Technology for Mass Surveillance* Endorsements, PUB. VOICE, https://thepublicvoice.org/ban-facial-recognition/endorsement [https://perma.cc/ME2U-L6VZ]; *see also* Selinger & Hartzog, *supra* note 150 ("We must ban facial recognition in both public and private sectors, before we grow so dependent on it that we accept its inevitable harms as necessary for 'progress.'").

274 *See* Selinger & Hartzog, *supra* note 150.

Even without banning the technology, there are proper ways to use this technology without becoming a dystopian surveillance state.[275] In this surveillance state, there would be little escape from data-driven technologies that mark the future of criminal enforcement, even before entering the perceived fifth era of *Autonomous Policing*.[276]

To clarify again, this Article focuses on the possible applications of recognition technology as a tool for identification—not as a surveillance tool. If the use of recognition technology constitutes, by any means, surveillance on individuals that extends beyond mere identification, then such use must be strictly banned by Congress before becoming ubiquitous.[277] Any China-like live surveillance or tracking in real time must never be permissible by any democratic state and should be deemed unconstitutional regardless of the racial aspects that this Article seeks to address, as they defeat the core purposes behind rights afforded by the Constitution.[278]

While not without drawbacks, identification is a different story, and much like the use of other biometrics, it should be gradually allowed upon passing several regulatory steps and ensuring a proper legal framework to govern its use. Thus, when discussing identification, policymakers must tackle any risks of using this technology for social control and misuse against specific cohorts or marginalized communities or any misuse in general. Unfortunately, as Section III.A showed, the constitutional protections that might aid in reducing the risks of racial recognition are currently limited. And while the aspects of racial recognition should fall under any antidiscrimination provision on the constitutional level, it is unlikely that courts will agree given current jurisprudence, and it will be upon plaintiffs to prove a constitutional violation on an individual basis. This is not sufficient by any means. As argued by Selinger and Hartzog, we simply cannot wait

---

275 *See generally* Simon Denyer, *China's Watchful Eye: Beijing Bets on Facial Recognition in a Big Drive for Total Surveillance*, WASH. POST (Jan. 7, 2018), https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance [https://perma.cc/ZY2G-LBRN]. In Russia, the police were reported to use facial recognition to enforce its COVID-19 lockdowns. *See* Patrick Reevell, *How Russia Is Using Facial Recognition to Police Its Coronavirus Lockdown*, ABCNEWS (Apr. 30, 2020, 5:06 AM), https://abcnews.go.com/International/russia-facial-recognition-police-coronavirus-lockdown/story?id=70299736 [https://perma.cc/99NA-WKCL].

276 *See* Ferguson, *supra* note 30, at 509 ("Big data policing is the future of law enforcement.").

277 *See Ferguson Testimony*, *supra* note 161, at 20 ("[T]echnology that allows arbitrary, aggregated, permanent tracking likely violates the Fourth Amendment and should be banned.").

278 *See* FERGUSON, *supra* note 117, at 140–42; Blount, *supra* note 158, at 72–73 (arguing that applying the Court's logic in *Kyllo* when using facial recognition technology in real time might lead such practice to constitute a Fourth Amendment search). *See generally* Ferguson, *supra* note 53, at 1138–44.

for the Supreme Court to update its privacy protections in this regard, as by then, the use of such technology might become ubiquitous.[279] We must not wait for new judicial interpretations of the Fourth Amendment in this context, or, in the words of Justice Alito in *Riley v. California*, "it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment."[280]

To address racial recognition, we must regulate the use of recognition technology through laws or other regulations that are adaptive to changes. Here, too, it is crucial to regulate these technologies more broadly. To date, policymakers and academics have focused almost solely on facial recognition within their proposed laws or analyses but seldom mention its applicability to other recognition technology like voice or gesture recognition. While facial recognition is a more imminent threat than other recognition technology, this reality could swiftly change,[281] and policymakers must adhere to a technologically neutral approach as to accommodate how recognition technology—like that of voice or gesture—might be shaped and used in the future.

Regulating recognition technology necessitates following three regulatory stages. The first stage is to broadly stop its current governmental use. Banning any governmental use of recognition technology is crucial, as the ramifications of continuing to use this technology without further studying its drawbacks and how to mitigate the risks that stem from its use might eventually normalize it. Congress must act without further delay to pass a moratorium on any use of such technology by any state department until further notice, while also ceasing their funding.[282] If used within any criminal proceedings,

---

279 *See* Selinger & Hartzog, *supra* note 150.

280 Riley v. California, 573 U.S. 373, 408 (2014) (Alito, J., concurring).

281 Chinese authorities are using gait recognition to identify people's body shapes and how they walk. *See* Dake Kang, *Chinese 'Gait Recognition' Tech IDs People by How They Walk*, ASSOCIATED PRESS (Nov. 6, 2018), https://apnews.com/article/bf75dd1c26c947b7826d270a16e2658a (last visited Sept. 14, 2021).

