ARTICLES

HOW TO SAVE FACE & THE FOURTH AMENDMENT: DEVELOPING AN ALGORITHMIC AUDITING AND ACCOUNTABILITY INDUSTRY FOR FACIAL RECOGNITION TECHNOLOGY IN LAW ENFORCEMENT

*Patrick K. Lin**

"[S]omething merciless that carried a printed list and a gun, that moved machine-like through the flat, bureaucratic job of killing. A thing without emotions, or even a face; a thing that if killed got replaced immediately by another resembling it. And so on, until everyone real and alive had been shot."[1]

* Patrick K. Lin, Author of Machine See, Machine Do: How Technology Mirrors Bias in Our Criminal Justice System; J.D., Brooklyn Law School (2022); B.A., New York University (2017). I am grateful for the invaluable guidance, feedback, and comments from Professor Frank Pasquale, Professor Cecilia A. Silver, and Juyoun Han. I also wish to thank Carly J. Goldberg for her constant love, support, and genuine enthusiasm for what I find interesting—and for always reminding me to sleep. All views expressed are my own.

[1] PHILIP K. DICK, DO ANDROIDS DREAM OF ELECTRIC SHEEP? 158 (Doubleday & Co. ed., 1968). Big Brother from George Orwell's *1984* continues to be the metaphor of choice for mass surveillance; however, as surveillance technology becomes more complex, so do the problems it poses. Lora Kelley, *When 'Big Brother' Isn't Scary Enough*, N.Y. TIMES (Nov. 4, 2019), https://nytimes.com/2019/11/04/opinion/surveillance-big-brother.html. *1984* does not capture the reality that the effects of the surveillance state are not felt equally by all

CONTENTS

INTRODUCTION

On June 8, 2020—just two weeks after the police killing of George Floyd—IBM CEO Arvind Krishna told members of Congress that the company will no longer produce facial recognition software, citing the technology's potential for abuse and misuse.[2] That same week, Amazon announced that it would

citizens but are instead felt more harshly by vulnerable and marginalized people. *Id.* A more nuanced and prescient depiction can be found in Philip K. Dick's *Do Androids Dream of Electric Sheep?* which renders "a bureaucratic machinery of terror" that, in the era of police brutality and Black Lives Matter, looks uncomfortably familiar. Noah Berlatsky, *Blade Runner's Source Material Says More About Modern Politics than the Movie Does*, VERGE (Oct. 5, 2017, 2:45 PM), https://theverge.com/2017/10/5/16428544/blade-runner-philip-k-dick-do-androids-dream-of-electric-sheep-analysis-adaptation.

[2] *See* Letter from Arvind Krishna, CEO, IBM, to U.S. Cong. (June 8, 2020), https://www.ibm.com/blogs/policy/wp-content/uploads/2020/06/Letter-from-IBM.pdf; Jay Greene, *Microsoft Won't Sell Police Its Facial-Recognition*

implement a one-year moratorium on police use of Rekognition, the company's facial recognition software.[3] Microsoft followed suit when its president stated in an interview that it would not sell facial recognition technology to police departments until there is a federal law, "grounded in human rights," that will regulate this technology.[4] "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," wrote Krishna, the first non-white CEO in IBM's 110-year history.[5]

While recent demonstrations against police brutality have shined a spotlight on the surveillance tools the tech industry sells to law enforcement,[6] state and local police have been using facial

Technology, Following Similar Moves by Amazon and IBM, WASH. POST (June 11, 2020, 2:30 PM), https://washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition [https://perma.cc/CGW7-KZPJ].

[3] *See We Are Implementing a One-Year Moratorium on Police Use of Rekognition*, AMAZON NEWS (June 10, 2020), https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition [https://perma.cc/3WKN-QBA6].

[4] Greene, *supra* note 2.

[5] *See* Krishna, *supra* note 2; *see* Will Knight, *IBM's Withdrawal Won't Mean the End of Facial Recognition*, WIRED (June 10, 2020, 7:00 AM), https://wired.com/story/ibm-withdrawal-wont-mean-end-facial-recognition [https://perma.cc/TEM8-2AGA]. While Amazon, Microsoft, and IBM appear to have kept their promise stop selling facial recognition to police, smaller companies—like Clearview AI—have filled that void. Jonathan Greig, *One Year After Amazon, Microsoft and IBM Ended Facial Recognition Sales to Police, Smaller Players Fill Void*, ZDNET (May 26, 2021), https://zdnet.com/article/one-year-after-amazon-microsoft-and-ibm-ended-facial-recognition-sales-to-police-smaller-players-fill-void [https://perma.cc/CXD2-B32P]. The large tech companies still support police in other ways, such as Amazon brokering more than 1,800 partnerships with local law enforcement agencies since 2018, allowing police to request recorded videos from Ring users without a warrant. Lauren Bridges, *Amazon's Ring is the Largest Civilian Surveillance Network the US Has Ever Seen*, THE GUARDIAN (May 18, 2021, 8:51 AM), https://theguardian.com/commentisfree/2021/may/18/amazon-ring-largest-civilian-surveillance-network-us [https://perma.cc/33EH-6ZVP].

[6] *See* Rebecca Heilweil, *Big Tech Companies Back Away from Selling Facial Recognition to Police. That's Progress*, VOX (June 11, 2020, 5:02 PM), https://vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police [https://perma.cc/VV94-UXDS]; *see also* Caroline Haskins, *Many Police Departments Have Software that Can Identify People in Crowds*, BUZZFEED NEWS (June 12, 2020, 12:52 PM), https://buzzfeednews.com/article/carolinehaskins1/police-software-briefcam [https://perma.cc/EG4J-8RS8] (highlighting privacy concerns when police departments purchase facial recognition and surveillance video analysis software that can "surveil protesters and enforce social distancing without the public knowing").

recognition technology since the early 2000s.[7] Facial recognition has given law enforcement the ability to monitor, track, and identify faces among crowds, in state driver's license databases, in surveillance videos of public streets, and virtually everywhere else.[8] According to a 2016 report from the Georgetown Law Center on Privacy and Technology, the faces of more than half of all adults in the United States are in facial recognition databases that can be searched by police departments without a warrant.[9] As many as one in four police departments in the United States can access facial recognition tools, and many use them in routine criminal investigations.[10] The Federal Bureau of Investigation (FBI) conducts four thousand facial recognition searches per month, and twenty-one states allow the FBI to access states' Department of Motor Vehicles (DMV) for driver's license photos.[11] Despite the widespread use of facial recognition in law enforcement, there are no federal laws governing the use of this technology.[12] Furthermore, the Supreme Court has stayed silent on whether the Fourth Amendment's prohibition of unreasonable searches and seizures applies to facial recognition.[13]

[7] *See* Clare Garvie & Jonathan Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, THE ATLANTIC (Apr. 7, 2016), https://theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991 [https://perma.cc/JR7Y-RDYN].

[8] Clare Garvie et al., *The Perpetual Line-up: Unregulated Police Face Recognition in America*, CTR. ON PRIV. & TECH. GEO. L., Oct. 2016, at 28.

[9] *See id.* at 8.

[10] *See id.* at 2; *see also* Reis Thebault, *California Could Become the Largest State to Ban Facial Recognition in Body Cameras*, WASH. POST (Sept. 11, 2019, 11:24 PM), https://washingtonpost.com/technology/2019/09/12/california-could-become-largest-state-ban-facial-recognition-body-cameras [https://perma.cc/4VWA-4XJZ] ("[M]ore than 50 state or local police agencies across the country have at some point used [facial recognition] technology in attempts to identify criminal suspects or verify identities.").

[11] Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019), https://washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches.

[12] *See* Thomas Germain, *Federal Agencies Use DMV Photos for Facial Recognition. Here's What You Need to Know*, CONSUMER REPORTS (July 8, 2019), https://consumerreports.org/privacy/federal-agencies-use-dmv-photos-for-facial-recognition [https://perma.cc/2MZ5-C382].

[13] *See id.*; *see also* Barry Friedman & Andrew Guthrie Ferguson, *Here's a Way Forward on Facial Recognition*, N.Y. TIMES (Oct. 31, 2019), https://nytimes.com/2019/10/31/opinion/facial-recognition-regulation.html. ("Federal agencies have no clear democratic mandate nor any explicit legislative authority to use facial recognition. And this sort of data mining usually is done without a warrant.").

The Fourth Amendment was designed to limit police power and prevent privacy intrusions by the government.[14] One could hardly be blamed for thinking that the Fourth Amendment—specifically enacted to protect against "unreasonable searches"[15]—would somewhat limit powerful and intrusive technologies such as facial recognition.[16] But since the Fourth Amendment's inception, Fourth Amendment jurisprudence has been at odds with technological changes.[17] The current Fourth Amendment doctrine has struggled to keep up with facial recognition and other surveillance technologies.[18] The Supreme Court's interpretative practices, especially its commitment to originalism, and reluctance to acknowledge the new capabilities of surveillance technology in a digital age have resulted in a too-slow expansion of what constitutes a "search" under the Fourth Amendment.[19] Even if there was a clear way forward on the Fourth Amendment "search" issue, facial recognition raises challenging questions about racial bias, the legitimacy and power of police, and ethical issues in artificial intelligence (AI) design.[20]

[14] *See* Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 25 (2020) ("The Fourth Amendment was designed 'to place obstacles in the way of a too permeating police surveillance.'").

[15] U.S. CONST. amend. IV.

[16] *See* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1129 (2021) ("One might hope that the Fourth Amendment—designed to restrain police power and enacted to limit governmental overreach—would have something to say about this powerful and overreaching technology").

[17] *See* MICHAEL WASHINGTON & NEIL RICHARDS, DIGITAL CIVIL LIBERTIES AND THE TRANSLATION PROBLEM, *in* THE OXFORD HANDBOOK OF CRIMINAL PROCESS 368 (Darryl K. Brown et al. eds., 2019).

[18] *See* Sam duPont, *Facial Recognition Is Here But We Have No Laws*, NEXTGOV (July 8, 2020), https://nextgov.com/ideas/2020/07/facial-recognition-here-we-have-no-laws/166711 [https://perma.cc/ZF5Q-RTZH].

[19] WASHINGTON & RICHARDS, *supra* note 17, at 387 ("The difficulty of changing civil liberties through interpretation is compounded by judicial commitments to originalism, which are shared to a greater or lesser extent across the political spectrum, though they are more common and likely to be stricter among judges who identify as judicial minimalists or conservatives.").

[20] *See* Tawana Petty, *Defending Black Lives Means Banning Facial Recognition*, WIRED (July 10, 2020, 8:00 AM), https://wired.com/story/defending-black-lives-means-banning-facial-recognition [https://perma.cc/7HNG-JLFE] (describing facial recognition as "perfectly designed for the automation of racism" because "[s]urveillance is the foundation of modern policing" and "has ties to a long racist legacy"); *see also* Malkia Devich-Cyril, *Defund Facial Recognition*, THE ATLANTIC (July 5, 2020), https://theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771 [https://perma.cc/8WQ6-FLNF] ("America has long used science and technology to categorize and

Facial recognition technology, with the assumptions of their developers embedded in their code, often perform poorly at recognizing people of color.[21] Facial recognition consistently misidentifies Black[22] people and ethnic minorities, young people, and women at higher rates than white people, older people, and men, respectively.[23] Data sets used to train facial recognition algorithms are overwhelmingly composed of faces from lighter-skinned, older, and male-identifying individuals.[24] And due to decades of "well-documented, racially biased police practices," criminal databases, especially gang databases and mugshot databases, include a disproportionate number of Black people, Latinx people, and immigrants, replicating historical racial biases.[25] These realities alone mean facial recognition systems' inaccuracies force people of color into more frequent and more

differentiate people into hierarchies that, even today, determine who is able and unable, deserving and undeserving, legitimate and criminal. As with the scientific racism of old, facial recognition doesn't simply identify threats; it creates them, and as such intensifies a dangerous digital moment with a long history.").

[21] *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, PROC. MACH. LEARNING RSCH., Feb. 2018, at 7–8 (2018) (finding that facial analysis algorithms misclassified darker female faces nearly 35% of the time, while correctly identifying lighter male faces about 99% of the time).

[22] Although terms for race are generally not capitalized in major publications, there has been a push to treat "Black" as a proper name for persons of the African Diaspora akin to the proper names of "nationalities, peoples, races, tribes" that are capitalized. *See* Lori L. Tharps, *The Case for Black with a Capital B*, N.Y. TIMES (Nov. 18, 2014), https://nytimes.com/2014/11/19/opinion/the-case-for-black-with-a-capital-b.html [https://perma.cc/K6LP-QAX4]. The author of this article made a conscious decision to capitalize "Black" throughout this note in order to respect this position.

[23] *See* Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology*, AT ELEC. FRONTIER FOUND., Apr. 2020, at 2, https://eff.org/files/2020/04/20/face-off-report-2020_1.pdf [https://perma.cc/W6YD-LPUK].

[24] *See* Buolamwini & Gebru, *supra* note 21, at 1–2, 7–11.

[25] *See* Lynch, *supra* note 23, at 2. The New York Police Department ("NYPD") acknowledged that as many as 95% of the people in its gang database are Black or Latinx. *See* Jeff Coltin, *Why Everyone is Suddenly Talking about the NYPD Gang Database*, CITY & STATE N.Y. (June 13, 2018), https://cityandstateny.com/policy/2018/06/why-everyone-is-suddenly-talking-about-the-nypd-gang-database/178384 [https://perma.cc/D4FA-JAAB]; Emmanuel Felton, *Gang Databases are a Life Sentence for Black and Latino Communities*, PAC. STANDARD (Mar. 15, 2018), https://psmag.com/social-justice/gang-databases-life-sentence-for-black-and-latino-communities [https://perma.cc/5HUC-8DBS] (discussing the secretive nature of gang databases as well as how easy it is for individuals to be added to a gang database, even for social media activity).

dangerous encounters with law enforcement than white people.[26] Ultimately, the lack of regulations or standards in the development of facial recognition tools, along with widespread law enforcement use of this technology, exacerbates issues of racial bias in policing.[27]

Facial recognition appears to be a genie that is not going back in the bottle. That does not mean legislation and regulation cannot effectively manage and limits its use. Still, until enforceable rules and ethical AI design standards are set, a moratorium on untested government use of facial recognition should be established.[28] Although there have been useful applications of facial recognition beyond the traditional law enforcement and surveillance contexts,[29] the immediate dangers of facial recognition's accuracy and bias problems are simply too great.[30] It is possible to fix facial recognition's shortcomings in

[26] *See* Lynch, *supra* note 23, at 2.

