October 21, 2019

Facial Recognition and the Fourth Amendment

Andrew Guthrie Ferguson, *American University Washington College of Law*

(REVISED DRAFT)

FACIAL RECOGNITION AND THE FOURTH AMENDMENT

Andrew Guthrie Ferguson [*]

Abstract

Facial recognition offers a totalizing new surveillance power. Police now have the capability to monitor, track, and identify faces through networked surveillance cameras and datasets of billions of images. Whether identifying a particular suspect from a still photo, or identifying every person who walks past a digital camera, the privacy and security impacts of facial recognition are profound and troubling.

This Article explores the constitutional design problem at the heart of facial recognition surveillance systems. 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 permeating surveillance technology. But current doctrine and constitutional theory offers little privacy protection and less practical security than one might expect. Even worse, by studying the Fourth Amendment through the lens of facial recognition technology other doctrinal limitations come into focus. Issues of error rates, racial bias, unfairness, and transparency in policing more generally become magnified when trying to design a new surveillance system for law enforcement.

The Article then offers a constitutional design solution to some forms of facial recognition surveillance. The Supreme Court's recent cases on *digital technologies suggest a way to "future-proof" the Fourth Amendment in the face of certain types of mass surveillance technologies. In addition, this Article suggests a new legislative framework for facial recognition to fill in the privacy and legitimacy gaps left by the current Fourth Amendment doctrine.*

[*] Visiting Professor of Law, Washington College of Law at American University. Professor of Law, UDC David A. Clarke School of Law. Thank you to Professors Andrew Selbst, Richard Re, Elizabeth Joh, Megan Thorn Stevenson, Stephen Henderson, Kiel Brennan-Marquez, Manon Jendly, Elana Zeide, Alicia Solow-Niederman, Barry Friedman, Kate Weisburd, Avlana Eisenberg, Chad Flanders, Lewis Grossman, and Daniela Kraiem. Thank you also to the ABA/AALS Criminal Justice Scholars workshop for terrific feedback.

INTRODUCTION

Artificial intelligence systems are edging into policing.[1] Massive troves of sensor data, unstructured video surveillance feeds, and many other digital clues all allow artificial intelligence to make sense of otherwise overwhelming amounts of information.[2] The ability to harness artificial intelligence for police surveillance and investigation portends an era-defining shift of power and capabilities.

Leading the charge of game-changing new surveillance technologies is facial recognition – namely the ability to identify faces among crowds, in videos, in photo datasets, and almost everywhere else.[3] From scanning Super Bowl crowds and public streets, to searching stored arrestee mugshots, police are beginning to experiment with facial recognition technology.[4] This development is also causing great public concern, because the scope and scale of these new surveillance systems threatens to upend the existing power relationship between police and the people.[5]

This Article explores the constitutional design problem at the heart of facial recognition surveillance systems. One might hope that the Fourth Amendment[6] – designed to restrain police power and enacted to limit governmental overreach – would have something to say about this powerful and overreaching generalized surveillance technology. But current doctrine and constitutional theory offers little privacy protection and less practical security than one might expect. Even worse, by studying the Fourth Amendment through the lens of facial recognition technology other doctrinal limitations come into focus. Issues of error, bias, unfairness, and opacity in

[1] Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 GA. L. REV. 109, 113 (2017); *see generally* Sarah Brayne, *The Criminal Law and Law Enforcement Implications of Big Data*, 14 ANN. REV. L. & SOC. SCI. 293, 294 (2018); Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 16 (2016).

[2] *See generally*, Andrew Guthrie Ferguson, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017).

[3] Clare Garvie et al., Geo. L. Ctr. on Privacy & Tech., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 1 (2016).

[4] *See e.g.*, Declan McCullagh, *Call It Super Bowl Face Scan I*, WIRED (Feb. 2, 2001), http://www.wired.com/politics/law/news/2001/02/41571; Dakin Andone, *Police Used Facial Recognition to Identify the Capital Gazette Shooter. Here's How It Works*, CNN (June 29, 2018, 6:22 PM), https://www.cnn.com/2018/06/29/us/facial-recognition-technology-law-enforcement/index.html [https://perma.cc/D7JC-EWJ]; Benjamin Powers, *Eyes over Baltimore: How Police Use Military Technology to Secretly Track You*, ROLLING STONE MAG. (Jan. 6, 2017).

[5] John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns-Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97 (1997) ("Any high-integrity identifier [such as biometric scanning] represents a threat to civil liberties, because it represents the basis for a ubiquitous identification scheme, and such a scheme provides enormous power over the populace. All human behavior would become transparent to the state, and the scope for non-conformism and dissent would be muted to the point envisaged by the anti-Utopian novelists.") (quoting Roger Clarke, *Human Identification in Information Systems: Management Challenges and Public Policy Issues*, Info. Tech. & People, Dec. 1994, at 29).

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

policing more generally become magnified when trying to design a new surveillance system for law enforcement.[7]

Understanding the limitations of the Fourth Amendment in the face of new law enforcement technology is important for three independent reasons. First, the analysis shows that the Fourth Amendment will not save us from the privacy threat created by facial recognition surveillance. The Supreme Court's recent Fourth Amendment jurisprudence only goes so far, leaving significant privacy gaps to fill. Second, the planned designs for facial recognition systems raise core police legitimacy issues around error rates, racial bias, fairness, and transparency, issues that the current Fourth Amendment has largely ignored.[8] The danger of building an algorithmic model to match a flawed Fourth Amendment doctrine invites deeper inquiry into the weaknesses of both the technology and the doctrine itself. Finally, the revealed weaknesses help shape a more privacy protective and legitimate legislative framework to regulate any future growth of facial recognition technology.[9]

Part I of this Article describes how facial recognition technology will be used by police. This section looks at the surveillance capabilities of the technology as well as how police might use different versions to conduct face surveillance, face tracking, face identification, and other non-law enforcement tasks like face verification at the international border.

Part II examines how the Fourth Amendment (as the traditional constitutional protection against police power) might respond to the privacy concerns raised by facial recognition technology. The answer is unfortunately unsatisfying as the Supreme Court's recent guidance on digital surveillance searches remains inadequate, leading to a frustrating sense of uncertainty.[10] The discussion reveals the gaps in Fourth Amendment doctrine which will require a legislative response.

Part III examines how the Fourth Amendment fails to address issues of error, racial bias, fairness, and transparency in policing generally, and facial recognition more specifically. This part reveals how traditional Fourth Amendment doctrine largely sidesteps problems that are central to police legitimacy. Arguably, the current design of the Fourth Amendment would allow for the design of facial recognition systems rife with error, bias, unfairness, and opacity, further undermining police legitimacy.

Finally, Part IV takes on the task of proposing a legislative framework to regulate facial recognition consistent with existing Fourth Amendment law. This section examines the core principles that any legislative response to facial recognition should include – principles that prohibit law enforcement

[7] *See infra* Part III.
[8] *Id*. at III.A.
[9] *See infra* Part IV.
[10] *See infra* Part II.A

access to some face surveillance technology, tighten the legal protections for access to face identification and face tracking technology, and address the recurring concerns of bias, accuracy, transparency, fairness and privacy in all types of facial recognition technology.

By studying the Fourth Amendment through the lens of facial recognition technology, new insights surface about the doctrine's limitations as a check on constitutional policing. Equally revealing, however, is the new legislative framework which emerges to regulate systems of digital surveillance like facial recognition.

I. FACIAL RECOGNITION TECHNOLOGY

If there is one technological innovation that has gotten the attention of the privacy and civil rights community it is facial recognition.[11] The simple idea behind facial recognition is to have a computer program automatically match a digital image of a face with a similar digital image of a face in a stored database.[12] To work, a computer program is run on existing digital photographs or video surveillance cameras turning images into a digital network of identifiable objects and faces. As will be discussed in this Part, there are different types of facial recognition technologies with corresponding applications for police use.

A. The Technology

Facial recognition is a digital matching technology.[13] In practice, digital images of faces are broken down into identifiable component parts.[14] Traditionally, facial recognition technology has been "feature-based"

[11] *See e.g.*, Matt Cagle & Nicole A. Ozer, *Amazon Teams up with Law Enforcement to Deploy Dangerous New Face Recognition Technology*, ACLU of N. Cal. (May 22, 2018), https://www.aclunc.org/blog/amazon-teams-law-enforcement-deploy-dangerous-new-face-recognition-technology [https://perma.cc/WYF4-7XDT*]*; Fran Spielman, *ACLU Sounds the Alarm About Bill Allowing Use of Drones to Monitor Protesters*, CHI. SUN-TIMES (May 1, 2018, 5:17 PM), https://chicago.suntimes.com/politics/aclu-sounds-the-alarm-about-bill-allowing-use-of-drones-to-monitor-protesters; Clare Garvie et al., Geo. L. Ctr. on Privacy & Tech., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 1 (2016).

[12] Kirill Levashov, *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) ("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."); Clare Garvie & Jonathan Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, ATLANTIC (Apr. 7, 2016), https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/ [https://perma.cc/4L5J-AXR4].

[13] For purposes of this article "facial recognition" will be used as a generic term covering all of the different types of face matching technology. Facial recognition is the global term whereas face surveillance, face identification, face tracking, and face verification are more specific types of facial recognition technology.

[14] *In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 HARV. L. REV. 1870, 1870-71 (2007).

utilizing identifying measures like one's eyes, nose, and mouth and the distances between these features,[15] or "appearance-based" which attempts to match the whole face image.[16] In recent years, other forms of identification have emerged looking at skin textures,[17] shadows,[18] or three dimensional models,[19] or some combination of all of these types.[20]

In simple form, the digital faceprint is like a digital fingerprint, a map written in code that measures the distance between features, lines, and facial elements or some other digital code.[21] When one digital representation of a face is compared to another digital representation of a face and the code lines up the same, the computer will deem the process a match. These digitized images are stored in large datasets so that a computer model can train itself on what constitutes a "match." In many systems, returned "matches" involve more than one image and may involve as many as 20-50 similar faceprints. These face images are provided in order of the closeness of an overlap of the fixed digital features. So, for example, a police officer who seeks a match for a probe photograph of a suspect may receive 20 faceprints back as possible matches.