282 Notably, however, the use of this technology is relatively cheap. *See* Wingfield, *supra* note 60 ("[Amazon's Rekognition] was also cheap, costing just a few dollars a month after a setup fee of around $400."). *See generally* Devich-Cyril, *supra* note 57; SEASKATE, INC., *supra* note 16, at 89–90 (discussing funding for police technology as a potential obstacle for embracing technologies). For a proposal that relates to limitations within governmental funding of governmental use of facial recognition, see To Prohibit Federal Funding from Being Used for the Purchase or Use of Facial Recognition Technology, and for Other Purposes, H.R. 3875, 116th Cong. (2019); Facial Recognition and Biometric Technology Moratorium Act of 2020, H.R. 7356, 116th Cong. (2020).

previous or ongoing, it must not be considered reliable or admissible evidence.[283]

Upon banning the technology, Congress can proceed to the second stage—studying how to craft an exception for law enforcement for purposes of identification. This must be done on the federal level, operating under a single federal office,[284] as city or statewide legislation and regulation are merely bandages.[285] This is highly important, as a single regulatory body that operates on the federal level will be an efficient and optimal way to avoid inconsistencies, thus creating standardized police practices in this field.[286]

Within and outside the federal office, Congress should continue its efforts to study the benefits and drawbacks of using this technology in the context of identification, while preparing to legislate a proper and effective regulatory framework to govern it. Within this tradeoff, it is highly important to study if, and to what extent, the use of recognition technology is fruitful in aiding law enforcement agencies.[287] Only upon proving that the benefits of using this technology outweigh its drawbacks, assuming for now that it yields accurate results, can Congress craft exceptions to the ban.

The third stage is the creation of such a regulatory framework. This framework should address the concerns raised in this Article, i.e., how to improve the accuracy of outputs and how to reduce biased or otherwise flawed decision-making within the process. It should apply to discrimination of any kind. But before directly addressing the problems of racial recognition, there are several regulatory steps that should accompany such regulations.

---

283 *See* Ringrose, *supra* note 106, at 62.

284 *See generally* FACIAL RECOGNITION TECHNOLOGIES IN THE WILD, *supra* note 179 (arguing that the complexity of facial recognition technologies requires creation of a new federal office).

285 *Id.* at 12 ("Legislation that is domain specific, regionally placed, and time limited leaves many applications and deployment areas unaddressed.").

286 *See* Susan McCoy, Comment, *O'Big Brother Where Art Thou?: The Constitutional Use of Facial-Recognition Technology*, 20 J. MARSHALL J. COMPUT. & INFO. L. 471, 491 (2002) (proposing a single federal body to govern facial recognition technology).

287 Currently, this technology was reported by some to only rarely aid the police in identifying suspects, while not reducing crime rates. *See* Valentino-DeVries, *supra* note 72 (referring to the Florida program, indicating that "[o]nly a small percentage of the queries break open investigations of unknown suspects"); Petty, *supra* note 74 ("[T]hese invasive programs have shown little to no impact on crime."). Others, however, claim that this technology has already aided in many criminal cases, along with aiding in identifying child victims of abuse, even preventing or thwarting abuse. *See, e.g.*, Kashmir Hill & Gabriel J.X. Dance, *Clearview's Facial Recognition App Is Identifying Child Victims of Abuse*, N.Y. TIMES (Feb. 10, 2020), https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html?smid=nytcore-ios-share [https://perma.cc/XT9C-DXS7].

The first relates to biometric datasets in any sector. Generally, biometric data must be regulated on the federal level, that is, until all states provide at least a minimal level of protection to regulate such conduct by private entities. As these datasets are highly sensitive, it is crucial to deploy proper security measures.[288] Databases could be hacked, and highly sensitive biometric data could then be compromised.[289] Thus, while some states, including Illinois, went along the path of regulating biometric data within the private sector, it is crucial that the United States follow other regimes, like the European Union, in protecting sensitive data more holistically within privacy regulations or at least within the regulation of law enforcement.[290]

Within regulation of racial recognition, accuracy is a real problem that must be directly addressed. It begins with asymmetrical data gaps that must be filled.[291] No one should be able to use recognition technology of any kind, for any reason, if the training data or datasets used lack sufficient diversity or statistically misrepresent cohorts of any kind.[292] At a minimum, algorithms must show equal (and low) error

---

288 *See* PRIVACY AND ACCURACY ISSUES, *supra* note 59, at 14 (discussing the importance of data security in facial image datasets).

289 Not surprisingly, perhaps, this has already happened. A governmental facial recognition pilot program containing biometric data was hacked, while some photos were released on the dark web. *See* Matthew Gault, *DHS Admits Facial Recognition Photos Were Hacked, Released on Dark Web*, VICE (Sept. 24, 2020, 12:45 PM), https://www.vice.com/en/article/m7jzbb/dhs-admits-facial-recognition-photos-were-hacked-released-on-dark-web [https://perma.cc/94Z5-L4L3].

290 Both the GDPR and the Data Protection Law Enforcement Directive in the EU treat biometric data as a special category of data considered sensitive. They define biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data." *See* Regulation 2016/679 of Apr. 27, 2016, art. 4, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 34; Council Directive 2016/680 of Apr. 27, 2016, art. 3, On the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 98 [hereinafter LED]. Under LED, the EU allows the processing of biometric data for law enforcement purposes only when it is directly authorized by the State, when protecting vital interests of the data subject or of another natural person, or "where such processing relates to data which are manifestly made public by the data subject." *See* LED, art. 10, 2016 O.J. (L 119) 109.