[27] *See* Garvie et al., *supra* note 8, at 72.

[28] Facial recognition, in its current state and application, is detrimental to society. *See* Max Read, *Why We Should Ban Facial Recognition Technology*, N.Y. MAG. (Jan. 30, 2020), https://nymag.com/intelligencer/2020/01/why-we-should-ban-facial-recognition-technology.html. The harms that result from unregulated technology "are rarely felt, let alone understood, until the technology is sufficiently powerful and entrenched." *Id.* An immediate, nationwide moratorium is necessary. However, the longer-term goal should be an outright ban on the use of facial recognition in public places and for surveillance purposes, as well as severe restrictions on the use of this technology by private companies and individuals. *See* Evan Greer, *The Case for an Outright Ban on Facial Recognition Technology*, LEAPS.ORG (Oct. 21, 2019), https://leaps.org/the-case-for-an-outright-ban-on-facial-recognition-technology/. ("Like biological or nuclear weapons, facial recognition poses such a profound threat to the future of humanity and our basic rights that any potential benefits are far outweighed by the inevitable harms.").

[29] *See* Luke Stark, *Facial Recognition is the Plutonium of AI*, ASS'N. FOR COMPUTING MACH. (Apr. 10, 2019), https://dl.acm.org/doi/10.1145/3313129 [https://perma.cc/K9C8-2RAQ] (noting that proponents of facial recognition point to benefits in "public safety, consumer convenience, and the general verification of individual identity online."). *See* Joshua New, *Balancing the Conversation About Facial Recognition*, CNTR. FOR DATA INNOVATION (July 12, 2018), https://datainnovation.org/2018/07/balancing-the-conversation-about-facial-recognition [https://perma.cc/A4YE-W8D5] (explaining that "[t]he Department of Homeland Security runs a program called Child Exploitation Image Analytics . . . to evaluate and deploy facial recognition algorithms that can identify children in child pornography.").

[30] *See* Stark, *supra* note 29. ("Yet given the ways facial recognition systems embed racializing and racist logics into its structure, the potential harm for these systems' use in public safety and law enforcement contexts should be obvious; it is the equivalent of deploying a tactical nuclear weapon to demolish an ordinary office building."). While this note focuses on Fourth Amendment issues, the right to due process and First Amendment rights to free speech and

the foreseeable future; however, it can still be used in disparate and detrimental ways as long as the underlying power imbalance between civilians and police remains unaddressed.[31] Even if legislatures allow facial recognition in some instances, the technology should be kept on a short leash.

The fact remains that the Fourth Amendment alone cannot protect civilians from the unfettered use of facial recognition.[32] The law must catch up to the rapid advancements made in surveillance technology if it hopes to effectuate regulation and prevent misuse and abuse.[33] Understanding the limitations of the Fourth Amendment in reining in law enforcement surveillance technology is crucial for developing approaches to "future-proof" the Fourth Amendment and enacting new policies to supplement it.[34] The gaps in the current Fourth Amendment framework, coupled with the lack of federal laws, is the perfect storm.[35] As law enforcement agencies continue to roll out facial recognition technology across the country, more must be done to explore and

freedom of assembly are also at risk. *See* Clare Garvie & Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, GEO. L. CTR. ON PRIVACY & TECH. (May 16, 2019), https://americaunderwatch.com.

[31] *See* Osonde A. Osoba & Douglas Yeung, *Bans on Facial Recognition Are Naïve—Hold Law Enforcement Accountable for Its Abuse*, THE HILL (June 17, 2020, 8:00 AM), https://thehill.com/opinion/technology/503070-bans-on-facial-recognition-are-naive-hold-law-enforcement-accountable-for [https://perma.cc/3ETS-5W5V] ("If people distrust police officers' human interactions, how can we ever start to trust them to deploy an imperfect but potentially valuable tool like facial recognition?").

[32] *See* Ferguson, *supra* note 16, at 1108 (arguing that current Fourth Amendment doctrine and constitutional theory "offer little privacy protection and less practical security" in the face of modern surveillance technology). *See also* Tokson, *supra* note 14, at 56 ("[T]he Supreme Court has said . . . that a person's 'facial characteristics' are not private or intimate and are constantly exposed to the public," making it unlikely that facial characteristics would be protected under the Fourth Amendment if surveilled during isolated acts that do not constitute a search).

[33] *See* duPont, *supra* note 18 (warning that, "without legal safeguards, [facial recognition] technology will undermine democratic values and fundamental rights"); *see also* Angelique Carson, *Lawmakers (Continue to) Grapple with How to Regulate Facial Recognition*, INT'L ASS'N PRIV. PROS. (Jan. 16, 2020), https://iapp.org/news/a/lawmakers-continue-to-grapple-with-how-to-regulate-facial-recognition [https://perma.cc/2YG8-945V] ("False positives on identification may 'present privacy and civil rights and civil liberties concerns, such as when matches result in additional questioning, surveillance, errors in benefit adjudication or loss of liberty.'").

[34] *See* Andrew Guthrie Ferguson, *Future-Proofing the Fourth Amendment*, HARV. L. REV. BLOG (June 25, 2018), https://blog.harvardlawreview.org/future-proofing-the-fourth-amendment [https://perma.cc/3YGA-5VJK].

[35] *See* duPont, *supra* note 18.

correct the bias that is built into facial recognition systems and how that bias reinforces racist police practices.[36]

This article argues that the current Fourth Amendment doctrine is ill-equipped to address privacy and racial bias concerns that arise from police use of facial recognition, leaving Black people and other people of color most vulnerable to the misuse and abuse of this untested and unregulated technology.[37] Ideally, facial recognition should be banned nationwide. However, in the likely event that a federal ban does not come to pass, federal legislation should be enacted to severely limit government use of facial recognition so that it can begin to close the gaps left by the traditional Fourth Amendment framework. Lawmakers should define very narrow circumstances where the technology can be used, if at all. Legislation can also address the Fourth Amendment's unanswered questions with respect to facial recognition's bias and design issues. Developing a competitive algorithmic auditing and accountability industry will allow the federal government to set directives for facial recognition while creating incentives for private actors to formulate more effective and less burdensome ways to meet those directives.

Part I of this article provides a background on facial recognition technology, examines how its design disproportionately affects Black people and people of color, and discusses how US law enforcement agencies are currently using the technology. Part II explores significant Supreme Court cases that have shaped the "reasonable expectation of privacy" standard[38] and evaluates the ineffectiveness of the existing Fourth Amendment doctrine in protecting overpoliced communities of color against facial recognition technology. Part III discusses guiding principles for restricting facial recognition in a manner that is consistent with but will expand the existing Fourth Amendment doctrine and proposes establishing a new algorithmic auditing and accountability industry.

Evaluating the current Fourth Amendment framework through the lens of facial recognition reveals the doctrine's limitations as a shield against policing and surveillance.

[36] *See* Garvie & Frankle, *supra* note 8.

[37] *See infra* Part I.B.

[38] The shift from analog surveillance to digital surveillance has forced the Supreme Court to reassess the meaning of the reasonable expectation of privacy test. *See infra* Part II.

However, introducing a regulatory framework that prioritizes transparency and scrutinizes the current state of policing in America may redeem the Fourth Amendment in the face of new digital surveillance capabilities.

I. BACKGROUND: FACIAL RECOGNITION TECHNOLOGY

While facial recognition technology is a relatively recent development, its use has quickly proliferated. One of facial recognition's first appearances on the US public stage was at Super Bowl XXXV in 2001, where law enforcement officials scanned everyone passing through turnstiles and compared their faces to criminal mugshots.[39] That year also saw the first widespread police use of facial recognition technology when the Pinellas County Sheriff's Office began operating a photo database to investigate crimes.[40] This database is currently one of the largest local databases in the US.[41] Ten years later in 2011, the US government used facial recognition to identify Osama bin Laden.[42] Edward Snowden released documents from 2011

[39] Declan McCullagh, *Call It Super Bowl Face Scan I*, WIRED (Feb. 2, 2001, 12:00 PM), https://www.wired.com/2001/02/call-it-super-bowl-face-scan-i/. In addition to being one of the earliest instances of police use of facial recognition, Super Bowl XXXV was also facial recognition's first big controversy, with critics calling its use a violation of Fourth Amendment rights. *See id.*

[40] *See* Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://nytimes.com/2020/01/12/technology/facial-recognition-police.html [https://perma.cc/84DJ-4J9F]; *see also* Kathryn Varn, *Study: Pinellas Sheriff's Facial Recognition System Has Danger of Abuse and Little Oversight*, TAMPA BAY TIMES (Oct. 18, 2016), https://tampabay.com/news/publicsafety/study-pinellas-sheriffs-facial-recognition-system-has-danger-of-abuse-and/2298543 [https://perma.cc/3CPS-5VTX] ("The database is used by all of Pinellas County's roughly 800 deputies as well as officers from 243 agencies across the state . . . . Pinellas has also partnered with 40 of those agencies to expand the number of arrest photos in the database.").

[41] *See* Thorin Klosowski, *Facial Recognition Is Everywhere. Here's What We Can Do About It*, N.Y. TIMES: WIRECUTTER (July 15, 2020), https://nytimes.com/wirecutter/blog/how-facial-recognition-works [https://perma.cc/GRN6-L4ZA]. The Pinellas County Sheriff's Office's facial recognition program is known as Face Analysis Comparison & Examination System (FACES) and "searches over 33 million faces, including 22 million Florida driver's license and ID photos and over 11 million law enforcement photos." *See* Garvie & Frankle, *supra* note 7. Pinellas County's database is searched nearly 8,000 times per month, and the Florida police do not need reasonable suspicion to conduct searches. *Id.*

[42] *See U.S. Tests bin Laden's DNA, Used Facial ID: Official*, REUTERS (May 2, 2011, 1:21 AM), https://reuters.com/article/us-binladen-dna/u-s-tests-bin-ladens-dna-used-facial-id-official-idUSTRE7411HJ20110502 [https://perma.cc/X39R-

revealing that the National Security Agency (NSA) was collecting millions of facial images per day to build a federal facial recognition database.[43] And in 2017, former President Donald Trump issued an executive order expediting the use of facial recognition at US borders and ports of entry, including airports.[44]

Over the course of two decades, facial recognition technology went from a novelty to an everyday staple.[45] The 2010s ushered in the modern era of facial recognition when improvements in computing power made it possible to train neural networks, resulting in facial recognition becoming a standard feature in government and consumer technology alike.[46] Facial recognition and the machine learning techniques that power it are heralded for their potential to transform the world, yet even the most well-intended technologies can have nefarious applications.[47]

A. The Technology & the Impact of Algorithmic Bias

Facial recognition is most commonly used to identify and match faces.[48] Before someone can be identified, a face

KWSY].

[43] James Risen & Laura Poitras, *N.S.A. Collecting Millions of Faces from Web Images*, N.Y. TIMES (May 31, 2014), https://nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html [https://perma.cc/3ECM-R84R]; *see* Klosowski, *supra* note 41.

[44] Davey Alba, *The US Government Will Be Scanning Your Face At 20 Top Airports, Documents Show*, BUZZFEED NEWS (Mar. 11, 2019, 9:27 AM), https://buzzfeednews.com/article/daveyalba/these-documents-reveal-the-governments-detailed-plan-for [https://perma.cc/L3KE-LYCK]; *see also* Francesca Street, *How Facial Recognition is Taking Over Airports*, CNN (Oct. 8, 2019), https://cnn.com/travel/article/airports-facial-recognition/index.html [https://perma.cc/B3AZ-5DF9] (explaining how facial recognition is used in airports).

[45] *See* Klosowski, *supra* note 41.

[46] *Id.* "Neural networks are a means of doing machine learning, in which a computer learns to perform some task by analyzing training examples." Larry Hardesty, *Explained: Neural Networks*, MIT NEWS (Apr. 14, 2017), https://news.mit.edu/2017/explained-neural-networks-deep-learning-0414 [https://perma.cc/4DM9-F7FF]. Neural networks are used to recognize the face by first being trained on the pictures from a face database. *See* discussion *infra* Part I.A. Overtime, the facial recognition software will become more accurate based on the facial images it was trained on. *Id.*

[47] *See* Joy Buolamwini, *When the Robot Doesn't See Dark Skin*, N.Y. TIMES (June 21, 2018), https://nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html.

[48] *See* Bennett Cyphers et al., *Face Recognition Isn't Just About Face Identification and Verification: It's Also Photo Clustering, Race Analysis, Real-time Tracking, and More*, ELEC. FRONTIER FOUND. (Oct. 7, 2021), https://eff.org/deeplinks/2021/10/face-recognition-isnt-just-face-identification-

identification algorithm must first locate that individual's face in an image.[49] Once the face is detected, it is reconfigured to match the same size, position, and orientation of every face that was used to train this algorithm, making it easier to compare faces.[50] Next, the algorithm isolates and measures structural components of the face to determine a person's identifying features, such as distance between the eyes and the length of the jawline.[51] The combination of these features produces that individual's "faceprint," which functions much like a fingerprint in that it is unique and specific to that person.[52] Facial recognition tries to match two or more faceprints to determine if they are a match.[53] Instead of generating "yes" or "no" outputs, these systems generally pick out "more likely" or "less likely" matches.[54]

Facial recognition's face matching capabilities can be used to perform a variety of tasks. First, face matching can be used to identify an unknown person by comparing their faceprint to that of a known person.[55] Law enforcement agencies frequently use this feature to identify suspects in camera footage or photos uploaded to social media.[56] Face matching can also be used to verify a known person's identity.[57] Smartphones use this functionality to enable users to unlock their phones with just their face.[58] These applications of face matching are typically used for one-to-one matches,[59] but face clustering can scan an image to determine how many unique faces are present in them, allowing for one-to-many matches.[60] All forms of face matching

and-verification [https://perma.cc/5Q4W-2RL8]; *see also* JOY BUOLAMWINFACIAL RECOGNITION TECHNOLOGIES: A PRIMER 2–3, 5 (May 29, 2020) (available at https://people.cs.umass.edu/~elm/papers/FRTprimer.pdf [https://perma.cc/9BRM-8SGV]).