[15] Jagdish Chandra Joshi and K K Gupta, *Face Recognition Technology: A Review*, 1 THE IUP JOURNAL OF TELECOMMUNICATIONS, 53, 54 (2016) ("[F]eature-based methods… are based on local facial characteristics (such as eyes, nose and mouth) and use parameters such as angles and distances between ducial points on the face as descriptors for face recognition."); Relly Victoria Virgil Petrescu, *Face Recognition as a Biometric Application*, 3 JOURNAL OF MECHATRONICS AND ROBOTICS, 237, 240 (2019) ("Certain face recognition algorithms identify facial features by extracting markers or features from a face-to face image. For example, an algorithm can analyze the position, size and/or relative shape of the eyes, nose, cheekbones and jaw. These features are then used to look for other matching features."); Mary Grace Galterio et.al., *A Review of Facial Biometrics Security for Smart Devices*, COMPUTERS 2018, 7, 37 at 3 ("Face metric uses the normal face picture, or the canonical image, to inspect special features of the face. These features include the distance between the eyes, distances of eyes to nose, mouth to nose, and many others. These metrics are used and stored as a template to be compared to for future recognition.")

[16] Jagdish Chandra Joshi and K K Gupta, *Face Recognition Technology: A Review*, 1 THE IUP JOURNAL OF TELECOMMUNICATIONS, 53, 53-54 (2016) ("Appearance-based methods consider the global properties of the face and use the whole face image (or some specific image regions) to extract facial features."); Relly Victoria Virgil Petrescu, *Face Recognition as a Biometric Application*, 3 JOURNAL OF MECHATRONICS AND ROBOTICS, 237, 240 (2019) ("Other algorithms normalize a gallery of images and compress the face data, saving only image data that is useful for face recognition. A probe image is then compared to face data.").

[17] Relly Victoria Virgil Petrescu, *Face Recognition as a Biometric Application*, 3 JOURNAL OF MECHATRONICS AND ROBOTICS, 237, 241 (2019) ("Another emerging trend uses the visual details of the skin as captured in standard or scanned digital images. This technique, called Skin Texture Analysis, transforms lines, patterns and unique stains into a person's skin in a mathematical space.").

[18] Mary Grace Galterio et.al., *A Review of Facial Biometrics Security for Smart Devices*, COMPUTERS 2018 7, 37 at 3 ("The eigenface technology works differently, as it changes the presented face's lighting by using different scales of light and dark in a specific pattern. The different light and dark areas computed on the face cause the picture displayed to not actually look like a face anymore. The pattern created from the shaded areas is very important, however, as it is a way to portray and calculate how the different features of the face are singled out and to evaluate the symmetry of the face. The pattern is calculated to a degree of eigenfaces, or eigenvectors, that is determined by including facial hair or the size of facial features. Using different numbers of eigenvectors to calculate a face can allow for easy reconstruction.").

[19] Relly Victoria Virgil Petrescu, *Face Recognition as a Biometric Application*, 3 JOURNAL OF MECHATRONICS AND ROBOTICS, 237, 240-41 (2019) ("Three-dimensional face recognition technology uses 3D sensors to capture information about the shape of a face. This information is then used to identify distinctive features on the surface of a face, such as the outline of the eye, nose and chin sockets").

[20] *Id*. at 241.

[21] *See generally*, Kirill Levashov, *The Rise of A New Type of Surveillance for Which the Law Wasn't Ready*, 15 COLUM. SCI. & TECH. L. REV. 164, 167 (2013).

To work, systems must acquire faces, classify them, train the data, and test the training sets, so the systems can identify the overlapping nodal points of any face in the system.[22] Even after a list of matching faceprints is returned by the system, an analyst will review the images to select a final suspect for investigation (if any).

Facial recognition technology comes in different forms and can be used for different purposes. As will be discussed in more detail later, one use is "face surveillance" which involves the generalized mass identification of individuals using face matching technology.[23] Face surveillance has been used in China as a means to identify people on busy streets or in train stations.[24] Another use is "face identification" which involves the matching of a particular face (a suspect) to a database of existing photographs (a mugshot database or DMV records).[25] Face identification is being piloted by police as a revolutionary investigative tool akin to DNA matching[26] and is also being piloted in some commercial venues to enhance private security.[27] Third, there is "face tracking" which is a hybrid of face surveillance and face identification. Face tracking involves police use of stored or real time video to track a targeted suspect. For example, after a bank robbery, police could search city video feeds to find the path of the fleeing suspect. Finally, there is "face verification" which involves confirming that a particular human face matches a preset digital image of that face.[28] Face verification is already

[22] U.S. Gov't Accountability Office, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law* 3 (2015), http://www.gao.gov/assets/680/671764.pdf [perma.cc/U9GG-J7NS].

[23] "Face surveillance" is defined here in as the mass collection of faceprints for pure monitoring and surveillance purposes. This will be distinguished from "face identification" which involves the matching of face images only after police have some individualized suspicion of an individual with static photo datasets.

[24] Simon Denyer, *China's Watchful Eye: Beijing Bets on Facial Recognition in a Big Drive for Total Surveillance*, WASH. POST (Jan. 7, 2018), https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance; Josh Chin, *Chinese Police Add Facial-Recognition Glasses to Surveillance Arsenal*, WALL STREET J. (Feb. 7, 2018, 6:52 AM), https://www.wsj.com/articles/chinese-police-go-robocop-with-facial-recognition-glasses-1518004353.

[25] Joy Buolamwini, *Response: Racial and Gender Bias in Amazon Rekognition—Commercial AI System for Analyzing Faces*, MEDIUM (Jan. 25, 2019) https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced.

[26] Asha McLean, *How One Sheriff's Office Is Using Machine Learning to Uncover Persons of Interest*, ZDNET (Nov. 30, 2017, 11:31 PM), https://www.zdnet.com/article/how-one-sheriffs-office-is-using-machine-learning-to-uncover-persons-of-interest/ [https://perma.cc/4KJS-D49T].

[27] Lisa Respers, *Taylor Swift Reportedly Used Facial Recognition to Try to ID Stalkers*, CNN (Dec. 13, 2018).

[28] Joy Buolamwini, *Response: Racial and Gender Bias in Amazon Rekognition—Commercial AI System for Analyzing Faces*, MEDIUM (Jan. 25, 2019) https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced ("Some facial recognition is used to perform tasks like unlocking a phone or getting access to a bank account. This is known as facial verification.").

being piloted at international borders to confirm identity[29] and in airports to replace airplane boarding passes.[30]

Of the four types of facial recognition, *face verification* tends to be a most accurate, because the match is a binary confirmatory yes/no choice built around a high quality photo like a passport or government identification card.[31] Either the face image from your passport matches the digital photo just taken of you standing in the airport line or not (there is no searching of a larger dataset to compare the images against).[32] On the other hand, *face identification* requires searching through thousands (millions) of images for the appropriate match and finding the "best" match.[33] Still portraits like those in passport or drivers' license identifications are easier to match than photographs taken of people while moving or with hats or glasses which require understanding angles, perspectives, and lighting. *Face surveillance* and *face tracking* are the most complicated use because the matches are being done in real time or across vast streams of digital images with many more possibilities for error or misidentification.[34] Issues of age, race, clothing, facial hair, hair style, hats and other accessories all can impact the accuracy of the identification done at scale.

To work as intended, facial recognition needs at least two sets of images. A photograph or collection of known faces digitized to their faceprint and a second digital dataset to match those faceprints against. The set of faceprints can come from still images (driver's license photos, mugshot photos, Facebook photos), and once digitized be matched to other still photos

[29] Mallory Locklear, *DHS Will Use Facial Recognition to Scan Travelers at the Border*, ENGADGET, (June 6, 2018); https://www.engadget.com/2018/06/05/dhs-facial-recognition-scan-travelers-at-border/; Relly Victoria Virgil Petrescu, *Face Recognition as a Biometric Application*, 3 JOURNAL OF MECHATRONICS AND ROBOTICS, 237, 238 (2019) ("Face recognition has become a normal activity in many airports around the world. Many people today have a so-called biometric passport that allows them to go faster to the gate without having to be controlled."); *id.* at 242 ("The Australian Border Service and New Zealand have created an automated border processing system called SmartGate, which uses face recognition, which compares the passenger's face with the e-passport microchip data.").

[30] Lori Aratani, *Your Face is Your Boarding Pass at this Airport*, WASH. POST (Dec. 4, 2018) ("An increasing number of airports are using biometrics to process passengers as they move through the system. Dulles International Airport recently unveiled a system that uses iPads to scan passengers' faces before they board flights. U.S. Customs and Border Protection has been using biometrics to track passengers entering the U.S.).

[31] Eisa Anis Ishrat Ullah & M. AkheelaKhanum, *A Comparative Study of Facial Recognition Systems*, 9 INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE, 114, 114 (2018) ("A facial recognition algorithm has its focus on two main tasks i.e. recognition and verification with verification being much more easier as compared to recognition, as verification does a kind of binary mapping by verifying the input image which is already present in the database.").