291 Huq, *supra* note 35, at 1077 (suggesting algorithmic tools that might be used to compensate for asymmetrical data gaps).

292 Kate Crawford defined the omission of data about certain subsets of a population as "black holes." *See* Kate Crawford, *The Anxieties of Big Data*, NEW INQUIRY (May 30, 2014),

rates between different groups.[293] Accuracy could be promoted by various regulatory mechanisms. It could begin with standardization, e.g., that public entities like the NIST will issue standards that apply to any provider of recognition technology or standards to which datasets must adhere. While the NIST already runs a series examining facial recognition under its Face Recognition Vendor Test program, its reports are currently not mandatory and are thus insufficient.[294] In the words of Andrew Ferguson, the State can "require testing, auditing, and third-party certification requirements and forbid use if the technology does not pass the test," all within the stage of product development, and all of which should be conducted by independent researchers.[295]

Specifically regarding bias, Ferguson argues that these systems must be tested on how they are applied to "people of different races, ethnicities, genders, ages, or other demographic characteristics" and that "the training data and on-going data being fed into the system should be revealed."[296] Factually, auditing large training datasets for embedded bias might be difficult to accomplish, as recently demonstrated by some researchers.[297] But there could be other accompanying solutions to improve accuracy. Some initiatives, for instance, call for developing a "Nutrition Label" for datasets, i.e., creating a label that will grant overview of dataset "ingredients."[298] Other ongoing congressional proposals suggest requiring private

https://thenewinquiry.com/the-anxieties-of-big-data [https://perma.cc/GQ3C-8ZAX]. Zachary Lipton coined this as "bias by omission." *See* Zachary C. Lipton, *The Foundations of Algorithmic Bias*, APPROXIMATELY CORRECT (Nov. 7, 2016), http://approximatelycorrect.com/2016/11/07/the-foundations-of-algorithmic-bias [https://perma.cc/MS3S-MXF3].

293 *See* PRIVACY AND ACCURACY ISSUES, *supra* note 59, at 35–36.

294 *See Face Recognition Vendor Test (FRVT) Ongoing*, NAT'L INST. OF STANDARDS & TECH. (June 29, 2021), https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing [https://perma.cc/6HXC-PC2D]; *see also* PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS, NAT'L INST. OF STANDARDS & TECH. 1 (2019).

295 *See* Ferguson, *supra* note 53, at 1207. Ferguson also offers that the "auditing measures to continue to test the technology could be required." *See id.* at 1207.

296 *Id.* at 1208.

297 The article, "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?," was written by several researchers including Timnit Gebru, the co-founder of the "Gender Shades" project, who served as the co-lead of Google's ethical AI team and was reportedly forced out of Google, allegedly due to her involvement in the paper. *See* Karen Hao, *We Read the Paper that Forced Timnit Gebru Out of Google. Here's What It Says.*, MIT TECH. REV. (Dec. 4, 2020), https://www.technologyreview.com/2020/12/04/1013294/google-ai-ethics-research-paper-forced-out-timnit-gebru [https://perma.cc/3P8R-355E].

298 *See* DATA NUTRITION PROJECT, https://datanutrition.org [https://perma.cc/KAK6-8FYM].

entities to study and fix their algorithms if they make inaccurate, unfair, biased, or discriminatory decisions.[299]

Still, accuracy of facial recognition (and other recognitions) will likely improve over time, depending, inter alia, on various factors, like lighting, angles, and quality of the images.[300] Within the context of algorithmic decisions, inherent biases must also be governed. The problem with algorithms in this context is their black box nature. Without knowing how the algorithm works, as they are often complicated and proprietary,[301] it will be difficult to ferret out any hidden discrimination within it.[302]

This is where transparency steps in. Frank Pasquale argued that the answer to black box discrimination is transparency.[303] But transparency of algorithms, while often suggested as a remedy even in the criminal context,[304] might be a rather limited solution for various reasons: algorithms might be manipulated; transparency may compromise trade secrets;[305] and perhaps most importantly, they may be too complicated to understand or not reveal much about the decisions made.[306] To address this, Anupam Chander suggested focusing on transparency of inputs and outputs rather than on how the algorithm operates.[307]

Still, it is important to remember that the human brain is also somewhat of a black box, and while algorithms and data might not be fully transparent, there are still ways to provide transparency of the

---

299 *See* Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong. (2019).

300 There are also other ways that could make the identification much more accurate, like connecting facial recognition to other systems, e.g., signals from cellphones, to verify identification, much like what China does. Naturally, however, this is highly intrusive in the context of human rights and liberties and must not be promoted. *See* Valentino-DeVries, *supra* note 72; Mozur, *supra* note 147.

301 *See* FERGUSON, *supra* note 117, at 136–40.

302 FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 38 (2015).

303 *See id.* at 218.

304 *See, e.g.*, Dean DeChiaro, *Convicted by Software? Not So Fast, Says California Lawmaker*, ROLL CALL (July 14, 2020, 6:00 AM), https://www.rollcall.com/2020/07/14/convicted-by-software-not-so-fast-says-california-lawmaker [https://perma.cc/858N-7R75].