[49] *See* Garvie et al., *supra* note 8, at 9.

[50] *See id.*

[51] *See* 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, 167–68 (2013).

[52] *See id.*

[53] Cyphers et al., *supra* note 48.

[54] Garvie et al., *supra* note 8, at 9.

[55] Cyphers et al., *supra* note 48.

[56] Lynch, *supra* note 23, at 5, 8–9.

[57] *See id.* at 5.

[58] *See id.*

[59] A one-to-one match is when a facial recognition system compares images of two faces and determines if they are the same person. Cyphers et al., *supra* note 48.

[60] *Id.* A one-to-many match occurs when a reference image is compared to a data set of images to determine if that reference image matches any of the

can be used to track an individual's real-time movements, raising concerns around intrusive and abusive law enforcement uses for both surveillance and investigation if legislatures and the judiciary alike do not set limits for when, why, and how this technology is used.[61]

Facial recognition relies on AI to perform the above-mentioned tasks. In other words, AI is a development that allows machines to "learn, reason, and act for themselves."[62] AI systems can make decisions when given new information, imitating intelligent human behavior.[63] Facial recognition systems use AI to automatically pick out a person's specific, distinctive features in an image, such as a photograph or surveillance video, and compare those facial features to images stored in a database to determine whether they represent the same individual.[64]

Many facial recognition systems define which features are the most reliable signals of similarity through machine learning.[65] Machine learning algorithms provide AI the ability to automatically learn and improve by identifying patterns in data.[66] During this learning process, an algorithm designed for facial recognition is fed images of identical faces.[67] As the

individual images in the data set. Cyphers et al., *supra* note 48.

[61] *Id.* ("Any face recognition system used for 'tracking', 'clustering', or 'verification' of an unknown person can easily be used for 'identification' as well. The underlying technology is often exactly the same. For example, all it takes is linking a set of 'known' faceprints to a cluster of 'unknown' faceprints to turn clustering into identification.").

[62] Karen Hao, *What is AI? We Drew You a Flowchart to Work It Out*, MIT TECH. REV. (Nov. 10, 2018), https://technologyreview.com/2018/11/10/139137/is-this-ai-we-drew-you-a-flowchart-to-work-it-out [https://perma.cc/6MWZ-JNBJ].

[63] *Id.*

[64] *See Street-Level Surveillance: Face Recognition*, ELEC. FRONTIER FOUND., (Oct. 24, 2017), https://eff.org/pages/face-recognition; *See* Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work*, HOWSTUFFWORKS (last visited Jan. 2, 2023), https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm [https://perma.cc/9EDA-JUCM]; Levashov, *supra* note 51 ("[Facial recognition] software is able to detect and isolate human faces captured by the camera and analyze them using an algorithm that extracts identifying features. The algorithm identifies and measures 'nodal points' on the face, which are defined by the peaks and valleys that make up human facial features. Using these measurements, the algorithm determines an individual's identifying characteristics, such as distance between the eyes, width of the nose, shape of cheekbones, and the length of the jawline.").

[65] *See* GARVIE ET AL., *supra* note 8, at 9.

[66] Karen Hao, *What is Machine Learning?*, MIT TECH. REV. (Nov. 17, 2018), https://technologyreview.com/2018/11/17/103781/what-is-machine-learning-we-drew-you-another-flowchart [https://perma.cc/2U8P-LDQY].

[67] *See* GARVIE ET AL., *supra* note 8, at 9.

algorithm processes more faces, it learns to spot the features that are the best indicator that a pair of facial images contain the same individual.[68] The diversity of faces used to train an algorithm ultimately determine the photos and faces a facial recognition system is most adept at identifying.[69] If the set of facial images is not representative, skewing towards a certain race or demographic, that algorithm will likely be more accurate when identifying members of that group and less accurate when identifying individuals of other groups.[70]

AI systems are "shaped by the priorities and prejudices—conscious and unconscious—of the people who design them."[71] A 2011 study conducted by the National Institute of Standards and Technology (NIST)[72] found that "East Asian algorithms" developed in countries like China, Korea, and Japan recognized East Asian facial features more accurately than Caucasian features.[73] In contrast, "Western algorithms" designed in countries like France, Germany, and the United States were substantially better at recognizing Caucasian faces.[74] These results show that the conditions in which an algorithm is developed, specifically the racial composition of its design team and training data set, can impact the accuracy of its results.[75]

In May 2019, MIT researcher and digital activist Joy Buolamwini testified before the House Committee on Oversight and Reform that many data sets companies use "to test or train facial [recognition systems] are not properly representative."[76]

[68] *See* GARVIE ET AL., *supra* note 8, at 9.

[69] *Id.*

[70] *Id.*

[71] *See* Buolamwini, *supra* note 47.

[72] "NIST is a government organization responsible for setting scientific measurement standards and testing novel technology." Dave Gershgorn, *From RealPlayer to Toshiba, Tech Companies Cash In on the Facial Recognition Gold Rush*, ONEZERO (June 2, 2020), https://onezero.medium.com/from-realplayer-to-toshiba-tech-companies-cash-in-on-the-facial-recognition-gold-rush-b40ab3e8f1e2 [https://perma.cc/JF5K-256D] ("NIST is a government organization responsible for setting scientific measurement standards and testing novel technology."); *Id.* ("As a public service, NIST also provides a rolling analysis of facial recognition algorithms, which evaluates the accuracy of a vendor's algorithms. . . . NIST has previously found evidence of bias in a majority of algorithms studied.")

[73] *See* P. Jonathan Phillips, et al., *An Other-Race Effect for Face Recognition Algorithms*, NAT'L INST. STANDARDS & TECH., MAY 13, 2010, at 1-12.

[74] *Id.*

[75] Garvie & Frankle*, supra* note 7.

[76] Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, WIRED (July 22, 2019, 7:00 AM), https://wired.com/story/best-

The most convenient place to gather a massive collection of faces is the Internet, "where content skews white, male, and western."[77] Many of the most widely used facial recognition systems are able to correctly identify photos of white men at least 99 percent of the time.[78] Meanwhile, error rates quickly increase the darker someone's skin is.[79] Facial recognition systems can only be as good as the data used to train them.[80] To adapt a computer-science maxim, "garbage in, garbage out."[81]

AI is often depicted as a panacea that can fix the world's problems, but it can instead amplify bias and exclusion, even when it is used with the best intentions.[82] Similarly, machine learning can produce powerful predictions, but its reliance on data collected from biased systems and institutions of today will simply ensure that today's problems are preserved for the future.[83] Thus, biases in the real world can seep into the AI systems that inform facial recognition development and deployment.[84]

Given facial recognition's well-documented tendency to mirror

algorithms-struggle-recognize-black-faces-equally [https://perma.cc/68QY-F38F]; *see Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties: Hearing Before the H. Comm. On Oversight & Reform*, 116th Cong. 4–5 (2019) (statement of Joy Buolamwini, Founder, Algorithmic Justice League), https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Transcript-20190522.pdf [https://perma.cc/6PB9-VZEC].

[77] *See* Simonite, *supra* note 76.

[78] Buolamwini & Gebru, *supra* note 21, at 10.

[79] *Id.*

[80] *See* Steve Lohr, *Facial Recognition Is Accurate, if You're a White Guy,* N.Y. TIMES (Feb. 9, 2018), https://nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

[81] The expression "garbage in, garbage out" refers to the fact that regardless of how accurate an algorithm's logic is, the results will always be incorrect if the input is invalid. *See* Sandra G. Mayson, *Bias In, Bias Out*, 128 YALE L.J. 2218, 2224 n. 23 (2019). Professor Sandra G. Mayson recently coined "bias in, bias out" to refer to algorithmic predictions that rely on biased, historical data. *Id.* ("[I]f the thing that we undertake to predict—say arrest—happened more frequently to [B]lack people than to white people in the past data, then a predictive analysis will project it to happen more frequently to [B]lack people than to white people in the future.").

[82] Buolamwini, *supra* note 47.

[83] Mayson, *supra* note 81, at 2224; *see also* Dan McQuillan, *People's Councils for Ethical Machine Learning*, SOC. MEDIA & SOC'Y, April–June 2018, at 1, https://journals.sagepub.com/doi/10.1177/2056305118768303 ("[M]achine learning is a form of numerical pattern finding with predictive power, prompting comparisons with science. But rather than being universal and objective, it produces knowledge that is irrevocably entangled with specific computational mechanisms and the data used for the training.").

[84] Lohr, *supra* note 80.

gender and racial biases, public institutions should be particularly mindful of how these systems are designed and applied to ensure that they are not reinforcing biases that inform racist policing practices.[85] Regulators and legislators should hold agencies and corporations accountable when flawed data sets result in foreseeable errors, particularly if these institutions fail to disclose limitations of the data set.[86]

According to a 2016 report published by the Center on Privacy and Technology at Georgetown Law, the faces of half of all adults in the United States—over 117 million people—are currently in facial recognition database networks that can be searched by police departments without a warrant.[87] Furthermore, these searches rely on facial recognition technology that has not been "tested for accuracy on different groups of people."[88] Misidentification can subject innocent people to police scrutiny or erroneous criminal charges.[89]

B. "If the only tool you have is a hammer . . . ": How Facial Recognition Became a Law Enforcement Tool

Although early uses of facial recognition at the state and local levels were "notoriously unreliable," today's law enforcement agencies have access to far more advanced surveillance camera systems.[90] Surveillance camera systems installed in public spaces are capable of capturing and identifying faces in real-time.[91] Photos taken while on patrol or extracted from surveillance footage can also be instantaneously compared to facial images in government databases, such as driver's licenses, mugshots, and jail booking records.[92] Today's police can identify a suspect

[85] Buolamwini, *supra* note 47.

[86] Frank Pasquale, *Data-Informed Duties in AI Development*, 119 COLUM. L. REV. 1917, 1927–28 (2019).

[87] Garvie et al., *supra* note 8, at 2, 36–37.

[88] Buolamwini, *supra* note 47.

[89] *See* Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/23LV-DAMA] (discussing Robert Julian-Borchak Williams who, in January 2020, was misidentified by the Detroit Police Department, wrongfully arrested, and "may be the first known account of an American being wrongfully arrested based on a flawed match from a facial recognition algorithm.").

[90] Garvie & Frankle, *supra* note 7.

[91] *Id.*

[92] John Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC NEWS (May 11, 2019, 4:19 AM), https://nbcnews.com/news/us-

caught on camera, verify a driver's identity when they do not hand over a license, or search for suspected fugitives in a state driver's license database—all at the touch of a button.[93] While forensic DNA analysis is costly and time-intensive,[94] facial recognition is inexpensive and convenient once the software has been installed.[95]

Police are able to incorporate facial recognition into their day-to-day work because of its relative ease of use.[96] As a result, officers are turning to facial recognition to solve ordinary crimes and quickly identify people perceived to be suspicious rather than reserving the technology for urgent or high-profile cases.[97] Without limits on when this technology should be used, police have more frequently used facial recognition for shoplifting than more dangerous crimes.[98] When an untested and unregulated tool is used this often, errors also become more frequent.[99] The ease of operation and incorporation into routine police matters sets up substantial potential for misuse and abuse.

For instance, the FBI quietly developed a massive facial recognition system, which launched in April 2015 with over 411 million face photos in its repository.[100] A US Government Accountability Office report published in June 2019 indicated that the FBI can draw from over 641 million photos in its facial recognition database.[101] The FBI regularly uses facial recognition

news/how-facial-recognition-became-routine-policing-tool-america-n1004251 [https://perma.cc/UZ6M-N68E]; *see also* Garvie & Frankle, *supra* note 7 (Sheriff's departments in Florida and California employ "smartphone [and] tablet facial recognition systems that can be used to run drivers and pedestrians against mugshot databases.").

[93] Garvie & Frankle, *supra* note 7.

[94] Schuppe, *supra* note 92 (analyzing DNA evidence "can take a laboratory days to produce" results).

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] Alfred Ng, *Police Are Using Facial Recognition for Minor Crimes Because They Can*, CNET (Oct. 24, 2020), https://cnet.com/tech/services-and-software/police-are-using-facial-recognition-for-minor-crimes-because-they-can [https://perma.cc/9APH-3N5C].

[99] *See id.*

[100] U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-267, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY 7 (2016).

[101] 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 5–6 (2019) [hereinafter GAO-19-579T].

systems to identify people during their investigations.[102] Moreover, as of June 2019, 21 states permit federal agencies, such as the FBI, to conduct routine searches of driver's license and government identification photo databases.[103] And in February 2020, the Department of Homeland Security (DHS) reported that 43.7 million people in the United States had been scanned by facial recognition technology, primarily to check the identity of people boarding flights and cruises and crossing borders.[104]

Market research firm Grand View Research published a report in May 2021, predicting that the market for facial recognition technology will grow at an annual rate of 15.4 percent between 2021 and 2028, driven by "[r]ising adoption of the technology by the law enforcement sector."[105] In spite of its rapid adoption over the past two decades, facial recognition systems deployed by the police are not subjected to any public or independent testing requirements to check for bias or even evaluate accuracy.[106] This lack of oversight has the potential to result in everyday civilians being at the mercy of unregulated and unreliable systems.[107] Worse yet, when facial recognition vendors do agree to be tested by organizations like NIST, many systems are found to have

[102] *See* Mariko Hirose, Comment, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1593, 1597 (2017); Neema Singh Guliani, *The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database*, ACLU (June 7, 2009), https://aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through [https://perma.cc/B3UQ-KQHJ].