[32] Customs and Border Patrol Biometric Information, https://www.cbp.gov/frontline/cbp-biometric-testing

[33] Drew Harwell, *Oregon became a testing ground for Amazon's facial-recognition policing. But what if Rekognition gets it wrong?* WASH. POST (April 30, 2019) https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/?noredirect=on&utm_term=.10b8818b5bea)

[34] Eisa Anis Ishrat Ullah & M. AkheelaKhanum, *A Comparative Study of Facial Recognition Systems*, 9 INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE, 114, 114 (2018) ("The major concern for building these systems has remained the accuracy of these systems which varies significantly when put in an unconstrained environment. These systems have to particularly deal with issues such as illumination, lightning, brightness effect, variable poses, hairstyles, facial expressions, noise in the input image.").

or live or stored video stream (surveillance cameras, police body worn cameras, private surveillance cameras etc.). The tremendous scale of digital photographs, video feeds, and growing sophistication of video analytics makes the ability to match faces possible in a wide variety of settings.[35]

B. Police Use of Facial Recognition Technology

Facial recognition surveillance technology is a tool that has many possible uses for law enforcement.[36] Faces can be matched for generalized surveillance purposes, targeted tracking purposes, or just as a means of confirming identity for law enforcement and non-law enforcement purposes. Each potential use raises different Fourth Amendment questions. The next section provides a brief overview of the types of facial recognition technology that will be of most interest to law enforcement.[37]

1. Face Surveillance

Face surveillance involves the generalized monitoring of public places or third-party image sets using facial surveillance technologies to match faces with a prepopulated list of face images held by the government.[38] Police could use "face surveillance" in three ways: (a) scanning stored video footage to identify all faces in the stored data; (b) real-time scanning of video surveillance to identify all faces passing by the cameras; and (c) datamining stored images from third party platforms to identify individuals via their photographs. Each of these different uses will be discussed in turn.

a. Face Surveillance: Searching Stored Video Footage

One potential form of face surveillance is the ability to search stored

[35] *Police Unlock AI Potential To Monitor, Surveil, and Solve Crimes*, WSJ Video, https://www.wsj.com/video/police-unlock-ai-potential-to-monitor-surveil-and-solve-crimes/819D5F78-22BC-4A41-9517-AE31BE3C5E7E.html

[36] Mary Grace Galterio et.al., *A Review of Facial Biometrics Security for Smart Devices*, COMPUTERS 2018 ("Using facial recognition software for surveillance purposes would assist government authorities in locating certain criminals, extremists, and missing children.").

[37] Some portions of this article were originally written as testimony to the House Oversight Committee on how best to regulate facial recognition technologies. *See* Written Testimony of Professor Andrew Guthrie Ferguson Before the House of Representatives Committee on Oversight and Reform Hearing On: *Facial Recognition Technology: (Part 1) Its Impact on our Civil Rights and Liberties*, May 22, 2019, 115 Cong. https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-FergusonA-20190522.pdf.

[38] *See generally*, 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, 94 (2017) ("Generally the facial recognition systems are designed today to seek out patterns in captured images that compare favorably to facial model. Systems are typically programmed such that when a pattern is found to resemble a facial model, the software generates the assumption that there is a face presented in the photo.").

video footage from networked surveillance cameras.[39] Imagine the ability to sort through stored digital video surveillance to identify particular people as they travel through public streets or on public transportation.[40] These cameras can be government owned, private, or from mobile devices such as police-worn body cameras.[41] As digital storage becomes cheaper and more available and as video analytics technology becomes more sophisticated, the vast hours of daily video footage can be datamined for identifiable faces.[42] Face surveillance can match any face in a government dataset to any matching face captured in surveillance data. To be clear, the search in stored footage is not based on any individualized suspicion of a crime or to support a particular criminal investigation, but merely for generalized monitoring of people as they come into contact with the cameras. The resulting scans could locate individuals at any point they are identified by a camera, creating a virtual retrospective map of movements and activities over time.

b. Face Surveillance: Real-Time Monitoring

Another potential form of face surveillance technology is real-time public monitoring. The technology already exists (and is being used in countries like China) to watch the streets and identify people in public spaces using pattern matching technology.[43] Imagine a TV monitor of a city street with every human figure digitally framed by a box around his or her face. As they pass by cameras, personal information displays because the surveillance system has matched a pre-populated faceprint to their real-time presence.[44] Again, in this type of monitoring there is no individualized suspicion of criminal wrongdoing. Generally, the justification for use would be a form of public safety or social control, for example, to identify all of the people jaywalking,[45] or frequenting a sporting event, or entering a gun show.

[39] Clare Garvie & Laura Moy, *America Under Watch* (2019), https://www.americaunderwatch.com/.

[40] Allie Gross, *Experts: Duggan's Denial of Facial Recognition Software Hinges on 3 Words*, DETROIT FREE PRESS, (July 16, 2019) https://www.freep.com/story/news/local/michigan/detroit/2019/07/16/duggan-war-of-words-surveillance-tech/1701604001/

[41] Chris Burt, Motorola Could Offer Facial Recognition with Police Body Cameras with WatchGuard Acquisition, BIOMETRIC UPDATA.COM, (July 23, 2019); https://www.biometricupdate.com/201907/motorola-could-offer-facial-recognition-with-police-body-cameras-with-watchguard-acquisition; but see Madeline Purdue, Axon Body Camera Supplier Will Not Use Facial Recognition in its Products – For Now, USA TODAY (July 1, 2018)

[42] *Police Unlock AI Potential To Monitor, Surveil, and Solve Crimes*, WSJ Video, https://www.wsj.com/video/police-unlock-ai-potential-to-monitor-surveil-and-solve-crimes/819D5F78-22BC-4A41-9517-AE31BE3C5E7E.html.

[43] Paul Mozer, *One Month, 500,000 Face Scans: How China is Using A.I to Profile a Minority*, N.Y. TIMES (April 14, 2019) https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html; *Chinese Man Caught by Facial Recognition at Pop Concert*, BBC News (April 13, 2018) https://www.bbc.com/news/world-asia-china-43751276.

[44] Paul Mozer, *Inside China's Dystopian Dreams, A.I. Shame and Lots of Cameras*, N.Y. TIMES (July 8, 2018) ("China has an estimated 200 million surveillance cameras."). https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

[45] Christina Zhao, *Jaywalking in China: Facial Recognition Surveillance Will Soon Fine Citizens via Text*

Cameras can be fixed, mobile, on drones, or privately owned.

c. Face Surveillance: Datamining Third-Party Stored Images

The same type of generalized face surveillance can be done by scanning private photo datasets or private digital images. Billions of images and videos exist in third party systems like Facebook, Google, Instagram, Twitter, YouTube, and other platforms.[46] Acquiring those images and matching them would allow law enforcement to build dossiers of individuals in a community. Again, this type of face surveillance match would not done for a particularized law enforcement purpose but rather to gather intelligence about individuals in the community.[47] The resulting identifications could involve locational details (both in metadata of the photos and from the context/content of the photos themselves), personal connections, likes, interests, and activities. For example, the latest fabulous photo of your family beach vacation not only shows your family, associations, activities, but also the day, time, and location of the photo. One of the realities of digital photographs is that by design they encode information about location, time, date, camera type, and thus details about where, when, and how the photo was taken.[48] A composite of locational metadata can thus reveal interests, activities, and travel patterns through still digital photographs.

2. Face Identification[49]

Investigative *face identification* technology differs from generalized *face surveillance* because police have suspicion about a particular person. Police may have an image from a crime scene (surveillance tape, witness' iPhone video) or they might have a suspect's photograph and wish to match it with different photo datasets.[50]

Message, NEWSWEEK (March 27, 2018).

[46] Relly Victoria Virgil Petrescu, *Face Recognition as a Biometric Application*, 3 JOURNAL OF MECHATRONICS AND ROBOTICS, 237, 242 (2019) ("DeepFace is a deep learning facial recognition system created by a Facebook research group. It uses a nine-layer neural network with over 120 million connection weights and has been trained on four million images uploaded by Facebook users. It is said that the system is 97% correct.").

[47] Brennan Center Report, https://www.brennancenter.org/analysis/map-social-media-monitoring-police-departments-cities-and-counties.

[48] Thomas Germain, *How a Photo's Hidden 'Exif' Data Exposes Your Personal Information*, CONSUMER REPORTS, (Feb. 26, 2019) https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data/

[49] Note that in past discussions of the subject, I have used the term "face recognition" to cover the category of "face identification" and "face tracking" *See* Written Testimony of Professor Andrew Guthrie Ferguson Before the House of Representatives Committee on Oversight and Reform Hearing On: *Facial Recognition Technology: (Part 1) Its Impact on our Civil Rights and Liberties*, May 22, 2019, 115 Cong. https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-FergusonA-20190522.pdf. In this article, I use the terms face identification and face tracking instead of face recognition for greater clarity and precision.

[50] Jon Schuppe, *How Facial Recognition became a Routine Policing Tool in America*, NBC NEWS (May 11, 2019) https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251; Drew Harwell, *Oregon became a Testing Ground for Amazon's Facial-recognition Policing. But What*

In what has been a common practice in some jurisdictions, police may wish to match a target's face image with a database of other face images in their possession.[51] These databases could be drivers' license photos (state DMV records) or mugshot arrest photos (police-generated photos) or other more informal suspect identification systems (gang databases, jail photographs, intelligence-driven prosecution wikis).[52] In this scenario, police have an identified suspect and want to confirm the identity of the suspect through existing photo datasets.[53]

This type of facial identification process is used by the FBI through local state partners, and in certain states. For example, in a year and a half span between 2017-2019, the FBI conducted 152,500 searches for law enforcement investigation.[54] In New York City, NYPD conducted almost 8000 searches in 2018.[55] The Washington Post reported that one small Oregon police department used commercial software created by Amazon to conduct investigatory searches all sorts of cases.[56] Police in Detroit, Michigan have also admitted to using this type of facial recognition matching to track down violent suspects.[57]

Face identification, as defined here, is limited to static photographs (not video) and used only after a crime has been committed. In the near future, however, this type of database matching could even be during an on-going investigation or even during a police traffic stop. Private companies are already selling the capabilities to do the search on a mobile phone.[58] Especially in a situation involving a suspect unwilling or unable to provide

if Rekognition gets it wrong? WASHINGTON POST (April 30, 2019) https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/?noredirect=on&utm_term=.10b8818b5bea)

[51] James O'Neill, *How Facial Recognition Makes You Safer*, NY TIMES (June 9, 2019) ("When detectives obtain useful video in an investigation, they can provide it to the Facial Identification Section, of the Detective Bureau. An algorithm makes a template of the face, measuring the shapes of features and their relative distances from each other. A database consisting solely of arrest photos is then searched as the sole source of potential candidates.").

[52] Clare Garvie, *Flawed Face Data* (May 2019) https://www.flawedfacedata.com/; Amy Harmon, *As Cameras Track Detroit's Residents, a Debate Ensues Over Racial Bias,* N.Y. Times (July 8, 2019) ("The facial recognition program matches the faces picked up across the city against 50 million driver's license photographs and mug shots contained in a Michigan police database.").

[53] Clare Garvie, *Flawed Face Data* (May 2019) https://www.flawedfacedata.com/.

[54] House Oversight Committee Hearing Testimony, June 4, 2019.