305 Rebecca Wexler argued that in the context of criminal law, trade secrets should not be privileged, and she offered a framework to deal with the barriers of intellectual property in this context. *See generally* Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018). Recently, a state appeals court in New Jersey granted access to the source codes of a DNA software in a criminal proceeding. *See* State v. Pickett, 246 A.3d 279 (N.J. Super. Ct. App. Div. 2021).

306 Chander, *supra* note 134, at 1040; Kroll et al., *supra* note 224, at 638.

307 *See* Chander, *supra* note 134, at 1039.

process and the outcomes.[308] It would be wise, for instance, to design these systems with oversight and accountability of the designers and the design from the start.[309] Even without disclosing or fully understanding the biases that are potentially embedded within the algorithms, Congress should strive to find ways to diversify not only datasets, but also those who develop these algorithms—thus reducing fears of biased homogeneous developers. The diversification of training data and datasets must also be promoted by Congress, while remembering that willingness to share biometric data must be based on informed consent, as it might otherwise infringe upon individuals' privacy.[310]

Then comes the question of how to regulate misuse of this technology, even when accurate. After all, these systems are suggestive, and humans must enter the loop in evaluating their outcomes,[311] which might also amplify the bias.[312] Eliminating human bias will be nearly impossible. But there are many steps that could be taken to reduce the negative effects of such bias within decision-making. While it would be wise to increase external and internal checks and balances within police work in general,[313] the State must issue and regularly update institutional guidelines, followed by adequate and enforceable sanctions for any misconduct by agencies or agents.[314]

Such institutional guidelines, or any use of this technology in general, must be placed under constant scrutiny. This could be achieved by mandating meaningful and enforceable transparency and oversight. First, anything that relates to the use of recognition technology by enforcement agencies must be fully transparent to anyone this technology was used upon and, more broadly, to the public, including comprehensible explanations of how these systems operate and which

---

308 *See* Dwork & Mulligan, *supra* note 102, at 38 ("Code presents challenges to oversight, but policies amenable to formal description can be built in and tested for. The same cannot be said of the brain.").

309 *See* Kroll et al., *supra* note 224, at 640.

310 *See* INIOLUWA DEBORAH RAJI et al., SAVING FACE: INVESTIGATING THE ETHICAL CONCERNS OF FACIAL RECOGNITION AUDITING 148–49 (2020).

311 *See* Valentino-DeVries, *supra* note 72.

312 *See* Tene & Polonetsky, *supra* note 122, at 162 ("[H]uman intervention could conceivably heighten the risk of manipulation and bias [within automated decision-making], further aggravating inaccuracies and discrimination risks.").

313 *See, e.g.*, Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314 (2006) (discussing the importance of a system of checks and balances in an executive body).

314 When they first started to use this technology, many police departments did not have any guidelines. *See* Williams, *supra* note 50.

datasets are used.[315] Here we must have greater transparency on which datasets are used, to enable proper research on the ramifications of using such datasets on human rights and liberties.[316] This also applies to the algorithms used; as suggested by Andrew Selbst, before adopting any technology, the police should be required to perform "algorithmic impact statements. . . . [that] publicly detail the predicted efficacy of and disparate impact resulting from their choice of technology and all reasonable alternatives."[317] These choices must also be strictly disclosed within any court proceedings.[318] While some cities have enacted legislation or regulations to increase transparency in this context, it is crucial that these requirements be codified on the federal level.[319]

More specifically, searches that are made by enforcement agents should never be completely invisible to others.[320] And the results of other potential suspects that enforcement agencies receive must also be transparent to those affected by the software.[321] In terms of transparency, Ferguson calls for an annual public report that could reveal information about how such technology was used and on

---

315 *See* Nick Cumming-Bruce, *U.N. Panel: Technology in Policing Can Reinforce Racial Bias*, N.Y. TIMES (Dec. 7, 2020), https://www.nytimes.com/2020/11/26/us/un-panel-technology-in-policing-can-reinforce-racial-bias.html [https://perma.cc/M6EJ-RL2T]. An example of such transparency is that of the Los Angeles Police Department, which uses the County's Digital Mugshot System as their only database for facial recognition identification. *See* Alessandro Mascellino, *LAPD Face Biometrics Policy Approved by Commission*, BIOMETRIC UPDATE (Jan. 14, 2021), https://www.biometricupdate.com/202101/lapd-face-biometrics-policy-approved-by-commission [https://perma.cc/M99V-VSU5].

316 For example, some have suggested that "[m]ug shot databases used for face recognition should exclude people who were found innocent or who had charges against them dropped or dismissed." *See* GARVIE, BEDOYA & FRANKLE, *supra* note 1, at 62–63.

317 Selbst, *supra* note 35, at 118–19.

318 Currently, states might greatly differ on what the police must disclose within a court's proceedings. Without such a requirement, they might use vague terminology like "investigative means" without disclosing that recognition technology was used in their investigation. *See* Valentino-DeVries, *supra* note 72.

319 *See, e.g.*, N.Y.C., N.Y., ADMIN. CODE, ch. 1, tit. 14, § 188 (2020), https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0 [https://perma.cc/T7VZ-KR8Y] (scroll down to the "Attachments" section; then click "20. Local Law 65"); *see also* Alan Feuer, *Council Forces N.Y.P.D. to Disclose Use of Drones and Other Spy Tech*, N.Y. TIMES (Aug. 10, 2020), https://www.nytimes.com/2020/06/18/nyregion/nypd-police-surveillance-technology-vote.html [https://perma.cc/W8LJ-XU58].