[103] Germain, *supra* note 12; *see* GAO-19-579T, *supra* note 101, at 5 (showing the following states provide the driver's licenses of its residents to the FBI for use in its facial recognition database: Alabama, Arizona, Arkansas, Colorado, Delaware, District of Columbia, Idaho, Illinois, Indiana, Iowa, Kentucky, Maryland, Michigan, Nebraska, New Mexico, North Carolina, North Dakota, Pennsylvania, South Carolina, Tennessee, Texas, and Utah).

[104] *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II: Before the Comm. On Homeland Sec.*, 116th Cong. (2020) (statement of John P. Wagner, Deputy Assistant Executive Commissioner, U.S. Customs and Border Protection).

[105] *Facial Recognition Market Size, Share & Trends Analysis Report by Technology (2D, 3D, Facial Analytics), by Application (Access Control, Security & Surveillance), by End-Use, by Region, and Segment Forecasts, 2021–2028, Report Overview*, GRAND VIEW RSCH. (May 2021), https://grandviewresearch.com/industry-analysis/facial-recognition-market [https://perma.cc/AY3Z-Q26S].

[106] Garvie & Frankle, *supra* note 7.

[107] *See id.*

"troubling differences in accuracy across race, gender, and other demographics."[108]

Virtually all facial recognition systems have built-in biases.[109] Amazon's face-ID system, Rekognition, once identified Oprah Winfrey as male, while Microsoft's facial recognition system made the same error with Michelle Obama.[110] Rekognition also incorrectly matched twenty-eight members of Congress with people who have been arrested.[111] Looking at instances in which an algorithm wrongly identified two different people as the same person, a 2019 NIST study found that for facial recognition systems developed in the United States, error rates were highest in West and East African and East Asian people, and lowest in Eastern European individuals.[112] Repeating this exercise across a US mugshot database, NIST researchers found that algorithms had the highest error rates for Native Americans, along with high error rates for Asian and Black women.[113] Unfortunately, this research demonstrates how often facial recognition systems get it wrong, and as a consequence, how this technology can entrench and intensify systemic bias in policing.[114]

Bias in facial recognition is particularly disturbing given that policing practices, such as stop and frisk and the "war on drugs," have historically disadvantaged poor communities of color,

[108] *See* Garvie & Frankle, *supra* note 7.

[109] *See* Natasha Singer & Cade Metz, *Many Facial-Recognition Systems Are Biased, Says U.S. Study*, N.Y. TIMES (Dec. 19, 2019), https://nytimes.com/2019/12/19/technology/facial-recognition-bias.html [https://perma.cc/GQ5P-39Y5]; Irina Ivanova, *Why Face-Recognition Technology Has a Bias Problem*, CBS NEWS (June 12, 2020, 7:57 AM), https://www.cbsnews.com/news/facial-recognition-systems-racism-protests-police-bias [https://perma.cc/3NEY-EBT9] ("'If you look at the top three companies [in the field], none of them perform with 100% accuracy. So we're experimenting in real time with real humans,' said Rashida Richardson, director of policy research at the AI Now Institute.").

[110] Joy Buolamwini, *Artificial Intelligence Has a Problem with Gender and Racial Bias. Here's How to Solve It*, TIME (Feb. 7, 2019), https://time.com/5520558/artificial-intelligence-racial-gender-bias [https://perma.cc/U6U2-TLVK].

[111] Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, ACLU (July 26, 2018), https://aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [https://perma.cc/9W7F-7C5H].

[112] PATRICK GROTHER ET AL., NAT'L INST. STANDARDS & TECH., NISTIR 8280, FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 7 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf [https://perma.cc/99G6-G9PW].

[113] *Id.* at 47.

[114] duPont, *supra* note 18.

especially Black communities.[115] In the United States, Black people are more than twice as likely to be arrested than any other race and, "by some estimates, up to [two-and-a-half] times more likely to be targeted by police surveillance."[116] Ultimately, these futuristic tools are simply replicating biases of the past: facial recognition systems are more prone to misidentify Black people *and* Black people are more likely to be dragged into the very databases that train those systems.[117] As a result of the overrepresentation of Black people in surveillance photos and mugshot databases, algorithms consistently perform worse on Black people than on white people.[118]

But it is not enough to simply improve the accuracy of facial recognition software. In fact, even the most accurate facial recognition systems misidentify Black people five to ten times more often than they do white people.[119] Since early 2017, NIST has published results of demographic tests of facial recognition algorithms.[120] NIST's tests have repeatedly found that facial recognition software struggles to recognize people with darker skin.[121]

The end goal, however, cannot simply be to improve false-positive match rates because "unfair use of facial recognition technology cannot be fixed with a software patch."[122] Accurate facial recognition can still be used in disturbing and nefarious ways.[123] For instance, following Freddie Gray's death in Baltimore, the Baltimore police department used facial recognition to identify and arrest people who attended the 2015 protests against police misconduct.[124] Additionally, Immigration

[115] Garvie & Frankle, *supra* note 7.

[116] *Id.*

[117] *Id.*

[118] *See id.*

[119] Simonite, *supra* note 76.

[120] *See* GROTHER ET AL., *supra* note 112, at 18.

[121] Simonite, *supra* note 76. At sensitivity settings where some of the top-performing algorithms "falsely matched different white women's faces at a rate of one in 10,000, [they] falsely matched Black women's faces about once in 1,000—10 times more frequently." *Id.* In fact, white males is the demographic that experiences the lowest false match rate, while Black females face the highest false match rate. *Id.*

[122] Buolamwini, *supra* note 47.

[123] *Id.*

[124] Lynch, *supra* note 23, at 8–9; *see also* Benjamin Powers, *Eyes Over Baltimore: How Police Use Military Technology to Secretly Track You*, ROLLING STONE (Jan. 6, 2017), https://rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885

and Customs Enforcement (ICE) is interested in driver's license databases because several states issue driver's licenses to residents regardless of their immigration status.[125] Maryland, for example, grants "special driver's licenses" to undocumented immigrants.[126] Maryland also grants ICE access to its driver's license photo database, allowing the federal agency to scan millions of photos without first obtaining a warrant or approval from the court or state government.[127]

Facial recognition has and will continue to have a disparate impact on minorities, and especially Black communities, who are already subject to inequitable policing practices.[128] At its core, police use of facial recognition raises questions about the legitimacy of policing practices and how policing in the United States must change.[129]

[https://perma.cc/L88P-32RC] (bringing attention to the "large-scale aerial surveillance, advanced cell phone tracking and facial recognition technology" available to the Baltimore Police Department).

[125] Germain, *supra* note 12; McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, N.Y. TIMES MAG. (Oct. 3, 2019), https://nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html [https://perma.cc/E7Z8-2WSE] (highlighting another data-driven ICE program known as the Extreme Vetting Initiative, which was scrapped in 2018 and saw the government agency partnering with tech companies to analyze immigrants' social media activity to predict whether they would become a terrorist; potential partners including Thomson Reuters, LexisNexis, IBM, Booz Allen Hamilton, Deloitte, and PricewaterhouseCoopers); *see also* Catie Edmondson, *ICE Used Facial Recognition to Mine State Driver's License Databases*, N.Y. TIMES (July 7, 2019), https://nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html [https://perma.cc/XME9-VXNG] ("These states have never told undocumented people that when they apply for a driver's license they are also turning over their face to ICE. That is a huge bait and switch.").

[126] Drew Harwell & Erin Cox, *ICE Has Run Facial-Recognition Searches on Millions of Maryland Drivers*, WASH. POST (Feb. 26, 2020), https://washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers [https://perma.cc/Z3JZ-3LJK].

[127] *Id.*

[128] Phoebe Varunok, *Sounds About White: Constitutional Issues Surrounding the Advent of Facial Recognition Technology Used in Modern Data Policing*, AM. U. J. GENDER, SOC. POL'Y & LAW (2020), http://jgspl.org/sounds-about-white-constitutional-issues-surrounding-the-advent-of-facial-recognition-technology-used-in-modern-data-policing [https://perma.cc/7K9H-83FN].

[129] Alex Najibi, *Racial Discrimination in Face Recognition Technology*, SCI. NEWS (Oct. 24, 2020), http://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology [https://perma.cc/9744-MQFR]; Osoba & Yeung, *supra* note 31.

II. THE FOURTH AMENDMENT: A DOCTRINE IN NEED OF AN UPDATE

The Fourth Amendment to the US Constitution prohibits unreasonable searches and seizures by the government.[130] Yet the history of Fourth Amendment jurisprudence is characterized by a reluctance to develop bright-line rules for police and surveillance technologies.[131] Without clear guidance from courts and legislatures, police departments have developed systems that often fall short of the protections offered against other surveillance technologies.[132] For instance, facial recognition can be applied to photographs that were taken voluntarily, like photos posted on social media,[133] or with someone's acquiescence, such as someone's driver's license photo automatically being included in a DMV database.[134] Furthermore, one's face is not hidden when navigating a public space. Thus, collecting the appearance of the face does not typically constitute a seizure.[135] Since acquiring a facial image "does not give exposure to concealed things," collecting an image of a face is not considered a search.[136] However, despite facial images' apparent lack of fit into the traditional search and seizure, the question remains about whether exposed facial images can be constitutionally searched once they are collected.[137]

As discussed in Part I, facial recognition converts features of a

[130] U.S. CONST. amend. IV.

[131] *See infra* Part II.A.

[132] Garvie et al., *supra* note 8, at 32.

[133] Kashmir Hill, *Meet Clearview AI, The Secretive Company that Might End Privacy as We Know It*, CHI. TRIB. (Jan. 18, 2020), https://chicagotribune.com/nation-world/ct-nw-nyt-clearview-facial-recognition-20200119-dkdqz7ypaveb3id42tpz7ymase-story.html [https://perma.cc/6QUE-ZAAH]. Clearview AI developed "a database of more than three billion images . . . scraped from Facebook, YouTube, Venmo and millions of other websites." *Id.* Following the January 6th attack on the US Capitol, facial recognition app Clearview AI experienced "a 26 percent increase of searches over [the company's] usual weekday search volume." Kashmir Hill, *The Facial-Recognition App Clearview Sees a Spike In Use After Capitol Attack.*, N.Y. TIMES (Jan. 9, 2021), https://nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html [https://perma.cc/4BBB-K9ZF]. Local police departments around the country have been using facial recognition software to help the FBI identify insurrectionists in photos and videos posted on social media. *Id.*

[134] Jim Harper, *Administering the Fourth Amendment in the Digital Age*, NAT'L CONST. CTR. (May 8, 2017), https://constitutioncenter.org/digital-privacy/The-Fourth-Amendment-in-the-Digital-Age [https://perma.cc/U9T9-4ZJ5].

[135] *Id.*

[136] *Id.*

[137] *See id.*

facial image into a facial recognition signature based on biometric information, such as the distance between the eyes and color of the skin.[138] There may be no ongoing investigation when this signature is collected, making it a mere administrative process.[139] It is unclear whether facial recognition constitutes a search for Fourth Amendment purposes.[140] Yet converting an image of a face into a faceprint serves only one purpose: to search for something later.[141]

A. *The Fourth Amendment Framework During the Analog Age*

The story of the Fourth Amendment and the digital age starts with Justice Brandeis's dissent in *Olmstead v. United States*, a Prohibition-era case.[142] The Supreme Court found that, for purposes of the Fourth Amendment, the federal agents' wiretapping of suspected bootleggers did not constitute a search, and thus was constitutional.[143] Chief Justice Taft, writing for the Court, held that the government's warrantless wiretapping did not constitute a Fourth Amendment search because the wiretap did not require government agents to trespass upon Olmstead's house, papers, or effects.[144] In Chief Justice Taft's view, the Fourth Amendment only protected "what was deemed an unreasonable search and seizure when it was adopted."[145]

The *Olmstead* decision is noteworthy not just for the immediate outcome, but for Justice Brandeis's passionate dissenting opinion.[146] Justice Brandeis argued that the Founders "conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[147] Justice Brandeis foresaw the capabilities of today's surveillance technology, warning that "[w]ays may

[138] *See* discussion *supra* Part I.A.

[139] Harper, *supra* note 134.

[140] *See id.*

[141] *Id.*

[142] Olmstead v. United States, 277 U.S. 438, 471 (1928) (Brandeis, J., dissenting).

[143] *See id.*

[144] *See id.*

[145] *Id.* at 465 (quoting Carroll v. United States, 267 U.S. 132, 149 (1925)).

[146] *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) ("As Justice Brandeis explained in his famous dissent, the Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections.").

[147] *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting).

someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."[148] The reality Justice Brandeis feared is already upon us: Fourth Amendment jurisprudence has been outpaced by advances in technologies like facial recognition.[149]

Nearly forty years later, *Katz v. United States* reversed *Olmstead*.[150] Acting on a suspicion that Charles Katz was sharing gambling information over the phone to individuals in other states, federal agents attached a recording device to the outside of a public phone booth Katz was using.[151] In finding the government's actions to be unconstitutional, Justice Stewart, writing for the Court, declared that "the Fourth Amendment protects people, not places."[152] Before *Katz* was decided in 1967, the Court by and large applied a property-based interpretation of the Fourth Amendment, mostly relying on the existence of trespass to determine whether a Fourth Amendment search occurred.[153]

In addition to the reversal of *Olmstead*, *Katz* is also well known for Justice Harlan's concurrence, which established a two-part test to determine whether a person has a reasonable expectation of privacy, assessing whether: (1) the person exhibited an actual, subjective expectation of privacy and (2) that expectation is one that society recognizes as reasonable.[154] If the surveillance technology at issue violates a reasonable expectation of privacy, then the government action is a "search," and without a warrant or exception to the warrant requirement, the search is deemed unconstitutional.[155]

The following "privacy-protective" cases indicate that the Court recognizes that today's AI-enabled police surveillance presents

[148] *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting); Harper, *supra* note 134, at 2–3.