[55] James O'Neill, *How Facial Recognition Makes You Safer*, NY TIMES (June 9, 2019) ("In 2018, detectives made 7,024 requests to the Facial Identification Section, and in 1,851 cases possible matches were returned, leading to 998 arrests.").

[56] Drew Harwell, *Oregon became a testing ground for Amazon's facial-recognition policing. But what if Rekognition gets it wrong?* WASH. POST (April 30, 2019) https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/?noredirect=on&utm_term=.10b8818b5bea).

[57] Amy Harmon, *As Cameras Track Detroit's Residents, a Debate Ensues Over Racial Bias,* N.Y. Times (July 8, 2019) ("Facial recognition, the Detroit police stress, has indeed helped lead to arrests. In late May, for instance, officers ran a video image through facial recognition after survivors of a shooting directed police officers to a gas station equipped with Green Light cameras where they had met with a man now charged with three counts of first-degree murder and two counts of assault. The lead generated by the software matched the description provided by the witnesses.").

[58] *See e.g.,* FaceFirst Technology, https://www.facefirst.com/industry/law-enforcement-face-recognition/

identification, the ability to quickly identify someone by their photo would be useful.

3. Face Tracking

Face tracking is a hybrid between "face surveillance" and "face identification" because it involves the same generalized video facial recognition surveillance technologies, but with particularized suspicion of a specific target. Police are not just passively monitoring for generalized surveillance purposes, but actively investigating a particular crime with an identifiable suspect using facial recognition matching software. As a general matter, police might use "face tracking" in three different ways: (a) scanning stored video footage to identify a targeted face; (b) scanning real-time video feeds to identify a targeted face; and (c) scanning image databases from private third-party platforms to identify a targeted face.

a. Face Tracking: Searching Stored Video Footage

After a crime, police may wish to run a face image they possess against stored video surveillance from a network of city cameras.[59] The same matching technology can be used to search months of stored surveillance footage, networks of video feeds, or growing image databases to compare those images with the target's face.[60] For example, searching stored video footage from a network of cameras could reveal the location of the "target" over time, including time, date, place, and patterns of movement. Depending on the density of cameras, many public movements of the targeted face could be identified and mapped. In addition, because other identifying data about the locations exist, the facial recognition matches could reveal the target's interests, employment, religious preferences, health issues, or legal troubles. Over time, a mosaic of a person's activities would be revealed by the location of the face identified by face tracking.

It is important to recognize that the difference between face surveillance and face tracking when it comes to stored footage is less the *technology* than the *purpose* of why the scan is being conducted. The facial recognition technology is undertaking the same matching process in both, but with a particularized justification for face tracking (looking for one particular face, not identifying all faces). But, as may be evident, the danger of widespread mass surveillance exists with both types, as the line between generalized surveillance and particularized tracking is not always so clear.

[59] Such use of face tracking is not being done currently. Systems in Chicago, Illinois, and Detroit have the capabilities to do this, but have not done it. Clare Garvie & Laura Moy, *America Under Watch* (2019), https://www.americaunderwatch.com/.

[60] *Id.*

b. Face Tracking: Real Time Scans

Networked video systems also create the potential to track suspects in real-time. A networked system of real-time face tracking would be able to provide the specific location of a "wanted" suspect.[61] The "hit" or "match" would alert police to the location of a particular person at a particular time in the city.[62] Of course, once again in order to be able to track that one target, surveillance cameras with the ability to match other faces would be required to be in effect. This same type of matching would also work with single (non-networked) cameras. A single camera or drone with camera could spot a particular person at a particular place based on a face recognition match from a pre-populated dataset.

c. Face Tracking: Private Third-Party Image Scans

Private third-party providers hold massive numbers of face images, all potentially searchable with similar pattern matching technology.[63] Police access to this dataset (via informal request, subpoena, warrant, or purchase) can help identify suspects, groups, and associates.[64] Photos not only provide images and identification, but also locational data from metadata which can reveal where and when the photos were taken.[65] While not as structured, the same type of long-term, aggregated locational information could be revealed in the collected metadata and inferences from the photographs. Police are already monitoring social media for gang violence and threats, so this would just be a slight change in practice.[66]

4. Non-Law Enforcement Purposes

[61] Amy Harmon, *As Cameras Track Detroit's Residents, a Debate Ensues Over Racial Bias,* N.Y. Times (July 8, 2019) ("Although the department has the ability to implement real-time screening of anyone who passes by a camera — as detailed in a recent report by the Georgetown Law Center on Privacy and Technology — there is no plan to use it, he said, except in extraordinary circumstances.") https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html

[62] *Police Unlock AI Potential To Monitor, Surveil, and Solve Crimes*, WSJ Video, https://www.wsj.com/video/police-unlock-ai-potential-to-monitor-surveil-and-solve-crimes/819D5F78-22BC-4A41-9517-AE31BE3C5E7E.html.

[63] The numbers of photographs including a facial image on social media is in the billions as millions of photos are uploaded every day.

[64] James O'Neill, *How Facial Recognition Makes You Safer*, NY TIMES (June 9, 2019) (Police Commissioner of the NYPD, "We might find social media images of a person at a birthday party wearing the same clothing as the suspect in a robbery. That person then becomes a lead.").

[65] How Law Enforcement Decodes your Photos, THE CONVERSATION, (June 22, 2017); http://theconversation.com/explainer-how-law-enforcement-decodes-your-photos-78828

[66] *See e.g.,* Joseph Goldstein & J. David Goodman, *Seeking Clues to Gangs and Crime, Detectives Monitor Internet Rap Videos*, N.Y. Times (Jan. 7, 2014); Ben Austen, *Public Enemies: Social Media Is Fueling Gang Wars in Chicago*, Wired (Sept. 17, 2013).

Police may wish to use face matching for non-law enforcement purposes. Face verification technologies at airports or borders or even to enhance the security of public events may be utilized not for investigatory policing but for public safety purposes.[67] While the line between "security" and policing or public safety is blurred, some non-law enforcement uses can be imagined in high security areas.[68]

In other cases, the public safety interest runs to identifying victims of crime or lost children where police officials are not focused on ordinary law enforcement investigation but emergency response.[69] The limitations here involve the non-law enforcement purpose for which the face surveillance or face recognition technology is used.

These non-law enforcement uses seemingly avoid some of the problems of general face surveillance or investigatory face tracking, but, in fact, raise equally complicated questions. No matter who collects the images or who matches or for what purpose, the systems are being created to allow massive scans of large portions of the population. As a simple point, to find the lost child in the city, the surveillance system needs to be able to identify humans, children, boys, girls, race, face type, and then match the target face to all the others. This mass surveillance capability also exists if the dataset involves Facebook's billions of images. Once society builds the architecture of surveillance that supports non-law enforcement matching, we have by necessity also created the capabilities for police use.

The next section addresses the privacy-invading powers of facial recognition surveillance technology and how the Fourth Amendment might act as a regulatory check on growing police surveillance power. Later, Part III will tackle the equally fundamental questions going to issues of police legitimacy like fairness, bias, accuracy, and opacity.

II. The Fourth Amendment and the Privacy Problem of Facial Recognition

How does the Fourth Amendment fit the puzzle of facial recognition technology? It is not an easy answer because the Fourth Amendment has largely ignored pre-investigatory surveillance techniques[70] and failed to

[67] Jagdish Chandra Joshi and K K Gupta, *Face Recognition Technology: A Review*, 1 The IUP Journal of Telecommunications, 53, 58 (2016)

[68] Jon Schuppe, *Secret Service Tests Facial Recognition Surveillance System outside White House*, NBCNews, (Dec. 4, 2018) https://www.nbcnews.com/news/us-news/secret-service-tests-facial-recognition-surveillance-system-outside-white-house-n943536

[69] All Things Considered, *ICE Turned To DMV Driver's License Databases For Help With Facial Recognition,* NPR (July 8, 2019) ("[I]t is important to point out facial recognition has done plenty of good in this world. It's helped find missing children and reunite with them with their families.").

[70] Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 Harv. L. & Pol'y Rev. 15, 33 (2016).

regulate information seemingly exposed to the public.[71] But a new understanding of policing as more programmatic and systemic has shifted recent thinking about this traditional view,[72] and powerful new surveillance capabilities may force the Supreme Court to rethink its traditional Fourth Amendment approach.

This Part begins with a brief background on the Supreme Court's approach to the Fourth Amendment before the digital age, and then explores how this approach has had to adapt to new digital surveillance threats. The argument set forth is that certain "future proofing" principles can be divined from recent Supreme Court decisions which open up a new theory about how technologies like facial recognition should be analyzed under the Fourth Amendment. To be clear, this is my attempt to make sense of a muddled doctrinal landscape with a new interpretive theory.

As will be detailed, however, any global Fourth Amendment conclusion remains largely unsettled and likely dependent on which use of the technology we focus on (surveillance, identification, tracking, or non-law enforcement purposes) and whether the Supreme Court's recent privacy-conscious decisions about digital surveillance will be extended to cover facial recognition technology. These gaps will guide the legislative response proposed in Part IV.

A. Pre-Digital Face Searches

Under a traditional Fourth Amendment analysis, a court would ask whether the surveillance technology at issue violates a reasonable expectation of privacy.[73] This constitutional standard comes from the Supreme Court's interpretation of the Fourth Amendment in *Katz v. United States*.[74] If the technology violates a reasonable expectation of privacy, the government action would be a "search" and without a warrant or exception to the warrant requirement the search would be deemed unconstitutional.[75] While strange to think about today, the facts of *Katz* also involved new technology, although in 1967 that new technology was a wiretap of a public, free-standing telephone booth.[76] The Supreme Court held that the electronic interception of Charlie Katz's conversation violated a reasonable expectation of privacy

[71] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 566 (2009).

[72] Daphna Renan, *The Fourth Amendment As Administrative Governance*, 68 STAN. L. REV. 1039, 1041 (2016); Christopher Slobogin, *Policing As Administration*, 165 U. PA. L. REV. 91, 97 (2016); Tracey L. Meares, *Programming Errors: Understanding the Constitutionality of Stop-and-Frisk as a Program, Not an Incident,* 82 U. CHI. L. REV. 159, 162 (2015).

[73] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

[74] *Id*.

[75] *Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there 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.'").