320 *See* GARVIE, BEDOYA & FRANKLE, *supra* note 1, at 19 ("Most face recognition searches are effectively invisible.").

321 Recently, a state appellate court in Florida ruled that there is no right to see other matches returned by a facial recognition program. *See* Amy Harmon, *As Cameras Track 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/YN5A-LW8H].

whom.[322] But such transparency must be made both on the public and individual levels, as mentioned.

Oversight must also be placed on the shoulders of the judiciary. Much like Congress did with wiretapping or stored communications for law enforcement purposes, Congress must place limitations on the use of this technology within the discretion of courts. Congress should require enforcement agencies to obtain a warrant for any use of this technology.[323] Ferguson proposed a "Probable Cause-Plus Standard," much like for wiretaps, "requiring an assertion of probable cause in a sworn affidavit, plus declarations that care was taken to minimize unintended collection of other face images, and that proper steps have been taken to document and memorialize the collection."[324] Others have suggested setting a condition on recognition use by enforcement agents based on a showing of "an individualized suspicion of criminal conduct" and limiting its use to investigations of serious offenses.[325]

Without delineating the exact threshold for now, placing the judiciary as another barrier against misuse of these technologies is crucial to reduce chances of mistreatment. The judiciary will be tasked with ensuring that no constitutional violations occur, most notably violations of the Fourth Amendment, i.e., that enforcement agencies do not misuse their mandates to surveil individuals. Thus, courts will be able to consider how intrusive this technology becomes on the individual level, as they could examine the number of times this search was conducted on a given individual.

The market should also be regulated. Aside from generally regulating biometric datasets,[326] companies that provide recognition services should be barred from working with enforcement agencies without court orders. Such bans on the sharing of biometric data with other parties could be mandated to some extent by legislation.[327] The government should also join hands with the market in developing best practices or standards, to which both the market and the government

---

322 *See* Ferguson, *supra* note 53, at 1209.

323 *See* Ethical Use of Facial Recognition Act, S. 3284, 116th Cong. (2020); Rodrigo, *supra* note 234.

324 *Ferguson Testimony*, *supra* note 161, at 22; *see* Ferguson, *supra* note 53, at 1195–97; *see also* FACE Protection Act of 2019, H.R. 4021, 116th Cong. § 2(a) (2019).

325 *See* GARVIE, BEDOYA & FRANKLE, *supra* note 1, at 62. They also suggested, inter alia, to "[l]imit searches of license photos." *Id.*

326 For a proposal to limit commercial entities from "collecting, processing, storing, or controlling facial recognition data," see Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019).

327 *See* Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019).

must adhere.[328] But such partnerships must be strictly confined, as these collaborations are troubling to begin with. For one, law enforcement agencies might divulge sensitive data about investigations, and this information might be misused or compromised in another way.[329] Second, there are fears that the State will pressure companies to develop best practices or standards that fit them better. Here, it might be advisable for the U.S. Federal Trade Commission to use its authority to prohibit unfair and deceptive practices that include racially biased algorithms.[330]

Notably, creating such a regulatory regime will not solve all the inherent problems with racial recognition. Misuse could still occur but would likely be substantially reduced. One of the remaining issues would be misuse that bypasses these barriers or unauthorized use, especially when this technology is still under moratorium. This problem is mostly jurisdictional in scope, as the internet could offer free identification of individuals to anyone, including police officers. This might be a valid concern. Blocking or censoring websites is not only an undesirable form of control, but it will also likely be deemed unconstitutional.[331] And these websites or services might be governed under other legal regimes—PimEyes, for example, is governed by EU and Polish laws and regulations—meaning that the United States will be left depending on foreign legal concepts. Here, strong data protection regimes might aid in assuring that companies are unable to scrape the internet for photographs—or at least discouraged from doing so—thus making it impossible for them to grant any type of biometric service without risking heavy fines. PimEyes is likely in violation of the General Data Protection Regulation (GDPR) and is expected to face fines accordingly.[332]

---

328 *See, e.g.*, INT'L BIOMETRICS & IDENTIFICATION ASS'N, IBIA PRIVACY BEST PRACTICE RECOMMENDATIONS FOR COMMERCIAL BIOMETRIC USE (2014); Press Release, Fed. Trade Comm'n, FTC Recommends Best Practices for Companies that Use Facial Recognition Technologies (Oct. 22, 2012).

329 *See* Hill, *supra* note 90.

330 And such a move seems plausible, as recently echoed in a blog post written by an FTC staff attorney. *See* Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FTC BUS. BLOG (Apr. 19, 2021, 9:43 AM), https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai [https://perma.cc/7ZSD-KSPK].

331 *See generally* Anupam Chander & Uyên P. Lê, *Free Speech*, 100 IOWA L. REV. 501 (2015).

332 *See* Laufer & Meineck, *supra* note 213 ("Instagram and YouTube, whose content appears on PimEyes, want to take legal action against the search engine as a consequence of our investigation. With data protection experts warning of a large-scale violation of the European General Data Protection Regulation (GDPR), PimEyes risks heavy fines.").