[149] Harper, *supra* note 134, at 2, 23.

[150] Katz v. United States, 389 U.S. 347, 353 (1967).

[151] *Id.* at 348.

[152] *Id.* at 351.

[153] Garvie et al., *supra* note 8, at 33.

[154] *Id.* at 33; *Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

[155] *See* Garvie et al., *supra* note 8, at 33; *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

privacy and civil liberty threats that are distinct from the traditional police surveillance described in the *Olmstead* and *Katz* cases.[156] Today's digital, data-driven surveillance technology can operate on a scale unlike anything from the past.[157] The wiretapping and electronic eavesdropping that has taken place over the past 150 years was extremely individualized.[158] Today, with the help of big data and AI, our institutions can keep an eye on communities, cities, the whole country.[159] The reasoning employed in recent cases may provide a glimpse into how the Court might eventually rule when presented with a police facial recognition case.

B. Developing a More Tech-Savvy Fourth Amendment Framework for the Digital Age

At the start of the twenty-first century, in *Kyllo v. United States* (2001), the Court found law enforcement use of "sense-enhancing" tools not yet in "general public use"—here, thermal imaging—to be a Fourth Amendment search.[160] The Court's emphasis on the public prevalence of the technology was an attempt to "take account of more sophisticated systems that are already in use or in development.[161] Later, the Court's decision in *Carpenter* expands on the approach introduced in *Kyllo*, stating that the Fourth Amendment must keep pace with advances in technology.[162]

The Court in *United States v. Jones* (2012) found that the government's warrantless installation of a Global Positioning System (GPS) device on a person's vehicle and its use of that device to monitor the vehicle's movements constituted a Fourth Amendment search because the government "physically occupied

[156] Ferguson, *supra* note 16, at 1129.

[157] April White, *A Brief History of Surveillance in America*, SMITHSONIAN MAG. (Apr. 2018), https://smithsonianmag.com/history/brief-history-surveillance-america-180968399 [https://perma.cc/EV2U-3Q39].

[158] *Id.*

[159] *See id.*; *see generally* PATRICK K. LIN, MACHINE SEE, MACHINE DO (2021) (discussing automated and high-tech tools that surveil civilians, including Amazon's signature home security product, the Ring video doorbell, automated license plate readers, and surveillance drones).

[160] Kyllo v. United States, 533 U.S. 27, 40 (2001).

[161] *Id.* at 36.

[162] *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo*, 533 U.S. at 34). The Court's position on "the limited availability of the technology" in *Kyllo* may also be applicable to facial recognition. *Legal Questions Around Facial Recognition*, 99 CONG. DIG. 3, 5 (2020) [hereinafter *Legal Questions Around Facial Recognition*].

private property for the purpose of obtaining information."[163] In finding that the physical installation of a GPS onto a car for the purpose of obtaining information constituted a search, the *Jones* Court revived the trespass doctrine, further muddling the already complicated Fourth Amendment framework.[164] However, the Court was also "concerned about the device's specific use in tracking the vehicle's movements over a prolonged period of time," as well as the private information exposed during the course of such long-term tracking, including daily routines, associations, and the freedom to move without government monitoring.[165]

In *Riley v. California* (2014), the Court unanimously agreed that the Fourth Amendment protects the contents of a cell phone from warrantless search, even when obtained from a validly arrested suspect.[166] The Court held that sensitive data in modern smartphones reveal too many of the "privacies of life" not to require a probable cause warrant before acquiring that information.[167] Specifically, the decision discussed "the quantitative and qualitative realities of digital evidence" as sufficiently distinct from those of physical evidence to necessitate a different Fourth Amendment approach.[168] From a quantitative perspective, smartphones now have practically unlimited storage capacity, allowing them to collect and store a virtually infinite amount of personal information.[169] The nature and scope of digital information also exposes far more qualitative information than individuals ordinarily share with others.[170]

[163] *See* United States v. Jones, 565 U.S. 400, 404–05 (2012).

[164] *See Jones*, 565 U.S. at 400.

[165] Levashov, *supra* note 51, at 187; Ferguson, *supra* note 16, at 1130; *Jones*, 565 U.S. at 414–16 (Sotomayor, J., concurring); *see Jones*, 565 U.S. at 428–31 (Alito, J., concurring).

[166] *See* Riley v. California, 573 U.S. 373, 403 (2014).

[167] *Id.* (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

[168] Ferguson, *supra* note 16, at 1131; *see Riley*, 573 U.S. at 393 ("The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

[169] Ferguson, *supra* note 16, at 1131; *Riley*, 573 U.S. at 393–94 ("One of the most notable distinguishing features of modern cell phones is their immense storage capacity . . . . Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so.").

[170] *See* Ferguson, *supra* note 16, at 1131–32; *see Riley*, 573 U.S. at 393–94.

In short, "digital is different," and simple comparisons between digital and analog surveillance capabilities will not adequately address Fourth Amendment questions in a digital age.[171] The digital age also introduces novel constitutional questions that did not exist for traditional searches and seizures. Yet, as technology and corresponding legal issues become more prevalent and complex, judges seem to remain uncomfortable with resolving these questions. For instance, Chief Justice Roberts, who penned the *Riley* opinion, sidestepped the larger question of the third-party doctrine: "the notion that any data kept by a third party such as Verizon, AT&T, Google or Microsoft is fair game for a warrantless search."[172]

After gradually acknowledging the Fourth Amendment's deficiencies in a digital age, the Court in 2018 came to a crucial crossroads in *Carpenter v. United States*.[173] Here, the Supreme Court was forced to choose how to "fit the Fourth Amendment into [today's] world of digital surveillance."[174] The issue before the Court was whether police were required to obtain a probable cause warrant before collecting cell-site location information (CSLI) from private cell phone companies regarding the whereabouts of a suspect.[175] This historical cell phone data could reveal a person's physical location or movements at specific points in time.[176] The Court recognized that the data at issue presented did not adhere to existing Fourth Amendment precedents, but instead "lies at the intersection of two lines of cases."[177] The first set of cases deal with an individual's expectation of privacy with respect to their physical location and movements while the other set of cases address the expectation of privacy in information that was willingly given to third parties.[178]

Justice Roberts held that the government's acquisition of CSLI

[171] Andy Greenberg, *Why the Supreme Court May Finally Protect Your Privacy in the Cloud*, WIRED (July 26, 2014), https://wired.com/2014/06/why-the-supreme-court-may-finally-protect-your-privacy-in-the-cloud [https://perma.cc/B5VY-9VC7]; *Riley*, 573 U.S. at 403 ("The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.").

[172] *See* Greenberg, *supra* note 171.

[173] *See* Ferguson, *supra* note 34.

[174] *See id.*

[175] Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

[176] *See Carpenter*, 138 S. Ct. at 2212.

[177] *Id.* at 2209.

[178] *Id.*

without a probable cause warrant violates a person's Fourth Amendment rights.[179] The Court considered the sensitivity of CSLI as well as the far-reaching and unavoidable nature of its collection, and concluded that the Fourth Amendment protects this information even if it is gathered by a third party.[180] A government's acquisition of location data held by third parties constitutes a "search" for Fourth Amendment purposes because it "reveals private details of our lives and violates our reasonable expectation of privacy."[181]

Prior to the *Carpenter* decision, government agencies were able to acquire historical CSLI "with only a court order by explaining to a judge that the information was necessary to an investigation and that the information was in possession of a third party."[182] However, the Supreme Court in *Carpenter* imposed a higher standard on the government, requiring that a search warrant be obtained on the basis of "sworn facts that probable cause exists to search for the requested items."[183] Because of this ruling, law enforcement agencies can only gain access to personal cell phone data from phone companies if they obtain a search warrant, "where no exigent circumstances exist and for date ranges more than six days."[184]

Carpenter signaled the advent of a "digitally-aware" Fourth Amendment and a Court that is "cognizant of the limitations of applying analog precedent to a digital reality."[185] Justice Roberts outlined that as new technologies present news ways for the

[179] Ferguson, *supra* note 34; *Carpenter*, 138 S. Ct. at 2223. Furthermore, the Supreme Court concluded that "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere." *Carpenter*, 138 S. Ct. at 2217. In fact, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* (alteration in original) (quoting *Katz*, 389 U.S. at 351-–52).

[180] Ferguson, *supra* note 34; *Carpenter*, 138 S. Ct. at 2223 ("In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.").

[181] Ferguson, *supra* note 34.

[182] *Legal Questions Around Facial Recognition, supra* note 162, at 4.

[183] *Id.* at 4–5; *Carpenter*, 138 S. Ct. at 2221.

[184] *Legal Questions Around Facial Recognition, supra* note 162, at 5; *Carpenter*, 138 S. Ct. at 2224. Ultimately, an individual has an expectation of privacy in their personal information acquired in large quantities over an extended period of time, even when possessed by third parties. *Carpenter*, 138 S. Ct. at 2223.

[185] Ferguson, *supra* note 16, at 1132.

government to intrude on private spaces, courts must also identify new ways to protect individual privacy from government intrusion.[186] To that end, the *Carpenter* Court makes a meaningful departure from *Riley* by declining to apply the traditional third-party doctrine.[187] Until *Carpenter*, the third-party doctrine held that "any information shared with third parties (phone records, bank records) lost an expectation of privacy and thus protection of the Fourth Amendment."[188] With respect to cell-site records held by private parties, the majority reasoned, "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[189]

Carpenter is one of the most significant Fourth Amendment cases in recent history and will likely influence police practices and produce new litigation in this space.[190] However, because the *Carpenter* decision was so narrow, many questions remain with respect to how the Court will address government access to technology that can trace a person's location or movement.[191]

Carpenter is also noteworthy because four Justices penned four separate dissenting opinions, each of which advocated for a more analog-interpretation of the Fourth Amendment, each of which could have been the controlling opinion.[192] The task of future-proofing the Fourth Amendment "is made difficult by the age of its text, the structure of the constitutional system, and the interpretative practices of U.S. judges, particularly the commitment to originalism."[193]

C. Fitting Facial Recognition into the Fourth Amendment

Given the outcome in *Carpenter*, facial recognition technology

[186] *Legal Questions Around Facial Recognition, supra* note 162, at 5; *Carpenter*, 138 S. Ct. at 2223.

[187] Ferguson, *supra* note 34.

[188] *Id.*

[189] *Carpenter*, 138 S. Ct. at 2217. This outcome creates an opportunity for courts to interpret the Fourth Amendment to require a warrant to obtain information if a person "has a legitimate privacy interest in records held by a third party." Ferguson, *supra* note 34 (quoting *Carpenter*, 138 S. Ct. at 2222).

[190] *See generally* Ferguson, *supra* note 34.

[191] *Legal Questions Around Facial Recognition*, *supra* note 162, at 5.

[192] Ferguson, *supra* note 34, at 1130–31; *Carpenter*, 138 S. Ct. at 2223–35 (Kennedy, J., dissenting); *Carpenter*, 138 S. Ct. at 2235–46 (Thomas, J., dissenting); *Carpenter*, 138 S. Ct. at 2246–61 (Alito, J., dissenting); *Carpenter*, 138 S. Ct. at 2261–72 (Gorsuch, J., dissenting).

[193] WASHINGTON & RICHARDS, *supra* note 17, at 387.

used "on a limited, short-term basis with strictly public systems" does not trigger the Fourth Amendment since a person's face is exposed to the public.[194] Courts have generally found visual surveillance to be beyond the scope of the Fourth Amendment.[195] Similarly, video surveillance does not constitute a Fourth Amendment search because it captures what the naked eye observes.[196] Under this framework, facial recognition is essentially a form of visual surveillance.[197] Under the *Katz* privacy test, a person does not have an automatic expectation of privacy in their face because it is exposed to the public.[198]

In later cases, the Supreme Court "rejected simplistic comparisons of modern technology to older policing practices."[199] For instance, in *Riley*, Chief Justice Roberts criticized the government's argument that searching a person's smartphone incident to arrest was "materially indistinguishable" from a search of an arrestee's pockets.[200] Justice Roberts responded: "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon."[201] To date, no cases in the Supreme Court have weighed in on whether any law enforcement facial recognition would be a search for Fourth Amendment purposes.[202] Without clear legislative direction or legal precedent, it is difficult to ascertain whether the Court would compare facial recognition to ordinary observation—or space travel.[203]

[194] *Legal Questions Around Facial Recognition*, *supra* note 162, at 5.

[195] Susan McCoy, *O' Big Brother Where Art Thou?: The Constitutional Use of Facial-Recognition Technology*, 20 J. MARSHALL J. COMPUT. & INFO. L. 471, 485 (2002). In accordance with the English legal tradition, courts have concluded that visual observation is not deemed a search for Fourth Amendment purposes because "the eyes cannot be guilty of trespass." *Id.* at 481. Because facial recognition is rooted in visual surveillance, courts are not likely to consider its use to be a Fourth Amendment search. *Id.* at 485.

[196] *Id.* at 485–86.

[197] *See id.* (stating that "the implantation of facial recognition technology conforms to the rule in *Kyllo*").

[198] *Legal Questions Around Facial Recognition*, *supra* note 162, at 5.

[199] Garvie et al., *supra* note 8, at 33.

[200] *Id.*; Riley v. California, 573 U.S. 373, 393 (2014).

[201] Garvie et al., *supra* note 8, at 33; *Riley*, 573 U.S. at 393.

[202] Garvie et al., *supra* note 8, at 16.

[203] *Id.* at 33.