[76] *Id*. at 360–61 (Harlan, J., concurring).

and thus the Fourth Amendment.[77]

Under a pre-digital, traditional Fourth Amendment analysis, human observation of a face or manual photo matching likely would not violate a reasonable expectation of privacy. In 1973, the Supreme Court stated: "Like a man's facial characteristics, or handwriting, his voice is repeatedly produced for others to hear. No person can have a reasonable expectation that others will not know the sound of his voice, *any more than he can reasonably expect that his face will be a mystery to the world*."[78] This understanding has largely prevailed in the context of human observation of human faces. As a result, one traditional way of looking at the Fourth Amendment doctrine would be to assert that it offers little protection to faces in public, no protection from digital collection of face images, and no protection from subsequent searches of those face images.

Even more fundamentally, as a practical matter the Fourth Amendment would have little application without a person harmed. Most Fourth Amendment cases arise in the criminal context through a suppression hearing, so general challenges to generalized police powers are non-justiciable due to a lack of standing.[79] Large scale surveillance systems have always created a difficult puzzle for standing determinations.[80] While facial challenges to statutes are permissible,[81] and systems of Fourth Amendment violations have been litigated under civil rights law,[82] establishing concrete harm and getting those privacy claims before a court is not as easy.

Such a pre-digital understanding of a reasonable expectation of privacy in public, however, has undergone some rethinking in recent years as the Supreme Court has begun addressing the threat of new digital technologies to public activity. Legal commentators have recognized that when it comes to new digital surveillance technologies "digital is different" for Fourth Amendment purposes.[83] In addition, if interpreted broadly, the

[77] *Id.* at 360 (Harlan, J., concurring). Notably, this development spurred Congress to pass the Wiretap Act to regulate government use of new surveillance technology involving communications. This connection has not been missed by Supreme Court Justices who have relied on this parallel to encourage congressional action on other new surveillance innovations *Jones,* 565 U.S. at 427–28 (Alito, J. concurring) ("On the other hand, concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping. After *Katz,* Congress did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. Instead, Congress promptly enacted a comprehensive statute, see 18 U.S.C. §§ 2510–2522 (2006 ed. and Supp. IV), and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law.").

[78] *US v. Dionisio* , 410 US 1 (1973) (emphasis added).

[79] *Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 411 (2013) (denying standing for a lawsuit challenging mass surveillance under FISA); *see also* Christopher Slobogin, *Standing and Covert Surveillance,* 42 PEPP. L. REV. 517, 530 (2015).

[80] Stephen I. Vladeck, *Standing and Secret Surveillance*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 551, 575 (2014).

[81] *City of Los Angeles, Calif. v. Patel*, 135 S. Ct. 2443, 2449 (2015) ("We first clarify that facial challenges under the Fourth Amendment are not categorically barred or especially disfavored.").

[82] *Floyd v. City of New York,* 959 F. Supp. 2d 540, 558 (S.D.N.Y. 2013).

[83] Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras),* 18 U. PA. J. CONST. L. 933, 951 (2016) ("So, while *Riley* perhaps left things unanswered that it could have addressed, it made very clear that when it comes to the Fourth Amendment, digital is different."); Orin S. Kerr,

Supreme Court's analysis about particular cases may have application to generalized surveillance systems. Such an interpretation provides the analytical foundation to develop a future-proofing theory for future Fourth Amendment cases. This theory is the subject of the next section.

B. Future-Proofing the Fourth Amendment: A Theory[84]

To understand how the Supreme Court might resolve the puzzle of facial recognition surveillance, it is useful to study three recent Supreme Court decisions on new digital technologies.[85] These privacy-protective cases help frame the analysis because they recognize the privacy and liberty threat from technology-enhanced police surveillance as distinct from traditional police surveillance. Importantly, these cases also appear to be addressing more than just the particular defendant's case at issue, raising concerns with how new technologies impact everyone's privacy interests.

First, in *United States v. Jones*, the majority of the Supreme Court held that placing a GPS tracking device on a suspect's car was a search for Fourth Amendment purposes because the physical act of attaching the tracking device with the intent to gain information was a "trespass" which violated the constitutional rights of the driver.[86] More importantly for our analytical purposes, five justices concurred in the outcome, reasoning that the long-term (28 days) GPS location tracking of the car in public for a drug-related crime violated a reasonable expectation of privacy and thus was a "search" for Fourth Amendment purposes.[87] These concurring justices were concerned with the private details revealed by long term tracking in terms of habits, interests, associations, and the freedom to move without government monitoring.[88] In two overlapping concurring opinions, the Supreme Court drew a line at the government's ability to monitor individuals in public for weeks at a time. This understanding about locational privacy in public was reaffirmed in *Carpenter v. United States*.[89]

Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data, 48 TEX. TECH L. REV. 1, 27 (2015); *see also* Jennifer Granick, *SCOTUS & Cell Phone Searches: Digital Is Different*, JUSTSECURITY (June 25, 2014), https://www.justsecurity.org/12219/scotus-cell-phone-searches-digital [http://perma.cc/94RH-42EV].

[84] Andrew Guthrie Ferguson, *Future Proofing the Fourth Amendment*, Harvard Law Review Blog, (June 25, 2018) https://blog.harvardlawreview.org/future-proofing-the-fourth-amendment/; *see generally Carpenter*, 138 S. Ct. at 2218 ("[T]he rule the Court adopts "must take account of more sophisticated systems that are already in use or in development.").

[85] Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 216 (2018); Margaret Hu, *Cybersurveillance Intrusions and an Evolving Katz Privacy Test*, 55 AM. CRIM. L. REV. 127, 132 (2018).

[86] *See Jones*, 132 S. Ct. at 949–52.

[87] *See id.* at 955–56 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring). Chief Justice Roberts in *Carpenter* confirmed this consensus positively referencing the five justices who accepted the reasonable expectation of privacy protection of *Jones'* GPS data. *Carpenter*, 138 S. Ct. at 2215, 2217 (2018).

[88] *Id.*

[89] *Carpenter*, 138 S. Ct. at 2217 ("A majority of this Court has already recognized that individuals have a

In *Carpenter*, the Supreme Court held that police typically need a probable cause warrant to acquire digital cell-site location records (CSLI) held by third party cell phone service providers.[90] Timothy Carpenter was suspected of robbing a series of electronics stores and police sought access to his cell phone location data to link him to the crimes.[91] Using a court order authorized under the Stored Communication Act, police obtained seven days of his cell site location data.[92] This information provided police with a virtual map of his whereabouts that corresponded with his presence during the robberies. Carpenter filed a motion to suppress the third-party cell-site records, arguing that their acquisition was a search under the Fourth Amendment and unconstitutional without a probable cause search warrant.[93] The Supreme Court agreed with Carpenter holding that the acquisition of the data without a probable cause search warrant violated a reasonable expectation of privacy.[94] Chief Justice Roberts summarized the holding stating, "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."[95] The focus on "depth," "breadth," scope and scale makes it clear that the Court is concerned with systems of digital surveillance.[96] The reasoning again turned on the voluminous and personal nature of the locational data being sought by police without a warrant.

Finally, in *Riley v. California*, the Court held that police must obtain a warrant before searching a suspect's smartphone incident to arrest.[97] The Court reasoned that sensitive data[98] in modern smartphones revealed too many of the "privacies of life" not to require a probable cause warrant before acquiring the information.[99] In *Riley*, the Court emphasized the quantitative and qualitative realities of digital evidence as different enough to warrant a different Fourth Amendment approach from past rules for non-digital physical evidence.[100] The quantitative difference involves the "immense

reasonable expectation of privacy in the whole of their physical movements.") (citing *Jones*).

[90] *Id.* at 2221 ("Having found that the acquisition of Carpenter's CSLI was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records.").

[91] Stephen E. Henderson, *Carpenter v. United States and the Fourth Amendment: The Best Way Forward*, 26 WM. & MARY BILL RTS. J. 495, 497 (2017).

[92] *Carpenter*, 138 S. Ct. at 2212.

[93] *Id.*

[94] *Id.* at 2217.

[95] *Id.* at 2223.

[96] Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. (forthcoming 2019), https://osf.io/preprints/lawarxiv/bsedj [https://perma.cc/2EFF-UGJ3].

[97] 134 S. Ct. 2473, 2480 (2014).

[98] *See e.g.*, Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1133 (2015).

[99] *Riley*, 134 S. Ct. at 2495 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

[100] *Id.* at 2489 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. 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

storage capacity" which can in a very small space collect and maintain an almost infinite amount of personal data.[101] In addition, the nature and scope of digital information reveals much more qualitative information than citizens normally share with anyone else.[102]

These three cases signify the emergence of a digitally-aware Fourth Amendment and a Supreme Court cognizant of the limitations of applying analog precedent to a digital reality. One can also intuit a new awareness of systems of mass surveillance as a distinct concern not traditionally acknowledged in Fourth Amendment cases. The Court is not just talking about a particular defendant's rights *vis a vis* surveillance technologies, but everyone's rights. Such a digitally aware Fourth Amendment would, of course, apply to the question of mass deployment of facial recognition.

The next six subsections identify what I am calling the future-proofing principles helpful to analyze new surveillance technologies. Some of these principles are decidedly new, and some can trace their roots back to first principles, but combined, these principles help structure a rather disordered Fourth Amendment doctrine. The final subsection will then apply this future-proofing theory to the problem of facial recognition technology. The goal is to draw out common principles that underlie the Court's recent decisions to build an analytical framework to analyze future surveillance technologies.

1. Anti-Equivalence Principle

The Supreme Court's recent cases involving police surveillance have caused a reexamination of existing precedent crafted in a pre-technological age.[103] In its recent technological-enhanced surveillance cases, the Supreme Court has recognized that digital police capabilities are simply not the equivalent of traditional analog policing methods.[104]

In *Carpenter*, Chief Justice Roberts acknowledged that "a mechanical interpretation" of the third-party doctrine failed to account for the type of information now being collected by police through third parties.[105] He said

called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

[101] *Id.* at 2489 ("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.").