But even if websites like PimEyes are governed by the GDPR, perhaps the most comprehensive form of privacy regulation in the world, what will prevent other websites or services from reappearing when operating far beyond the reach of non-democratic countries? This could be handled to some extent by various forms of economic or political pressure, e.g., sanctions against States that do not regulate the private market's offerings of such technology—all without direct censorship. Similar sanctions could be placed directly on companies that aid totalitarian regimes, especially if these companies have financial or other interests in operating more globally.[333] The problem is that when authoritarian needs exist, there will be a market to fulfill them.[334] Thus, this is where regulation might fall short, leaving private companies to fight against any scraping of their data by competitors.[335]

What about exceptions to the use of this technology for national security or simply for aiding in non-criminal law purposes? If, for instance, America was under a terrorist attack, given the technological abilities, would we deny real-time use of recognition technology to find the terrorist(s)? Would we deny the use of these technologies to locate missing individuals—whether disoriented or abducted? This is not easy to answer. On the one hand, it seems implausible to bar the use of these tools for such purposes, and, at least for terrorism, the vague regulatory regime might be permissive of such uses already.[336] Still, with the fear of misuse, policymakers must issue direct rules that govern such use and place proper barriers against any potential misuse. And Congress must also regulate the use of recognition technology to identify those in imminent danger.[337] Unlike national security, and as an example, a court could more easily grant a "special" warrant for a missing child, especially when the consent of the caregiver is self-evident.

It is crucial, then, that Congress begin regulating racial recognition by placing a national moratorium on any use of recognition technology for any criminal-related task. Currently, despite regulatory suggestions

---

333 *See* Harwell & Dou, *supra* note 148 ("The U.S. government has also issued sanctions against Huawei, banning the export of U.S. technology to the company and lobbying other countries to exclude its systems from their telecommunications networks.").

334 *See* Mozur, *supra* note 147 ("Today, a new generation of start-ups catering to Beijing's authoritarian needs are beginning to set the tone for emerging technologies like artificial intelligence.").

335 *See supra* Section III.B.2.

336 *See generally* Niva Elkin-Koren & Eldar Haber, *Governance by Proxy: Cyber Challenges to Civil Liberties*, 82 BROOK. L. REV. 105 (2016) (discussing the vague regulatory regime that governs public-private partnerships in the context of national security).

337 *See Ferguson Testimony*, *supra* note 161, at 20 ("Separate rules can be designed for non-law enforcement purposes including public safety emergencies.").

and local moratoriums, the use of recognition technology is largely ungoverned by the law. This is where the power of society and the private sector come to the rescue. As the following Section argues, until such regulatory stages are completed, it is upon the market and social norms to slow down the governmental use of recognition technology before it is normalized.

2. Joining Forces: The Indirect Role of Markets and Society in Slowing Down Racial Recognition

The market of recognition technology is rapidly growing. While once almost a taboo for big tech companies,[338] today almost every major tech company runs some sort of facial recognition program along with heavy investment in other recognition technology.[339] And as mentioned, some markets, like those created by Clearview AI and by PimEyes, directly enable the use of recognition technology by enforcement agencies or by the general public, respectively.

With such a rise in capabilities, corporate social responsibilities—practices and policies undertaken by corporations intended to have a positive influence on society—are also on the rise in recent years.[340] The field of AI and ethics is now becoming broader to include guiding principles for ethical AI, like transparency, justice and fairness, non-maleficence, responsibility, and privacy.[341] And the market is increasingly becoming a powerful tool to regulate behavior, as the rise

---

338 As Google's then-CEO, Eric Schmidt, said in 2011, "We built that [facial recognition] technology and we withheld it. . . . As far as I know, it's the only technology Google has built and, after looking at it, we decided to stop." Bianca Bosker, *Facial Recognition: The One Technology Google Is Holding Back*, HUFFPOST (Dec. 6, 2017), https://www.huffpost.com/entry/facial-recognition-google_n_869583 [https://perma.cc/WE7A-67J5]; *see* Hill, *supra* note 90.

339 Facebook has run DeepFace since 2015 to tag people. Apple and Snapchat also use technology linked with facial recognition. *See* LaFrance, *supra* note 66.

340 *See, e.g.*, Peter Nobel, *Social Responsibility of Corporations*, 84 CORNELL L. REV. 1255 (1999) (discussing corporate social responsibilities).

341 These might also include promoting beneficence, accountability, freedom and autonomy, trust, sustainability, dignity, and solidarity. *See, e.g.*, Anna Jobin, Marcello Ienca & Effy Vayena, *Artificial Intelligence: The Global Landscape of Ethics Guidelines*, 1 NATURE MACH. INTEL. 389, 389, 394–95 (2019). *See generally* JESSICA FJELD, NELE ACHTEN, HANNAH HILLIGOSS, ADAM CHRISTOPHER NAGY & MADHULIKA SRIKUMAR, PRINCIPLED ARTIFICIAL INTELLIGENCE: MAPPING CONSENSUS IN ETHICAL AND RIGHTS-BASED APPROACHES TO PRINCIPLES FOR AI (2020).

in the involvement of tech companies within the regulation of AI is already spreading.[342]