III. SOLUTION: DEVELOPING AN AUDITING AND ACCOUNTABILITY MARKET

Lawmakers on both sides of the aisle have banded together in an effort to limit law enforcement agencies' ability to use facial recognition to surveil civilians.[204] For instance, the Facial Recognition Technology Warrant Act, introduced in November 2019, would severely restrict federal law enforcement use of facial recognition technology by requiring a court order before tracking someone for longer than three days.[205] Introduced in June 2020, the Facial Recognition and Biometric Technology Moratorium Act sought to make federal funding for state and local law enforcement contingent on banning the use of facial recognition and other biometric surveillance technology by federal law enforcement agencies.[206] As of the publication of this article, no other actions have been taken on these bills.[207] In the absence of federal laws, cities and states have led the charge in

[204] *See* Shirin Ghaffary, *How Facial Recognition Became the Most Feared Technology in the US*, VOX (Aug. 9, 2019, 4:00 PM), https://vox.com/recode/2019/8/9/20799022/facial-recognition-law [https://perma.cc/9NQV-TXQ6] [hereinafter Ghaffary I] (highlighting a new partisan bill that would dramatically limit the use of facial recognition across the US, using San Francisco, Oakland, and Somerville, Massachusetts as models since those cities passed laws banning government use of the technology); *see also* Shirin Ghaffary, *How to Avoid a Dystopian Future of Facial Recognition in Law Enforcement*, VOX (Dec. 10, 2019, 8:00 AM), https://vox.com/recode/2019/12/10/20996085/ai-facial-recognition-police-law-enforcement-regulation [https://perma.cc/MYY9-P3WH] (calling upon government and citizens to rein in the proliferation of facial recognition in both law enforcement and the private sector).

[205] Ghaffary I, *supra* note 204; Facial Recognition Technology Warrant Act of 2019, S. 2878, 116th Cong. (2019). The bill was co-sponsored by Senators Chris Coons, D-Del., and Mike Lee, R-Utah. Jon Schuppe, *New Federal Bill Would Restrict Police Use of Facial Recognition*, NBC NEWS (Nov. 14, 2019, 4:18 PM), https://nbcnews.com/news/us-news/new-federal-bill-would-restrict-police-use-facial-recognition-n1082406 [https://perma.cc/VUK4-N4DK].

[206] Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084, 116th Cong. § 4(a) (2020). Senators Edward Markey, D-Mass., and Jeff Merkley, D-Ore, introduced the bill, which has been supported by Representatives Ayanna Pressley, D-Mass., and Pramila Jayapal, D-Wash. Olivia Solon, *Facial Recognition Bill Would Ban Use by Federal Law Enforcement*, NBC NEWS (June 25, 2020, 1:08 PM), https://nbcnews.com/tech/security/2-democratic-senators-propose-ban-use-facial-recognition-federal-law-n1232128 [https://perma.cc/CH56-ZGPL].

[207] *See* S. 4084; S. 2878. The author of this article believes a temporary moratorium is critical to reducing or even avoiding misuse or abuse of law enforcement facial recognition. However, a federal bill should also include clear rules for when it is appropriate to deploy this technology, *see* discussion *infra* Part III.A, as well as how it is developed. *See* discussion *infra* Part III.B.

regulating facial recognition.[208] Several city councils have already outright banned law enforcement and government use of facial recognition technology, often by a unanimous vote.[209]

But the reality is facial recognition technology is already here—and it is everywhere.[210] People use it to unlock their phones;[211] airports and airlines use it to scan passengers' faces in lieu of their boarding passes;[212] even Taylor Swift uses facial recognition to screen people attending her concerts.[213] As a result of its prevalence, proponents of the technology, including law enforcement and big tech, downplay the power of facial recognition.[214] Instead, the focus is placed on its potential to solve crimes or identifying missing people.[215] Opponents, on the other

[208] *See* duPont, *supra* note 18; Susan Crawford, *Facial Recognition Laws Are (Literally) All Over the Map*, WIRED (Dec. 16, 2019, 8:00 AM), https://wired.com/story/facial-recognition-laws-are-literally-all-over-the-map [https://perma.cc/W4PV-P6R9].

[209] As of October 2021, the following cities passed measures to ban the use of facial recognition technology: Alameda, CA; Berkeley, CA; Boston, MA; Brookline, MA; Cambridge, MA; Jackson, MS; King County, WA; Madison, WI; Minneapolis, MN; New Orleans, LA; Northampton, MA; Oakland, CA; Pittsburgh, PA; Portland, ME; Portland, OR; San Francisco, CA; Somerville, MA; and Springfield, MA. *See Ban Facial Recognition—Map*, FIGHT FOR THE FUTURE (last visited Mar. 20, 2023), https://banfacialrecognition.com/map [https://perma.cc/5ZMZ-7UF3]. In October 2020, Vermont became the first state to ban the use of facial recognition by law enforcement. *Id.* In July 2021, Virginia's de facto ban went into effect, banning the use of facial recognition by police departments without legislative approval. Bill Atkinson, *Virginia Bill to Put De Fact Ban on Facial Recognition Tech*, GOV'T TECH. (Apr. 8, 2021), https://govtech.com/policy/virginia-bill-to-put-de-facto-ban-on-facial-recognition-tech.html [https://perma.cc/9JB8-PR5N].

[210] Rebecca Heilweil, *How Can We Ban Facial Recognition When It's Already Everywhere?*, VOX (July 6, 2020), https://vox.com/recode/2020/7/3/21307873/facial-recognition-ban-law-enforcement-apple-google-facebook [https://perma.cc/W4UB-36VR].

[211] *Id.*

[212] Alba, *supra* note 44; *see also* Jay Stanley, *The Government's Nightmare Vision for Face Recognition at Airports and Beyond*, ACLU (Feb. 6, 2020), https://aclu.org/news/privacy-technology/the-governments-nightmare-vision-for-face-recognition-at-airports-and-beyond [https://perma.cc/DNE4-2EAV].

[213] Gabrielle Canon, *How Taylor Swift Showed Us the Scary Future of Facial Recognition*, THE GUARDIAN (Feb. 15, 2019, 6:00 PM), https://theguardian.com/technology/2019/feb/15/how-taylor-swift-showed-us-the-scary-future-of-facial-recognition [https://perma.cc/628W-MJL5]; *see also* Steve Knopper, *Why Taylor Swift Is Using Facial Recognition at Concerts*, ROLLING STONE (Dec. 13, 2018, 11:24 AM), https://rollingstone.com/music/music-news/taylor-swift-facial-recognition-concerts-768741 [https://perma.cc/XWJ2-P3RG].

[214] Ghaffary I, *supra* note 204.

[215] Ryan Lucas, *How A Tip—And Facial Recognition Technology—Helped The FBI Catch A Killer*, NPR (Aug. 21, 2019, 5:01AM ET), https://npr.org/2019/08/21/752484720/how-a-tip-and-facial-recognition-technology-helped-the-fbi-catch-

hand, cite concerns that the unchecked use of facial recognition will exacerbate law enforcement's history of racial bias and discriminatory practices, as well as lead to the creation of a dystopian, surveillance state.[216] For example, the Chinese government regularly uses facial recognition on its citizens, particularly to surveil and oppress the Uyghurs, an ethnic group of predominantly Turkic-speaking Muslims native to the autonomous region of Xinjiang.[217]

At present, there are no federal laws or regulations specifically directed at the development and deployment of facial recognition by government and private actors.[218] At the state and local level, law enforcement use of facial recognition is widespread,[219] while regulation is primarily targeting the collection and storage of biometric information by private entities.[220] At the very least, a

a-killer [https://perma.cc/4GYM-8PPR]; Tom Simonite, *How Facial Recognition Is Fighting Child Sex Trafficking*, WIRED (June 19, 2019, 7:00 AM), https://wired.com/story/how-facial-recognition-fighting-child-sex-trafficking [https://perma.cc/7SYR-4QPT]. Law enforcement officers have been able to work with non-profit organization Thorn to scan pictures of missing children to help investigators find underage sex-trafficking victims. *Id.* Thorn's tool is called Spotlight and uses Amazon Recognition. *Id.*; *see also* Kashmir Hill & Gabriel J.X. Dance, *Clearview's Facial Recognition App is Identifying Child Victims of Abuse*, N.Y. TIMES (Feb. 10, 2020), https://nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html [https://perma.cc/AZX2-8BMD]; *see e.g.*, Daniel Castro, *Banning Facial Recognition Will Not Advance Efforts at Police Reform*, INFO. TECH. & INNOVATION FOUND. (June 16, 2020), https://itif.org/publications/2020/06/16/banning-facial-recognition-will-not-advance-efforts-police-reform [https://perma.cc/CPK5-JXEA] (criticizing facial recognition critics of relying on a "'slippery slope' argument about the potential threat of expanding police surveillance, rather than pointing to specific instances of harm. Banning the technology now would do more harm than good.").

[216] Evan Greer, *Opinion: Don't Regulate Facial Recognition. Ban It.*, BUZZFEED NEWS (July 18, 2019, 2:50 PM ET), https://buzzfeednews.com/article/evangreer/dont-regulate-facial-recognition-ban-it [https://perma.cc/D3CY-6DG3].

[217] 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://nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html [https://perma.cc/YGA9-LVJR]; Anna Hayes, *Explainer: who are the Uyghurs and why is the Chinese government detaining them?*, THE CONVERSATION (Feb. 14, 2019), https://theconversation.com/explainer-who-are-the-uyghurs-and-why-is-the-chinese-government-detaining-them-111843 [https://perma.cc/62LS-XCEZ].

[218] KELSEY Y. SANTAMARIA, CONG. RSCH. SERV., R46541, FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT: SELECT CONSTITUTIONAL CONSIDERATIONS 3 (2019).

[219] GAO-19-579T, *supra* note 101, at 3–6.

[220] SANTAMARIA, *supra* note 218, at 3.

moratorium should be put in place until a federal legislative framework makes clear what government applications of facial recognition should be banned altogether and what applications should be strictly regulated.[221] Moreover, while the bills introduced in the Senate attempt to limit the use of facial recognition, to give teeth to a federal law and provide meaningful protection for individuals' legitimate privacy interests, steps must also be taken to incentivize the development of ethical facial recognition systems and develop mechanisms to hold corporations accountable for faulty or biased systems.

A. Taming the Wild West: Establishing Standards and Limitations at the Federal Level

In the absence of regulation, the surveillance possibilities of facial recognition are virtually endless, with China's "social credit scores"[222] or the London police force's use of real-time crowd surveillance[223] offering a glimpse into one grim reality. Cities

[221] The author of this article supports a nationwide facial recognition moratorium because he does not believe mere reform or procedural justice is enough. Facial recognition, and, by extension, policing, must be fundamentally redesigned in order to remotely begin to rectify the long history of racially biased police practices in the US. Until regulations are in place to enforce error rate thresholds and limit its use for purely investigative purposes, a moratorium should be in place to prevent further misuse and abuse of facial recognition in law enforcement. *See* Alex S. Vitale, *The Answer to Police Violence Is Not 'Reform'. It's Defunding. Here's Why*, GUARDIAN (May 31, 2020, 5:13 AM), https://theguardian.com/commentisfree/2020/may/31/the-answer-to-police-violence-is-not-reform-its-defunding-heres-why [https://perma.cc/ZWB4-2R85] ("'[P]rocedural justice' has nothing to say about the mission or functioning of policing. It assumes that the police are neutrally enforcing a set of laws that are automatically beneficial to everyone. . . . What 'procedural justice' leaves out of the conversation are questions of substantive justice."); *see generally* ALEX S. VITALE, THE END OF POLICING (Verso ed. 2017) (asserting the solution to problems of modern policing is not simply enacting or investing in "procedural reform" to police institutions, such as police training programs or police diversity, but to dramatically shrink the functions of policing itself).

[222] Charlie Campbell, *How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens*, TIME (Jan. 16, 2019), https://time.com/collection/davos-2019/5502592/china-social-credit-score [https://perma.cc/6JTQ-NSAU]. First announced in 2014, China's controversial social credit system uses a combination of big data and facial recognition technology to monitor citizens and score them based on their deeds. *Id.* Millions of people in China have social scores low enough to be labelled as untrustworthy on an official blacklist. *Id.* The social score can determine what rights are available to people. *Id.* Blacklisted individuals, for instance, may be prevented from buying plane or train tickets and barred from working as civil servants or in certain industries. *Id.*

[223] Kelvin Chan, *London Police to Use Facial Recognition Cameras, Stoking*

across the US have attempted to strike a balance between facial recognition's potential to enhance public services and the government's ability to harm the public.[224] If a federal ban or moratorium is not achieved, a comprehensive federal facial recognition law should carefully consider *how* this technology is used; *when* it is being used; and, most importantly, *why* it is being used.[225]

Because police departments are not currently required to comply with any standards to ensure a minimum level of accuracy, law enforcement often neglect accuracy when making decisions to purchase facial recognition software.[226] While corporations may be pressured by competition to improve their facial recognition software, government and law enforcement are not subject to these same pressures.[227] Government use of facial recognition, particularly in the criminal justice context, is also higher stakes since mistakes have consequences on individuals' life, liberty, and justice.[228] Thus, accuracy and confidence thresholds as well as fairness standards should be set for facial recognition outputs.[229] NIST already established criteria for

Privacy Fears, PBS (Jan. 24, 2020), https://pbs.org/newshour/world/london-police-to-use-facial-recognition-cameras-stoking-privacy-fears [https://perma.cc/XUG7-W2F3]. In 2020, London police began employing real-time facial recognition surveillance cameras to identify suspects on crowded streets. *Id.* The cameras are deployed for around five to six hours per day. *Id.* "Real-time crowd surveillance by British police is among the most aggressive uses of facial recognition in wealthy democracies and raises questions about how the technology will enter people's daily lives." *Id.*

[224] Nila Bala & Caleb Watney, *What Are the Proper Limits on Police Use of Facial Recognition?*, BROOKINGS INST. (June 20, 2019), https://brookings.edu/blog/techtank/2019/06/20/what-are-the-proper-limits-on-police-use-of-facial-recognition [https://perma.cc/9BV2-CKJH].