[102] *Id.*

[103] Such an awareness of technological dangers is not necessarily new, as the Supreme Court has recognized mass surveillance concerns in older beeper tracking cases like *Knotts,* and one can even trace the technological fear back to Justice Brandeis' 1928 *Olmstead* dissent that the Court must be aware of "[s]ubtler and more far-reaching means of invading privacy [which] have become available to the Government"—to ensure that the "progress of science" does not erode Fourth Amendment protections. *Olmstead v. United States,* 277 U.S. 438, 473–474 (1928).

[104] *See supra* note 77.

[105] *Carpenter,* 138 S. Ct. at 2210 ("There is a world of difference between the limited types of personal

the same thing in *Riley* when comparing digital smart objects recovered incident to arrest and traditional physical objects recovered incident to arrest.[106] Justice Alito also recognized this truth in *Jones* when discussing the ease with which police could track automobiles in ways that would simply be impossibly difficult with human power.[107] In this way, the Court has been conscious of future-proofing its holdings.[108] In both *Kyllo*[109] and *Carpenter*,[110] the Court explicitly acknowledged that its decision was not limited to the technology of the particular case, but also meant to foresee the technology of the future. In tackling these surveillance cases, the Court has tried to maintain a balance between growing government power and shrinking personal liberty,[111] recognizing that Fourth Amendment principles are directly threatened by new surveillance technologies in ways that were not threatened by existing analog counterparts.[112]

This "digital is different" theme is an important framing change for facial recognition analysis because it recognizes that merely applying analog precedents to digital challenges does not maintain the status quo but significantly enhances police power at the expense of personal liberty.[113] It is no longer an answer to say "well police could have just done it without technology" so the surveillance technique is constitutional. Now, the Court has signaled that new technology requires new and arguably more protective constitutional analysis, especially where the amount of information available is quantifiably and qualitatively different.

But to say "digital is different" does not provide the contours of how the Supreme Court might evaluate digital surveillance technologies like facial recognition. The next few subsections examine the principles underlying the Courts recent decisions looking at the concerns with data aggregation, data

information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.").

[106] *Riley*, 134 S.Ct., at 2485 ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered [in prior precedents]."); s*ee also Carpenter*, 2018 WL 3073916, at *6 ("[W]e rejected in *Kyllo* a "mechanical interpretation" of the Fourth Amendment and held that use of a thermal imager to detect heat radiating from the side of the defendant's home was a search.).

[107] *Jones*, 565 U.S. at 415 (Sotomayor, J. concurring).

[108] Andrew Guthrie Ferguson, *Future Proofing the Fourth Amendment*, Harvard Law Review Blog, (June 25, 2018) https://blog.harvardlawreview.org/future-proofing-the-fourth-amendment/.

[109] *Kyllo v. United States*, 533 U.S. 27, 36 (2001) ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.")

[110] *Carpenter*, 138 S. Ct. at 2218 ("[T]he rule the Court adopts "must take account of more sophisticated systems that are already in use or in development.").

[111] Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 479 (2011).

[112] *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)) ("We have kept this attention to Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools. As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to "assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.").

[113] *Carpenter*, 138 S. Ct. at 2219 ("The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.").

permanence, long-term tracking, arbitrary monitoring, and the permeation of surveillance technologies.

2. Anti-Aggregation Principle

Underlying *Jones* and *Carpenter* is a particular privacy harm that occurs when police can aggregate personal data. Whereas one fact revealed about a person might not infringe on a reasonable expectation of privacy, the long-term aggregated collection of many of those same facts will be seen as a cognizable Fourth Amendment harm.[114] Both Justice Sotomayor and Justice Alito in *Jones* separately articulated the consequences of large-scale public data collection on individual liberty.[115] The principle was reaffirmed in *Carpenter* when the Court drew a clear line from *Jones* to the privacy-invading nature of aggregated cell-site tracking.[116] The same theme can even be observed in *Riley* with private smartphone data, when Chief Justice Roberts acknowledged how the sum of data collection can reveal more than the individual parts.[117] In a remarkable admission of the changing world, Chief Justice Roberts conceded that the aggregated information in a smartphone is probably more revealing and more privacy invading than the contents of our homes – traditionally the most protected of constitutional spaces.[118] In each of these cases, the Court found the mosaic of aggregated personal data collection a Fourth Amendment concern.

A city-wide web of digital cameras using face surveillance creates aggregation problems. If networked or searchable the locational privacy of an individual in a city will be at risk. As will be discussed later, this type of surveillance system may be just as revealing as GPS tracking or cell-cite tracking.

[114] *See generally*, Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1139 (2002).

[115] *See id.* at 955–56 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).

[116] *Carpenter*, 138 S. Ct. at 2225.

[117] *Riley*, 134 S.Ct., at 2489 ("The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.").

[118] *Id.* at 2491 ("Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.").

3. Anti-Permanence Principle

The anti-permanence principle involves not just the collection of data but the long-term storage and retrievability of that information. The Court in both *Jones* and *Carpenter* expressed concern about the government's ability to revisit that information for any reason and for all time.[119] This "time-machine" like capability to access permanently stored data acknowledged a fear about the creation of overbroad and unlimited data systems which allow for retrospective searching.[120] As the Court stated in *Carpenter*:

> Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers, which currently maintain records for up to five years.[121]

This retrospective power of collected data points offers guidance about the creation of any digital system that collects personal information to be used by police for investigative purposes. Just as *Riley* warned against collecting a trove of data about our intellectual or informational interests, and cell-site locations expose a similarly revealing dataset about the paths of all cell phone users, so would the ability to mine networked surveillance footage using facial recognition techniques.[122]

4. Anti-Tracking Principle

The Supreme Court in *Jones* and *Carpenter* was explicit in its concern about the locational tracking capabilities of new surveillance technologies. *Jones* was literally a case about GPS tracking[123] and *Carpenter* a case about a network of tracking capabilities.[124] The *Jones* Court expressed concern about the associational freedoms impacted, and the revealing nature of the tracking technology:

[119] *Jones*, 565 U.S. at 415 (Sotomayor, J. concurring) ("The Government can store such records and efficiently mine them for information years into the future."); *Carpenter*, 138 S. Ct. at 2218 ("With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers, which currently maintain records for up to five years.")

[120] Stephen E. Henderson, *Fourth Amendment Time Machines (And What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 939 (2016).

[121] *Carpenter,* 138 S. Ct. at 2218.

[122] *Id*.

[123] *Jones*, 565 U.S. at 403.

[124] *Carpenter* 128 S. Ct. at 2216.

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may alter the relationship between citizen and government in a way that is inimical to democratic society.[125]

The five concurring Justices' determination that long-term aggregated tracking was a Fourth Amendment search arose directly from the concrete harm of revealing locational data and the personal inferences derived from that information.[126] Similarly, Chief Justice Roberts in *Carpenter* recognized how the tracking capabilities of cellphones dwarfed the capabilities of GPS tracking,[127] allowing an "all-encompassing record of the holder's whereabouts"[128] and creating a much graver threat to personal privacy.[129] The Court has been adamant that locational data should receive some Fourth Amendment protection when threatened by tracking technologies.[130] Similarly, the intellectual tracking of ideas – as made manifest by the informational choices in our smartphone – also deserves protection under *Riley*. As facial recognition can track and identify location and generate inferences from private locational details the same privacy concerns arise.

5. Anti-Arbitrariness Principle

[125] *Jones*, 565 U.S. at 416 (Sotomayor, J. concurring)

[126] *Id.* (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."); *Id.* at 430 (Alito J., concurring) ("Society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4–week mark.").

[127] *Carpenter*, 138 S. Ct. at 2216 ("The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring we considered in *Jones*. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.").

[128] *Id.* at 2217 ("As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations.").

[129] *Carpenter*, 138 S. Ct. at 2217-18 ("In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*.").

[130] *Id. See also* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); David Gray, *A Collective Right to Be Secure from Unreasonable Tracking*, 48 TEX. TECH. L. REV. 189 (2015); Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527 (2017).

A related theme in the cases involved the desire to prevent arbitrary police actions. In *Carpenter*, Chief Justice John Roberts stated quite simply: "The "basic purpose of [the Fourth] Amendment," our cases have recognized, "is to safeguard the privacy and security of individuals against *arbitrary* invasions by governmental officials."[131]

This is, of course, the central principle animating much of constitutional criminal procedure involving checks to government power.[132] The Fourth Amendment's textual emphasis on warrants, probable cause, particularity, oaths, and other formalities speak to a concern about unconstrained, arbitrary government authority.[133] But specific emphasis on arbitrariness echoed Justice Sonia Sotomayor's concurrence in *Jones* where she stated equally plainly, "the Fourth Amendment's goal [is] to curb *arbitrary* exercises of police power."[134]

In both the context of cell-site locational tracking and GPS tracking the Court began with a focus on the arbitrariness of government agents gaining access to private information without a warrant. Again, from *Carpenter*:

> Although no single rubric definitively resolves which expectations of privacy are entitled to protection, the analysis is informed by historical understandings "of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted." On this score, our cases have recognized some basic guideposts. First, that the Amendment seeks to secure "the privacies of life" against "*arbitrary* power.[135]

This fear of arbitrary government power arose directly from a historical experience which amply demonstrated how unconstrained governmental police power could negatively impact liberty.[136] In the pre-revolutionary war colonies, arbitrary invasions directly interfered with private behavior,

[131] *Id.* at 2213.

[132] Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1326 (2002) (arguing that the Fourth Amendment is really about "power not privacy"); *see e.g., Fla. v. Riley*, 488 U.S. 445, 462 (1989) ("The basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."); *I.N.S. v. Delgado*, 466 U.S. 210, 215 (1984) ("The Fourth Amendment does not proscribe all contact between the police and citizens, but is designed "to prevent arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals.").

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

[134] *Jones*, 565 U.S. at 416–17 (Sotomayor, J. concurring).

[135] *Carpenter,* 2018 WL 3073916, at *6.

[136] Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 309 (1998) ("The Fourth Amendment was a creature of the eighteenth century's strong concern for the protection of real and personal property rights against arbitrary and general searches and seizures.").

manifesting both as physical home invasions and indirect government surveillance.[137]

In our modern times, facial recognition technology gives police the power to conduct arbitrary digital searches of its citizens. Governments can run pattern matching searches for any face. They can target surveillance in particular places or to find particular people. The power is arguably far broader than a general warrant. Instead of having a constable empowered to find out revealing information, you have an entire city designed to expose the people in it.