Until Congress takes proper measures to regulate racial recognition, it might be up to the market and society to slow down its implementation—nudging the State to promptly respond to it. Aside from general involvement in the regulation of AI, many of these companies are involved behind the scenes in regulating and drafting facial recognition laws, as, one might argue, they are motivated to ensure that the law does not negatively impact their business models.[343]

But other than nudging Congress directly, the market might also self-regulate by placing barriers on the use of such technology, which in turn could influence policymakers to regulate it. This has already begun. On June 8, 2020, IBM announced that it will cease to offer "general purpose facial recognition or analysis software" and will not develop or research the technology for now, largely due to its potential misuse by enforcement agencies.[344] It was only two days later that Amazon halted the use of Rekognition by law enforcement agencies for one year, to give Congress sufficient time to properly regulate the ethical aspects of its use.[345] Microsoft did the same a day after Amazon.[346] Other companies have also declared that they will take further steps to fight against bias

---

342 To exemplify, Microsoft's "FATE" "stud[ies] the complex social implications of artificial intelligence (AI), machine learning (ML), and natural language processing (NLP)." *FATE: Fairness, Accountability, Transparency, and Ethics in AI*, MICROSOFT, https://www.microsoft.com/en-us/research/theme/fate [https://perma.cc/LQ3W-GZWX].

343 *See* Allyn, *supra* note 60 ("[Amazon has] been calling for the federal government to 'regulate' facial recognition, because they want their corporate lawyers to help write the legislation, to ensure that it's friendly to their surveillance capitalist business model.").

344 *See* Jay Peters, *IBM Will No Longer Offer, Develop, or Research Facial Recognition Technology*, VERGE (June 8, 2020, 8:49 PM), https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software (last visited Sept. 15, 2021). In the words of IBM CEO, Arvind Krishna, in a letter to Congress, "We believe now is the time to begin a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies." *Id.*

345 They are still allowing some organizations, including the International Center for Missing and Exploited Children, to use their tool. *See* Amazon Staff, *We Are Implementing a One-Year Moratorium on Police Use of Rekognition*, AMAZON (June 10, 2020), https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition [https://perma.cc/76AK-LQCB]; Nick Statt, *Amazon Bans Police from Using Its Facial Recognition Technology for the Next Year*, VERGE (June 10, 2020, 5:37 PM), https://www.theverge.com/2020/6/10/21287101/amazon-rekognition-facial-recognition-police-ban-one-year-ai-racial-bias (last visited Sept. 8, 2021).

346 *See* Jay Greene, *Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM*, WASH. POST (June 11, 2020), https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition [https://perma.cc/T84L-W7HH].

and discrimination within their platforms more generally.[347] While it is almost impossible to know the exact motivations behind these moves, they may prove to be important on the path to regulation.

Currently, the State seems to be reliant on the market, which is good news in the context of slowing down racial recognition. Sure, the State has its own capacity to produce and engage in the development of recognition technology, but companies like IBM, Google, Amazon, and Facebook are likely to be more advanced in this field than the government. Until the State develops its own capacity within this realm—and it might be heading in that direction—it is somewhat dependent on the market to provide it with recognition tools. Thus, at least in theory, the market has some power over the State. IBM even announced that it wishes to work closely with Congress "in pursuit of justice and racial equity."[348] The problem is that these players are increasingly becoming a drop in a sea of facial recognition companies, while some might not even be major players in this field.[349]

Adding to efforts to reduce racial recognition, market players can also work to diversify datasets, making sure they will be compiled from a mix of ethnicities, genders, and ages, for the use of anyone constructing AI systems, and for those who practice in recognition technology specifically.[350] Diversifying the internet in general is a

---

347 Instagram's CEO Adam Mosseri said that the company "is looking into how its 'policies, tools, and processes impact black people.'" *See* Adam Smith, *Instagram Boss Says It Will Change Algorithm to Stop Mistreatment of Black Users, Alongside Other Updates*, INDEPENDENT (June 16, 2020, 8:51 AM), https://www.independent.co.uk/life-style/gadgets-and-tech/news/instagram-black-lives-matter-racism-harassment-bias-algorithm-a9567946.html [https://perma.cc/58K4-YUK4]. TikTok apologized upon discovery that its algorithm was hiding posts related to racial equality, such as the Black Lives Matter or George Floyd hashtags. *See* Andrew Griffin, *TikTok Apologises to Black Users After Black Lives Matter and George Floyd Posts Appeared to Be Hidden on Site*, INDEPENDENT (June 2, 2020, 4:10 PM), https://www.independent.co.uk/life-style/gadgets-and-tech/news/tiktok-black-lives-matter-george-floyd-apology-protests-views-a9544956.html [https://perma.cc/ND3A-W7HQ].

348 In a letter to Congress, IBM CEO Arvind Krishna wrote, "IBM would like to work with Congress in pursuit of justice and racial equity, focused initially in three key policy areas: police reform, responsible use of technology, and broadening skills and educational opportunities." Letter from Arvind Krishna, IBM Chief Exec. Officer, to Karen Bass, U.S House of Reps., Hakeem Jeffries, U.S. House of Reps., Jerrold Nadler, U.S. House of Reps., Kamala Harris, U.S. Senate & Cory Booker, U.S. Senate (June 8, 2020).