[225] *Id.*

[226] Garvie et al., *supra* note 8, at 47. In fact, law enforcement agencies have even been known to feed celebrity pictures and forensic sketches into facial recognition software in an attempt get matches. Bala & Watney, *supra* note 224; Sarah Emerson, *Police Are Feeding Celebrity Photos into Facial Recognition Software to Solve Crimes*, VICE (May 16, 2019, 4:25 PM), https://vice.com/en/article/xwngn3/police-are-feeding-celebrity-photos-into-facial-recognition-software-to-solve-crimes [https://perma.cc/CBZ9-84TG] (reporting that the NYPD fed its facial recognition system an image of actor Woody Harrelson when pixelated surveillance footage failed to produce a match and other police departments relied on poorly-drawn probe images to conduct facial recognition searches).

[227] Bala & Watney, *supra* note 224.

[228] *Id.*

[229] Mark MacCarthy, *Mandating Fairness and Accuracy Assessments for Law Enforcement Facial Recognition Systems*, BROOKINGS INST. (May 26, 2021), https://brookings.edu/blog/techtank/2021/05/26/mandating-fairness-and-

assessing the accuracy and fairness of facial recognition systems as part of its Facial Recognition Vendor Tests; however, the results of these assessments do not lead to fines or legal ramifications and the assessments are completely voluntary.[230] A federal law should set accuracy and fairness minimums for facial recognition systems used for governmental purposes while also requiring facial recognition vendors to be tested and evaluated before it can be marketed and sold. Private companies selling their facial recognition products to the government at any level should be required to disclose their program to the public.

The Food and Drug Administration (FDA) tests and sets standards for drugs to determine whether products should be approved for consumer use.[231] Financial institutions are subjected to audit and regulatory reporting requirements set by agencies like the Federal Reserve Board and the Securities and Exchange Commission (SEC).[232] The National Highway Traffic Safety Administration (NHTSA) conducts crash tests on new vehicles and rates their performance.[233] Every industry is subject to regulations that shape and restrain their activities with the public interest in mind. What prevents developers of facial recognition—a technology so pervasive and with such an immense potential to do harm—from being scrutinized in a similar fashion?

Next, a federal law governing police use of facial recognition technology must forbid real-time surveillance and limit its use to after-the-fact investigations.[234] This prohibition "would prevent police body cameras from becoming unrestricted surveillance

accuracy-assessments-for-law-enforcement-facial-recognition-systems [https://perma.cc/JZY8-JNA4].

[230] MacCarthy, *supra* note 229; *see* GROTHER ET AL., *supra* note 112.

[231] *What We Do*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/about-fda/what-we-do [https://perma.cc/DTT4-7RPH]; *Is It Really 'FDA Approved?'*, U.S. FOOD & DRUG ADMIN., https://fda.gov/consumers/consumer-updates/it-really-fda-approved [https://perma.cc/9429-2SJG].

[232] *See* FED. RSRV. BD., THE FEDERAL RESERVE SYSTEM PURPOSES & FUNCTIONS 116 (10th ed. 2016) (ebook), https://federalreserve.gov/aboutthefed/files/pf_complete.pdf https://federalreserve.gov/aboutthefed/files/pf_5.pdf [https://perma.cc/U3J4-73EK]; *What We Do*, U.S. SEC. & EXCH. COMM'N, https://www.sec.gov/about/what-we-do [https://perma.cc/Y8HZ-HT2C].

[233] *Ratings*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., https://nhtsa.gov/ratings (last visited Mar. 20, 2023) [https://perma.cc/ZU33-PX4T].

[234] Bala & Watney, *supra* note 224; Matthew Feeney, *Should Police Facial Recognition Be Banned?*, CATO INST. (May 13, 2019, 2:08 PM), https://cato.org/blog/should-police-facial-recognition-be-banned [https://perma.cc/G3Y3-89DK].

machines."[235] By limiting the use of facial recognition to investigations after the fact, third parties also have the opportunity to review and even scrutinize the decision to use the technology.[236] A federal facial recognition law should mandate a case-by-case judicial review of proposals to use facial recognition, not unlike the approval process for search warrants.[237] In fact, such an approach would mirror *Carpenter*'s holding for CSLI: law enforcement agencies can only use facial recognition for investigative or crime-solving purposes after obtaining a search warrant supported by probable cause.[238] Ongoing surveillance of a specific person must be prohibited unless there is a court order or bona fide emergency.[239] Furthermore, legislatures must ensure that law enforcement authorities never rely on facial recognition as the only piece of evidence for a warrant, arrest, or conviction.[240] Strict enforcement of this rule should help to protect people from misidentification.[241]

In addition to limiting facial recognition's use to after-the-fact investigations, federal legislation should only allow the technology to be used to solve the most serious crimes.[242]

[235] Bala & Watney, *supra* note 224.

[236] *Id.*

[237] *Id.*; *See* Micah Schwartzbach, *Search Warrants: What They Are and When They're Necessary*, NOLO, https://nolo.com/legal-encyclopedia/search-warrant-basics-29742.html [https://perma.cc/7L93-LF55] (explaining that police officers obtain a search warrant by presenting affidavits to convince a magistrate that they have probable cause).

[238] *See* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

[239] *See id.* (quoting Riley v. California, 573 U.S. 373, 403 (2014)) (noting that after all, the Founding Fathers "crafted the Fourth Amendment as a response to the reviled general warrants and writs of assistance of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." (internal quotation marks omitted)). Prohibiting the use of ongoing surveillance is an approach similar to that proposed in the Facial Recognition Technology Warrant Act; however, the Act only requires a court order when tracking a person for over three days. *See* Facial Recognition Technology Warrant Act of 2019, S. 2878, 116th Cong. (2019). Considering how much private information can be revealed within a span of three days, a federal law that limits the use of facial recognition should require a court order for any length of surveillance.

[240] Amitai Etzioni, *Facial Recognition Meets the Fourth Amendment Test*, NAT'L INT. (Sept. 22, 2019), https://nationalinterest.org/feature/facial-recognition-meets-fourth-amendment-test-82311 [https://perma.cc/J6JN-TYQF].

[241] *Id.*

[242] Jeffrey Bellin, *Crime-Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in a Changing World*, 97 IOWA L. REV. 1, 1 (2011) (introducing crime severity as a key feature of a revamped search and seizure jurisprudence because the traditional "reasonableness" standard creates risks of invasive law enforcement searches even for minor crimes).

Although the current Fourth Amendment doctrine emphasizes "reasonableness" in assessing disputed searches and seizures, it overlooks a critical factor of reasonableness: the crime being investigated.[243] Accounting for crime severity when determining when facial recognition can be used could modernize the Fourth Amendment doctrine.[244] Thus, as a part of the aforementioned review process, judges should ensure that facial recognition is only being employed for offenses that rise to a level of seriousness that would warrant this potential privacy intrusion, such as violent assaults, murders, or terrorist attacks.

Facial recognition technology has improved rapidly over the past decade, but the accuracy of facial recognition technology remains far from perfect.[245] But the final solution cannot stop at merely improving the accuracy of the technology.[246] Despite the fact that there are hundreds of vendors marketing and selling facial recognition software across the country, and the widespread bias issues plaguing that technology, there is no single regulatory agency administering the rollout of facial recognition software, nor is there a public list of companies working with or selling to law enforcement.[247] Consequently, the public is largely ignorant about the state of the facial recognition and surveillance vendor market.[248]

Local police departments often use facial recognition software developed by and purchased from private companies.[249] Therefore, a federal facial recognition law should institute and enforce an independent auditing or testing requirement—such as those employed in the financial services or automotive industries[250]—for any facial recognition systems that are employed in law enforcement or government contexts. A federal law must establish processes to help independent stakeholders, including regulators and the community, detect flaws in facial recognition systems and hold institutions accountable.[251] Facial

[243] Bellin, *supra* note 242.

[244] *Id.*

[245] 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, 95 (2017).

[246] *See supra* text accompanying notes 118–27.

[247] Gershgorn, *supra* note 72.

[248] *Id.*

[249] *See* Klosowski, *supra* note 41.

[250] *See supra* text accompanying notes 233–35.

[251] Osoba & Yeung, *supra* note 31.

recognition products and tools should be made open to third-party organizations, such as NIST,[252] or the public for independent review.[253] Such an approach may allow experts outside of the facial recognition development team to audit the accuracy of the system and catch potential biases.[254]

Like any other algorithmic system, law enforcement facial recognition is only as good as the data used to train it.[255] The result is that some algorithms risk reproducing and even magnifying human biases, especially those impacting historically vulnerable and marginalized groups.[256] Generally, most facial recognition training data sets are estimated to be more than 75 percent male and more than 80 percent white, resulting in high error rates for people and faces that do not fall into either of those categories.[257]

To improve the design of today's facial recognition systems, a federal rule must ensure a more diverse data set so that underrepresented demographics are better reflected in training data.[258] Algorithmic bias can arise from training data that is "unrepresentative or incomplete" as well as reliance on data that

[252] *See* Gershgorn, *supra* note 72 ("By framing its test as a competition, NIST has incentivized companies developing facial recognition to voluntarily step into the spotlight, and in the process created the most complete available list of companies in the space."). While NIST "maintains that its facial recognition vendor test is a purely scientific ranking of accuracy," NIST's work, including its vendor verification tests, are sponsored by organizations such as the FBI and DHS. *Id.* Currently, vendors need not obtain NIST verification to sell facial recognition software in the United States. *Id.* Although NIST's vendor list is not exhaustive, it is likely the most complete list available to the public, which underscores the lack of verifiable data on surveillance technology. *Id.*

[253] Osoba & Yeung, *supra* note 31.

[254] *Id.*

[255] Mayson, *supra* note 81, at 2224 ("[I]f the thing that we undertake to predict—say arrest—happened more frequently to [B]lack people than to white people in the past data, then a predictive analysis will project it to happen more frequently to [B]lack people than to white people in the future."); Lohr, *supra* note 80, at 1 ("In modern artificial intelligence, data rules. A.I. software is only as smart as the data used to train it. If there are many more white men than [B]lack women in the system, it will be worse at identifying the [B]lack women.").

[256] *See* Nicol Turner Lee et al., *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms*, BROOKINGS INST. (May 22, 2019), https://brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms [https://perma.cc/NU89-NJK9].

[257] *See* Buolamwini & Gebru, *supra* note 21, at 6–7 (citing to commonly used data sets which are overwhelmingly white and majority male).

[258] *See* Lee et al., *supra* note 256.

is tainted by historical inequalities.[259] If left to its own devices, biased algorithms can encode discriminatory policy decisions, even when designers and developers have the best intentions.[260] The goal of diverse training data sets is to have the data reflect the faces seen in the world, not just in mugshot databases or facial images collected from biased policing practices.[261]

Accordingly, federal facial recognition legislation should set requirements for training data used to train facial recognition systems. Specifically, face images used to train these algorithms should be representative of the communities they may be deployed in. Increasing phenotypic and demographic representation in facial recognition training data sets is the first step to ensuring the technology that is deployed is more accurate than it currently is.[262]

An auditing mechanism in a federal facial recognition law would also address the growing fears around the technology, particularly by ensuring transparency and even accountability in the ways the police, prosecutors, and tech companies use high-tech tools.[263] In February 2019, DHS published results from testing eleven commercial systems designed to check a person's identity.[264] DHS's internal privacy watchdog recommended publicly reporting the performance of its deployed facial recognition systems on different racial and ethnic groups.[265] Therefore, vendors should be required to provide documentation that explains the capabilities and limitations of their facial recognition products in terms that the general public can understand. Although a public disclosure mandate alone may not be enough to improve the accuracy and fairness of facial

[259] *See* Lee et al., *supra* note 256.

[260] *See id.* (discussing examples of Facebook and Amazon whereby seemingly race-neutral coding unintentionally resulted in algorithmic bias).

[261] *See id.* (advocating for diversity solutions that reduce disparities without compromising overall performance).

[262] Buolamwini & Gebru, *supra* note 21, at 3–4.

[263] *See* Etzioni, *supra* note 242, at 1 (proposing how transparency and openness about system capabilities and limitations may address constitutional concerns).

[264] Cynthia M. Cook et al., *Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*, IEEE TRANSACTIONS ON BIOMETRICS, BEHAV., & IDENTITY SCI. , Feb. 2019, at 1, https://ieeexplore.ieee.org/document/8636231 [https://perma.cc/WLY7-TJDV].

[265] U.S. DEP'T OF HOMELAND SEC., DATA PRIV. & INTEGRITY ADVISORY COMM., REP. 2019-01, PRIVACY RECOMMENDATIONS IN CONNECTION WITH THE USE OF FACIAL RECOGNITION TECHNOLOGY 10 (2019).

recognition, it is a necessary first step to holding vendors accountable for flawed technology. Still, tech companies cannot be left to their own devices, to continue developing and selling flawed products. Individual privacy cannot be at the whim of the self-regulating tech industry; however, the best aspects of industry, such as competition and innovation, can reform our inadequate regulatory system.[266]

B. Setting up Shop: Crafting a New Regulatory-Industry Model

In 2016, the Obama administration published a report on algorithmic systems and civil rights that called for the development of an algorithmic auditing and accountability industry.[267] More specifically, private actors, such as developers, should use emerging technologies to proactively address fairness and discrimination in algorithmic systems.[268] For our ability to benefit from AI-enabled tools as well as our ability to preserve civil liberties are contingent on our institutions' capacity to regulate the development and deployment of these technologies.[269] Unfortunately, government regulation of high-tech tools like facial recognition is insufficient because public institutions lack the resources, expertise, and political coherence to effectively rein in a tech industry that has largely avoided government oversight and neglected public interest.[270]

The U.S. government already outsources their responsibilities as regulators, often leaving industry to regulate itself.[271] After

[266] *See* Gillian Hadfield, *An AI Regulation Strategy That Could Really Work*, VENTUREBEAT (Feb. 8, 2020, 6:16 AM) (discussing the prospect and benefits of a private regulators market), https://venturebeat.com/2020/02/08/an-ai-regulation-strategy-that-could-really-work [https://perma.cc/XE47-7DC6]; *see also* Jack Clark & Gillian K. Hadfield, *Regulatory Markets for AI Safety*, ARXIV, at 9–10 (2019) (outlining potential benefits that may accrue from privatization of the regulation), https://arxiv.org/pdf/2001.00078.pdf [https://perma.cc/P2FH-9P9P].