6. Anti-Permeating Surveillance Principle

Finally, the Court in both *Carpenter* and *Jones* addressed the Fourth Amendment's foundational role in restricting invasive police surveillance.[138] In *Carpenter* the Court stated: "a central aim of the Framers was "to place obstacles in the way of a too permeating police surveillance."[139] In *Jones*, Justice Sotomayor made an even more direct reference to overbroad police power recognizing, "the Fourth Amendment's goal to … prevent "a too permeating police surveillance."[140]

Admittedly, the "too permeating" language is both vague and oddly unhelpful in a world of growing omnipresent surveillance. But the term may well have been chosen to respond to the growing sense that new digital technologies threaten to expose and undermine privacy in a whole host of areas. Both *Carpenter* and *Jones* have been interpreted to be less about deciding the particular cases involving particular technologies, and more about signaling that all new surveillance technologies will require greater scrutiny. In addition, the term reflects a long-standing constitutional concern with growing surveillance capacities which links back to a colonial history of invasive government practices which undermined personal liberty and security.[141]

Interestingly, while the Court did not define "too permeating" the concept shifts the focus to a systems analysis. The idea evokes concerns with scope and scale, and the larger *Carpenter* emphasis on depth, breadth, and comprehensive monitoring. It is a concept that only makes sense when

[137] *See e.g.,* United States v. Ortiz, 422 U.S. 891, 895 (1975) ("[T]he central concern of the Fourth Amendment is to protect liberty and privacy from arbitrary and oppressive interference by government officials."); Schneckloth v. Bustamonte, 412 U.S. 218, 242 (1973) ("[T]he Fourth Amendment protects the 'security of one's privacy against arbitrary intrusion by the police."').

[138] Tracey Maclin, *When the Cure for the Fourth Amendment Is Worse Than the Disease,* 68 S. CAL. L. REV. 1, 25 (1994) ("The warrant preference rule is a twentieth-century construction of the Fourth Amendment that is designed to restrain the discretion of police power -- a relevant concern today as it was in 1791.").

[139] *Carpenter,* 138 S. Ct. at 2214.

[140] *Jones*, 565 U.S. at 416–17 (Sotomayor, J. concurring).

[141] Timothy Williams, *Can 30,000 Cameras Help Solve Chicago's Crime Problem*, N.Y. TIMES (May 2, 2018). Chicago police have the capabilities to use facial recognition software, but have not used it.

talking about systems of tracking technologies and the privacy threat that emerges from overreaching monitoring capabilities.

7. Systems of Surveillance

These six principles suggest a way to analyze some developing *systems* of digital surveillance, although they leave others unprotected. The working theory is that the more a system of surveillance violates these principles the more likely it will be seen as violating a reasonable expectation of privacy and be struck down by the Supreme Court on Fourth Amendment grounds.

Equally important, the Court seems to be concerned with the collective harm of surveillance not just the collection of data about a particular suspect.[142] The language chosen in *Carpenter* is about how a system of surveillance could impact everyone, not just Mr. Carpenter. The underlying argument being that if police cannot conduct surveillance *with individualized suspicion* against a particular person without a warrant, then police certainly cannot conduct generalized surveillance *without individualized suspicion* on almost everyone.

Thus, to study the problem of facial recognition, we should look at issues of aggregation, permanence, locational tracking, arbitrariness, and pervasive surveillance through a "digital is different" lens. The next section attempts to apply these future-proofing principles to the various ways police might use facial recognition technology.

C. Analysis: How the Fourth Amendment Fits Facial Recognition Surveillance Technology

This section examines the main types of facial recognition surveillance technology available to police. As will be observed, the Fourth Amendment question depends on how the future-proofing principles of (1) anti-equivalence; (2) anti-aggregation, (3) anti-permanence, (4) anti-tracking, (5) anti-arbitrariness, and (6) anti-permeating surveillance are balanced. The Fourth Amendment may provide a different level of protection from different types of facial recognition technology. Even more importantly this analysis reveals the constitutional gaps in coverage requiring legislative action which will be discussed in Part IV.

1. Face Surveillance

[142] David Gray, *A Collective Right to Be Secure from Unreasonable Tracking*, 48 TEX. TECH. L. REV. 189 (2015).

How does the Fourth Amendment apply to generalized face surveillance? Again, face surveillance is the scenario involving suspicion-less, mass surveillance of all people in a public area or using a third party records image set.[143] As an example, imagine police wish to identify everyone walking on a public street or appearing in an image on a third party social network like Facebook for the purposes information gathering (not criminal investigation). Applying the future proofing principles articulated in Part II.B to the problem of face surveillance all of the principles point to this type of generalized surveillance (identifying everyone, everywhere, for all time) being a search for Fourth Amendment purposes.

The first question to ask is whether digital, networked surveillance cameras with facial recognition should be considered the equivalent of ordinary security cameras. The Supreme Court in *Carpenter* made clear that the opinion did not cover "conventional surveillance techniques and tools, such as security cameras."[144]

The anti-equivalence principle suggests, however, that facial recognition technology is not a conventional surveillance tool because of the qualitative and quantitative differences between traditional security cameras and networked systems of identification utilizing facial recognition software. The overlay of facial recognition software and the scope and scale of digital networks are just too different to equate. In terms of scope, generalized surveillance is troubling because everyone observed becomes a target. If you think about it, in order to identify every person on a street, police would need to match those people with some identified list (which for surveillance purposes could be potentially everyone). Scale is also a problem depending on the datasets the targets are matched against. Public spaces or third-party social networks of images provide a vast search field for potential matches. All stored video footage kept for months or all images in a third-party social network over the years would provide a scale of potential matches that covers millions of people. This type of overbroad matching seems to cut against the Fourth Amendment's preference for particularized, individualized suspicion.

Escaping the equivalence trap, allows us to distinguish face surveillance from the analog tradition of officers taking photos on the street or watching fixed camera feeds. The difference is the matter of scope, scale, detail, personal data, locational data, and retrieval capabilities at play. Further, the other principles regarding aggregation, tracking, and permanence suggest that this type of on-going constant monitoring system would be a Fourth Amendment search, although the analysis for stored footage and real time images is slightly different.

[143] *See supra* part xx.

[144] *Carpenter*, 138 S. Ct. at 2210.

i. Face Surveillance: Stored Footage

The power of face surveillance is that it allows police to scan through stored footage and track individuals by their face, aggregate their movements, interests, and patterns, and store and study these pathways for long periods of time (all without individualized suspicion).[145] In terms of applying the future-proofing principles, the anti-tracking, anti-aggregation, and anti-permanence principles all apply, suggesting it would be considered the type of system of surveillance that would be of Fourth Amendment concern.

After all, the surveillance would be directed against everyone in public creating a pervasive sense of police power that could be arbitrarily used or abused. If the Supreme Court was concerned with tracking a single car (*Jones*)[146] or a single cell-phone (*Carpenter*),[147] the idea of tracking everyone without a warrant should also raise constitutional concerns. Certainly, for a system that routinely scanned the faces and identified everyone in public or allowed for searching stored data, the problem would raise constitutional red-flags.

Perhaps even more fundamentally, the operative limiting terms of the Fourth Amendment "probable cause" and "warrants" makes little sense in a world of generalized surveillance.[148] With generalized surveillance there is no cause at all. There can certainly be no probable cause warrant predicate for generalized surveillance of everyone. The lack of a limiting principle and the overbroad nature of suspicionless surveillance highlights the unreasonable nature of this type of surveillance.

While there exist real issues of standing to challenge face surveillance under traditional Fourth Amendment law, one can imagine that a surveillance system that identified and tracked everyone in a city environment would be challenged under section 1983 civil rights law, or as a facial matter, or could be litigated if a criminal defendant was stopped based on the technology. Such a threat to public privacy would find objection under the principles suggested in *Jones* and *Carpenter,* and would likely be the target of litigation.

ii. Face Surveillance: Real-Time

In the context of generalized face surveillance, real-time scans to identify individuals face a similar Fourth Amendment infirmity. A city-wide system could flag every time an identifiable face appears on the screen. This

[145] *See supra* note xx.

[146] *Jones*, 565 U.S. at 403.

[147] *Carpenter* 128 S. Ct. at 2216.

[148] Barry Friedman, UNWARRANTED: POLICING WITHOUT PERMISSION, 143-84 (2017); Barry Friedman, Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 299 (2016).

would result in an equivalent tracking system, marking where people are located, what they are doing, and when. While a real-time system would only provide a snapshot of localized presence, the data could be stored and be searchable (raising the stored footage issue). Equally importantly, the system itself "runs against everyone" and creates a similar warrantless dragnet. The future proofing principles point to a Fourth Amendment search problem, as the system can aggregate personal location data, can track individuals, and is permanent, pervasive, and arbitrary.

At the same time, the real-time nature of the collection might mitigate some of the Fourth Amendment harms. Real-time scans involve broad mass collection of information, but not deep or aggregated data collection. If the system did not save the collected data, the retrospective harm principle might not apply. Similarly, if the system did not track, but just identified a particular person at a particular point in time, the tracking and aggregation principles might be less important. Under a *Carpenter* analysis, one might imagine that the Supreme Court would allow real-time scans in certain locations, under certain circumstances (special events, targeted locations), although generalized use for suspicionless surveillance would run afoul of Fourth Amendment search principles.

This distinction is important for showing the gaps in Fourth Amendment coverage. The Court in *Carpenter* emphasized the "depth, breadth, and comprehensive reach"[149] of CSLI data, leaving open the question of what happens when surveillance is broad but not deep or comprehensive.[150] This gap may need to be addressed by legislation as the Court's Fourth Amendment cases leave the question open.

iii. Face Surveillance: Third Party Records

Generalized use of datamining techniques to scan face images acquired from third party datasets presents a related but different problem. Again, this is a situation where the scans are without suspicion and simply for monitoring purposes. First, the fact that the images are held by third parties does not change the Fourth Amendment analysis. The Supreme Court in *Carpenter* held that the Fourth Amendment applies to government acquisition of private third party records that people have a reasonable expectation of privacy over.[151] While there may be an open question about whether images that individuals post in public deserve any Fourth Amendment protection, the scans here would go beyond individual public posting and include the hundreds of millions of photos available as well as

[149] *Carpenter*, 138 S. Ct. at 2223.