349 *See* Fowler, *supra* note 111 (noting that IBM, Amazon, and Microsoft are not major players in the police facial recognition market).

350 IBM, for example, did so in 2018 when releasing "[a] dataset of annotations for over 1 million images to improve the understanding of bias in facial analysis" along with "[a]n annotation dataset for up to 36,000 images—equally distributed across skin tones, genders, and ages, annotated by IBM Research, to provide a more diverse dataset for people to use in the evaluation of their technologies." The second set is derived from a dataset that was released by

worthy pursuit regardless of recognition technology, and some initiatives currently focus on this important task.[351] Some market players might even generate solutions that would, at a minimum, make automated biometric recognition less possible.[352]

These exemplify steps that could slow down racial recognition, and other initiatives might emerge from the private sector, as some already have, if Congress does not step in. Still, the law should be the prime candidate to properly regulate the use of recognition technology in general and, more specifically, its proper use within the context of law enforcement. Without belittling the debate on ethics or corporate responsibilities in the age of AI, private interests must not be the guardians of criminal enforcement. It is the State that must regulate this realm.

To some extent, the suggested stages presented in this Section are also insufficient to address the bigger question that lies within the heart of this Article—that of human racism. After all, if there were no inequalities in society and humans were not biased, then the development and use of recognition technology for purposes of identification would not raise such issues. Unless society dramatically changes its norms, discrimination will keep reappearing in different forms. In the words of Chief Justice Roberts, "The way to stop discrimination on the basis of race is to stop discriminating on the basis

---

Yahoo Labs and Flickr for the purpose of research. *See* IBM Rsch. Ed. Staff, *IBM to Release World's Largest Annotation Dataset for Studying Bias in Facial Analysis*, IBM RSCH. BLOG (June 27, 2018), https://www.ibm.com/blogs/research/2018/06/ai-facial-analytics [https://perma.cc/U3HQ-578R]; Vincent, *supra* note 137. Notably, IBM was later criticized for not informing or obtaining consent for those within the dataset to be used to develop facial recognition systems. *See* Shannon Liao, *IBM Didn't Inform People When It Used Their Flickr Photos for Facial Recognition Training*, VERGE (Mar. 12, 2019, 7:14 PM), https://www.theverge.com/2019/3/12/18262646/ibm-didnt-inform-people-when-it-used-their-flickr-photos-for-facial-recognition-training (last visited Sept. 15, 2021).

351 The World White Web attempts to "put an end to the norm of whiteness on the Internet" by granting users the ability to download diverse images so as to potentially increase the likelihood that such images will appear in a Google search. *See* WORLD WHITE WEB, https://www.worldwhiteweb.net [https://perma.cc/CKH8-2PXY].

352 One potential solution was suggested by D-ID, a company that claims that its product "modifies images to prevent the identification by automated face recognition systems while preserving the identification by humans." Such modification, they claim, preserves visual similarity, without affecting data utility. *See The EU General Data Protection Regulation (GDPR) and Facial Recognition*, D-ID (May 11, 2019), https://www.deidentification.co/the-eu-general-data-protection-regulation-gdpr-and-facial-recognition [https://perma.cc/6L9E-HEY4]. Researchers also proved that some accessories (eyeglass frames in their experiment) when printed and worn, are able to "fool state-of-the-art face-recognition systems." *See* MAHMOOD SHARIF, SRUTI BHAGAVATULA, LUJO BAUER & MICHAEL K. REITER, ACCESSORIZE TO A CRIME: REAL AND STEALTHY ATTACKS ON STATE-OF-THE-ART FACE RECOGNITION 1539 (2016).

of race."[353] Until such a utopian future arrives, it is upon Congress to actively fight against any form of discrimination and, perhaps most importantly, in the realm of the most liberty-limiting instrument in the arsenal of the State—that of criminal law.

CONCLUSION

Recognition technology, along with other advancements in the field of AI, might one day aid in making the world a safer place to live. A world awash with cameras and sensors could dramatically aid in detecting and solving crimes and perhaps reducing crime rates accordingly. It might even prove to be a tool that could greatly increase the public's trust in enforcement agencies, leading to increased transparency and accountability. Unfortunately, the current reality is that the use of recognition technology by enforcement agencies, and facial recognition as a primary example, will likely be discriminatory in nature toward specific cohorts—most profoundly, minorities and those with Black skin. We must stop this use now before it becomes an embedded norm within police work. We will be bound to take such racism for granted, and mistreatment will be amplified through new innovative technologies.

There are steps to be taken, and they must be taken now. This Article suggests a conceptual blueprint for policymakers on how to tackle the problems that arise from the use of this technology, under what was termed racial recognition, which, one can hope, will be taken into consideration in the ongoing and difficult policymaking that this conundrum deserves. While this Article mainly focuses on facial recognition, researchers and policymakers must continue to closely examine the embedded biases that stem from any use of recognition technology and, perhaps most profoundly, that of voice and gesture recognition. With a rise in the use of technologies that constantly capture our images, our voices, how we walk, the way and speed at which we type, or any other identifier, Congress must be ready to quickly respond to the threats that they might bring and guard them from being used in the realm of criminal enforcement.

---

353 Parents Involved in Cmty. Schs. v. Seattle Sch. Dist. No. 1, 551 U.S. 701, 748 (2007).