[267] *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, Executive Office of the President, May 2016, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf [https://perma.cc/G4U2-PGWC] (promoting academic research and industry development of algorithmic auditing and external testing of big data systems to ensure fair treatment).

[268] *See id.* at 23 (calling for market participants to independently develop and adopt accountability mechanisms).

[269] *See* Clark & Hadfield *supra* note 266.

[270] *See id.* at 1 (discussing the public sector's generally limited resources at developing comprehensive regulatory schemes and examples of such instances).

[271] *See generally* Sidney A. Shapiro, *Outsourcing Government Regulation*,

failed attempts in the late-1990s to use privacy torts to address data privacy issues online, companies on the Internet voluntarily drafted privacy policies to simultaneously promote their privacy practices and stave off regulation with self-regulation.[272] Today, tech companies continue to evade full responsibility by, for instance, using self-created entities like Facebook's Oversight Board—"an illegitimate substitute for adequate policy enforcement"—as a way to put off actionable steps to resolve misinformation, hate speech, and content moderation issues.[273] The consequences of flawed technology in the law enforcement context are even more dire, endangering life, liberty, and justice.

A competitive regulatory-industry model is a new approach that can close the gap left by traditional regulatory agencies' limited resources and enforcement measures while incentivizing private actors to devise "more effective and less burdensome ways to provide a service."[274] Establishing an industry model that pairs robust government oversight with independent private regulators can also lead to public-private collaboration and achievable goals and targets. The key player in this regulatory-industry model is the independent regulator, a private actor like a company or government contractor. This private regulator develops new ways to meet goals set by the federal government and regulatory agencies, competing to provide regulatory services facial recognition vendors are required by federal law to

DUKE L.J. (2003) ("The government has increasingly relied on private means to achieve public ends, not only involving services to the public, but the origination and implementation of regulatory policy as well.").

[272] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 593–94 (2014) ("The goal was in part to convince policymakers that self-regulation could work and that no additional regulation was needed.").

[273] Arisha Hatch, *Big Tech Companies Cannot Be Trusted to Self-Regulate: We Need Congress to Act*, TECHCRUNCH (Mar. 12, 2021, 9:26 AM) ("[L]eaders at these tech giants have demonstrated time and time again that they will choose not to implement and enforce adequate measures to stem the dangerous misinformation, targeted hate and white nationalist organizing on their platforms if it means sacrificing maximum profit and growth."), https://techcrunch.com/2021/03/12/big-tech-companies-cannot-be-trusted-to-self-regulate-we-need-congress-to-act [https://perma.cc/2NG7-3VQ9]; *see also* Brian Fung, *Facebook's Oversight Board is Finally Hearing Cases, Two Years After it was First Announced*, CNN (Oct. 22, 2020, 12:45 PM), https://cnn.com/2020/10/22/tech/facebook-oversight-board/index.html [https://perma.cc/M2DM-MURW].

[274] *See* Hadfield, *supra* note 266 (NIST, for example, already sets standards for facial recognition software, but lacks the regulatory power to actually enforce their standards, instead relying on the possibility that these standards become trade customs).

purchase. These regulatory services may involve auditing requirements for checking accuracy and bias or evaluating the composition of face images in the training data.[275]

To prevent this model from being a race to the bottom, with private regulators competing to be the most lenient regulator, the government must regulate the regulators.[276] Just as private regulators are expected to be experts in AI and algorithmic bias detection, the government has expertise in regulation and enforcement.[277] Private regulators must obtain a government-issued license to compete in this new algorithmic auditing and accountability industry.[278] The issue and maintenance of this license depends on a private regulator's demonstrated and reported services to achieve goals set forth by the government.[279]

As a result, strong government oversight and appealing economic incentives are crucial for the success of the regulatory-industry model. The government must effectively collaborate with private regulators to set goals that legitimately improve technology for the public interest and private regulators must fear losing their license to compete in this industry if they fail to meet the government's goals.[280] The federal government figured out how to attract tech startups with military contracts, so why not create similarly attractive incentives for regulatory solutions that can protect civil liberties?[281]

This public-private hybrid model can demystify facial recognition systems through, for example, audits and enforceable

[275] *See* discussion *supra* Part III.A.

[276] *See* Hadfield, *supra* note 266.

[277] *See id.*

[278] *See id.*

[279] *See* Clark & Hadfield, *supra* note 266, at 8–9.

[280] *Id.* at 9.

[281] *See* Jasmine Garsd, *When Technology Can Be Used to Build Weapons, Some Workers Take a Stand*, NPR (May 13, 2019, 6:23 PM), https://npr.org/2019/05/13/722909218/when-technology-can-be-used-to-build-weapons-some-workers-take-a-stand [https://perma.cc/4LF6-2LFR]; Mrinal Menon & Jeff Decker, *Why the Defense Industry Could be the Most Transformative Market for Startups*, FAST COMPANY (May 10, 2021), https://fastcompany.com/90634168/why-the-defense-industry-could-be-the-most-transformative-market-for-startups [https://perma.cc/F2PB-M3TF] ("The military awarded $445 billion contracts in 2020 . . . To attract interest the Defense Department is handing out unprecedented numbers of small contracts and in 2020 seeded 1,635 firms with more than $1.5 billion in early funding. Dozens of outreach programs across the military now offer quick revenue to early-stage companies. A startup could land a contract worth up to $3 million within months of entering the defense market.").

accuracy standards. There is potential here to revolutionize facial recognition regulation, making it a less daunting and opaque issue. At the very least, an algorithmic auditing and fairness industry could entice public interest technologists and algorithmic auditing companies that may be struggling to do business since fixing flawed technology remains a voluntary endeavor. Dangerous technologies like facial recognition must be regulated—and soon. What happens if AI-enabled tools are cemented in our daily lives before its flaws are fully addressed?

C. Beyond Technology: Rethinking Policing in America and Untangling Technological Inevitability

In 18th century New York, "lantern laws" required enslaved people to carry lanterns after dark to be publicly visible.[282] Some computer scientists argue that, with enough training from more diverse and representative data sets, AI systems that inform facial recognition can eventually be rid of bias.[283] However, even a system capable of recognizing people with perfect accuracy might still cause terrible harm.[284] A concern is that equitable facial recognition algorithms could still be deployed with the same intent as the 18th-century lantern laws, disproportionately affecting Black communities in the same ways as longstanding, racist law enforcement policies.[285] Inaccurate and defective facial recognition algorithms can be harmful to people of color, but accurate algorithms have the potential to be even more dangerous, enabling the government to target marginalized populations.[286]

George Floyd's murder by the Minneapolis Police Department called attention to discriminatory law enforcement practices.[287]

[282] *See* Claudia Garcia-Rojas, *The Surveillance of Blackness: From the Trans-Atlantic Slave Trade to Contemporary Surveillance Technologies*, TRUTHOUT (Mar. 3, 2016), https://truthout.org/articles/the-surveillance-of-blackness-from-the-slave-trade-to-the-police [https://perma.cc/V92J-HKRK], ("Lantern laws were 18th century laws in New York City that demanded that Black, mixed-race and Indigenous enslaved people carry candle lanterns with them if they walked about the city after sunset, and not in the company of a white person. The law prescribed various punishments for those that didn't carry this supervisory device. Any white person was deputized to stop those who walked without the lit candle after dark.").

[283] Ivanova, *supra* note 109.

[284] *Id.*

[285] Najibi, *supra* note 129.

[286] *Id.*

[287] *See generally* Erik Ortiz, *Aggressive Policing Tactics Called into Question*

Because police arrest and incarcerate Black Americans more often than white Americans, Black people are overrepresented in mugshot databases, which are used to train many police facial recognition systems.[288] The presence of Black people in these databases produce a "feed-forward loop whereby racist policing strategies lead to disproportionate arrests of Black people, who are then subject to future surveillance."[289]

For example, predictive policing systems generally rely on historical crime data to make predictions about where future crimes are likely to occur.[290] However, reported crime data is not neutral.[291] Historical crime data is "a reflection of the police department's practices and priorities; local, state, or federal interests; and institutional and individual biases."[292] A facial recognition system, especially one that relies on mugshot databases, "holds a mirror to the past."[293] Perfectly reproducing a pattern of biased policing and relying on data collected "under status quo conditions is simply to project history forward."[294]

Restrictions on the individuals included in facial recognition data sets can prevent people charged with lesser offenses, such as parking violations, from being caught in a police facial recognition dragnet.[295] Only individuals with an active arrest warrant should be included in the data set—and only for a short period of time.[296] Until proper legal and technical safeguards are developed and ready to be deployed, a moratorium should be put in place to prevent the inevitable harm that will result from a fundamentally flawed application of facial recognition. Over the past two decades, our commitment to "innovation" and "disruption" has bordered on religious. We must meet this zeal

as National Protests Flare, NBC NEWS (May 31, 2020), https://nbcnews.com/news/us-news/aggressive-policing-tactics-called-question-national-protests-flare-n1220471 [https://perma.cc/JHD5-XATP].

[288] Kade Crockford, *How is Face Recognition Surveillance Technology Racist?,* ACLU (June 16, 2020), https://aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist [https://perma.cc/4MV5-5CZM]; Najibi*, supra* note 129.

[289] Najibi, *supra* note 129.

[290] Ivanova, *supra* note 109.

[291] *Id.*

[292] *Id.*

[293] Mayson, *supra* note 81, at 2224 (explaining AI algorithm predictive analysis as effectively "distill[ing] patterns in past data and interpret[ing] them as projections of the future").

[294] *Id.*

[295] Bala & Watney, *supra* note 224.

[296] *Id.*

with an equally powerful conviction that technology can and should be designed and used with the public interest in mind.

CONCLUSION

Nearly a century later, as new technologies embed themselves in our society and legal system in earnest, Justice Brandeis's dissent in *Olmstead* is perhaps more poignant than ever:

> Time . . . brings into existence new conditions and purposes. Therefore, a principle . . . must be capable of wider application than the mischief which gave it birth. This is peculiarly true of Constitutions. They are not ephemeral enactments, designed to meet passing occasions. They are . . . designed to approach immortality as nearly as human institutions can approach it. . . . [T]herefore, our contemplation cannot be only of what has been but of what may be.[297]

The promise of facial recognition law and policy is to ensure that the owners and developers of this technology and its algorithms are more accountable to the public.[298] If left unchecked, these powerful tools will undermine privacy, entrench bias, and create a surveillance apparatus ripe for abuse.[299] A legislative response to facial recognition must go beyond limiting police use of this technology. A truly comprehensive federal facial recognition law should supplement the Fourth Amendment by considering crime severity when determining when it is appropriate to use facial recognition; requiring independent audit and review before the technology can be purchased by law enforcement agencies; and ensuring diverse training data sets so that the algorithms powering facial recognition can accurately identify different faces.

Facial recognition is already here. It is time for the law to catch

[297] Olmstead v. United States, 277 U.S. 438, 472–73 (1928) (Brandeis, J., dissenting) (internal quotations omitted).

[298] *See* Robyn Caplan et al., *Algorithmic Accountability: A Primer*, DATA & SOC'Y 22 (Apr. 18, 2018) ("Algorithmic accountability ultimately refers to the assignment of responsibility for how an algorithm is created and its impact on society; if harm occurs, accountable systems include a mechanism for redress."), https://datasociety.net/wp-content/uploads/2019/09/DandS_Algorithmic_Accountability.pdf [https://perma.cc/SBR3-B3CZ]. Edward Rubin has defined accountability as "the ability of one actor to demand an explanation or justification of another actor for its actions, and to reward or punish the second actor on the basis of its performance or its explanation." Edward Rubin, *The Myth of Accountability and the Anti-Administrative Impulse*, 103 MICH. L. REV. 2073, 2073 (2005).

[299] duPont, *supra* note 18.

up. One way or another, the response to the widespread use of facial recognition and other government surveillance technologies will determine whether hard-won civil liberties endure or become forgotten relics.[300] Facial recognition continues to be increasingly ubiquitous while information about the way it is used becomes more and more opaque.[301] Law enforcement's surveillance capabilities have come a long way: from reactive policing to proactive monitoring;[302] from individual surveillance to mass surveillance.[303] The algorithmic auditing and accountability industry model proposed in this article offers a far-reaching yet pragmatic solution that prioritizes transparency and targets the most problematic characteristics of facial recognition technology and the way law enforcement uses it. The development of enforceable standards is a necessary first step to ensure historical biases and systems of oppression are not replicated. If we do not demand racially neutral tools and radically revise racist police practices, new technologies will be doomed to repeat our country's racially unequal history.

[300] WASHINGTON & RICHARDS, *supra* note 17, at 366.

[301] Gershgorn, *supra* note 72. Hundreds of companies develop facial recognition systems. *Id.* But after IBM, Amazon, and Microsoft pulled access to its facial recognition software from law enforcement in June 2020, only a handful of other facial recognition companies took similar action. Kevin Truong, *We Asked 43 Facial Recognition Companies if They'll Refuse to Work with Cops*, VICE (June 11, 2020, 9:57 AM), https://vice.com/en/article/pkygg7/we-asked-43-facial-recognition-companies-if-theyll-refuse-to-work-with-cops [https://perma.cc/NB9U-6GKY].

[302] *See* JAMES FORMAN, JR., LOCKING UP OUR OWN: CRIME AND PUNISHMENT IN BLACK AMERICA 20, 22–25 (Farrer, Straus and Giroux eds., 2017).

[303] *See* LIN, *supra* note 159, at 13.