[150] Thank you to Andrew Selbst for providing the insight about how *Carpenter* forces a conversation about broad versus deep surveillance technologies.

[151] *Carpenter*, 138 S. Ct. at 2220.

the accompanying metadata (revealing location, time, etc.) which is not generally thought to be publicly shared. All of the future-proofing principles apply to generalized suspicionless face surveillance of third party images. The images will reveal a great deal of information about associational connections, location, will offer a permanent search capability, and is largely an arbitrary use of government power to monitor all (or almost all) individuals with images in these datasets.[152] The quantity and quality of data shared is simply beyond what could ever have been found before raising similar fears to the *Riley* case.[153]

Two issues complicate the third-party records surveillance problem: the first is standing to challenge surveillance technologies, and the second is current practice. As discussed earlier, bringing a Fourth Amendment claim to challenge mass surveillance has proved difficult because the harm alleged is not easily justiciable. If the FBI decided to search all Facebook accounts for a particular gang sign and then used facial recognition to identify all of the people posing with that gang sign (building a dossier of gang members), it is not clear how one could bring a Fourth Amendment claim against this form of surveillance. In a criminal prosecution, the use of facial recognition software could be litigated if police acquired private records from a third party without a warrant, but in the general surveillance situation, it is not clear how the case would arise. That said, unlike the standing problem in *Clapper*,[154] there at least would be a digital trail linking the government action to a particular person (or group of persons), so proving the Fourth Amendment harm would be easier. A plaintiff could argue that the search was conducted, even if defining the individual Fourth Amendment harm remains difficult.

The second issue is that this practice of looking through social media images (without using facial recognition) is done regularly by law enforcement.[155] Because no Fourth Amendment case has challenged the practice of viewing non-private images and because there are no clear laws on the subject, this type of monitoring (at least through posted images) is a routine practice. The open question is whether overlaying a facial recognition search program on top of the regular practice changes things for Fourth Amendment purposes.

[152] *See supra* note xx.

[153] *Riley*, 134 S. Ct. at 2489 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be carried on an arrestee's person.").

[154] *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 411 (2013).

[155] Megan Behrman, *When Gangs Go Viral: Using Social Media and Surveillance Cameras to Enhance Gang Databases*, 29 HARV. J.L. & TECH. 315, 317 (2015).

2. Face Identification

On the other end of the Fourth Amendment spectrum is face identification, involving the matching of digital faceprints. Two types of facial recognition scans should be distinguished based on the type of dataset to be matched. One type of image database consists of police generated images (arrest photos, jail photos, police-generated suspect photos).[156] Another consists of larger government image databases like driver's license photos or passport photos that include a large majority of the population.[157] While the two datasets raise different privacy concerns (because of the source and scale of the datasets), they share a similar Fourth Amendment analysis.

First, as a general matter, there does not appear to be a strong claim that photographs taken by police or the government infringe on an expectation of privacy. Second, in terms of the future proofing principles, the Supreme Court's concerns are not directly implicated, thus leading to the conclusion that these are likely not Fourth Amendment searches. A facial recognition photo image match would reveal identity, but not necessarily location, tracking history, or aggregated private details. In addition, assuming there is some predicate level of suspicion (or internal police policy), the scan will not be arbitrary, and with some control over the use, the scan will not be a form of pervasive surveillance. Especially when using already created police-generated photographs (as opposed to DMV photos), there is little privacy claim to be made under the new digital is different cases. Under existing doctrine, it is unlikely that the Supreme Court would find a Fourth Amendment harm under this analysis.

As face identification is the most common use of facial recognition technology, the lack of Fourth Amendment oversight raises concerns. Under current doctrine there is no constitutional check on the use of the technology, allowing police to use it at will without legal process. There is also no current legislation on police use of the technology, raising the question of whether the gap should be filled with some form of legislation.

3. Face Tracking

Face tracking presents a harder Fourth Amendment analysis, but perhaps one of the most important. The potential to scan vast stores of stored video footage or image databases to find wanted suspects is quite attractive for law enforcement.[158]

[156] Jon Schuppe, *How Facial Recognition became a Routine Policing Tool in America*, NBCNews (May 11, 2019) https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251

[157] Clare Garvie & Laura Moy, *America Under Watch* (2019), https://www.americaunderwatch.com/.

[158] *See supra* note xx.

Because stored video exists from fixed city cameras, mobile body cameras, and private security cameras, the ability to search through a city's worth of images to identify the human needle in the digital haystack is seen as a game-changing power. In addition, the ability to match target face images with the accumulation of stored face images in third party social networks means that many more people can be identified for criminal prosecution.

Again, targeted tracking is distinguishable from generalized surveillance because police are seeking to find a particular person, not all people. Further, there is the predicate of alleged criminal activity that justifies the law enforcement action. For example, imagine that police wish to use an automated on-going facial recognition system to locate a "wanted" face in *stored* surveillance footage from a major city. The facial recognition system could be programmed to only identify the person with an open felony warrant and ignore everyone else. To make that match, the system is potentially identifying/matching all of the times that face shows up in front of a camera. So, a face might be observed dozens of times in a day as the face is recorded in dozens of cameras in a city.

To answer the open questions about whether targeted face tracking is a search for Fourth Amendment purposes, one must examine the future-proofing principles discussed above. As an initial matter, it should be noted that the fact that police could manually compare photos of targets to collected photobooks or other datasets does not end the analysis. Digital is again different. As the Justice Alito recognized in *Jones*, the fact that police could have manually followed Mr. Jones around the streets does not change the fact that monitoring him with digital technology requires a different analysis.[159] A manual search of all Facebook photos would take a lifetime, while a digital search can take mere seconds. *Riley's* "quantitative" and "qualitative" difference of digital technology is made even more obvious in the facial recognition context.[160] While a police officer could recognize a face from a most wanted poster in a city, that officer could never be able to search the entire city's worth of faces over months or years.

The next three subsections examine how the Fourth Amendment would apply to targeted investigation using three different types of face tracking. As will be clear, the difference turns on the dataset being used to match. The analysis focuses on matching from: (1) stored footage of public areas; (2) real-time footage; and (3) third party image datasets.

i. Face Tracking: Stored Footage

[159] *United States v. Jones*, 565 U.S. at 429 (Alito, J. concurring) ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken.").

[160] *Riley*, 134 S. Ct. at 2489.

Face tracking scans using a network of stored video footage might constitute a Fourth Amendment search under *Carpenter*. Like a cell-signal, a scan would reveal where a person was over time. A retrospective scan of stored video footage for a particular individual would (like Timothy Carpenter) involve police tracking a person's location over time, making inferences about the aggregated data, and keeping it for other uses, thus creating the same type of Fourth Amendment harms as in *Carpenter*. A mosaic of geo-locational clues could be mapped to reveal a pattern of activity, tracking personal details and exposing the privacies of life. Where one prays, loves, learns, and lives would all be trackable because of the identifying feature of a face. The data points could be aggregated and be permanently and continually searchable. The camera system would be a pervasive surveillance power, and while targeted to the individual suspect would also capture everyone else (even if they were not identified).

Again, if as has been explained, the Supreme Court is focused on the creation of a system of continuous, automatic surveillance that reveals location and personal details, a stored face tracking system seems to raise the same issues. In both *Jones* and *Carpenter*, the Court was concerned with the potential tracking capabilities as much as the actual details revealed about the particular defendants.[161] A face tracking system provides an even more powerful potential retrospective search system than GPS tracking or cell-site signals.

Of course, open questions remain such as the scale of the surveillance system, the length of time in which the data is held, and whether the revealing nature of face tracking is (under the facts) really more or less revealing than a cell site signal. Unlike cell-site towers, the continuous collection of face images would depend on the density of surveillance cameras and networks.[162] In some cities, there might be more locational details revealed than others. The Fourth Amendment question might thus depend on the sophistication and scale of the technology, which offers an unsatisfying and rather happenstance constitutional answer.

ii. Face Tracking: Real-Time

Real-time scans can identify whether a target is present as he/she/they pass by a facial recognition enabled camera and represent a different Fourth Amendment analysis. Police could run a suspect's face image into a system and in real-time find his current location in a city. Or the situation could

[161] In both cases, the Court spoke of the capacity of GPS tracking or more refined CSLI tracking technology. The focus was less on the particulars of the actual case as opposed to the technology that might yet come.

[162] In *Carpenter*, the Supreme Court was willing to imagine a future of more advanced surveillance capabilities beyond the stated limitations of CSLI technology the year Timothy Carpenter was arrested.

involve a fixed camera outside a shooting range (preventing a wanted felon from entering and possessing a gun) or a police worn body camera automatically alerting the officer to a person with an open arrest warrant.[163]

From one perspective, the animating concerns of the future-proofing principles are somewhat mitigated. The suspect is tracked (but to a particular location). The suspect's location is not aggregated (limited to the one identification at one location). The data is permanent (but not necessarily searchable for extended periods of time). The scan is not arbitrary to the target, even if it is arbitrary when directed to those innocents captured by the camera. Under this reading, the scope of privacy invasion would be real, but limited and may not be a *Carpenter*-like Fourth Amendment violation.

From another perspective, however, the privacy harms look less benign. In order to find that one targeted suspect, a system of facial recognition tracking must be in place to cull out the non-matched. Everyone is being surveilled, just not spotted. Police body cameras would have the potential to scan every face. A lot of innocent people would thus arbitrarily be included in the collection which was a concern in *Carpenter*.[164] In addition, while the search is in real time, the images may still be stored and thus permanently accessible (undermining a central limitation). Finally, other people with the suspect will be collected as part of the incidental collection. The net of associational and inferential connections will grow as never before, reshaping the power the government has over individuals. For this reason, the real-time tracking is less limited than one might think and may raise constitutionally significant questions.[165] But, as may be clear, the Fourth Amendment principles do not resolve the question, and standing problems may forestall any actual Fourth Amendment litigation. The issue remains open for debate and discussion unless resolved by the Supreme Court or Congress.

[163] Ava Kofman, *Real-time Face Recognition Threatens to Turn Cops' Body Cameras into Surveillance Machines*, THE INTERCEPT (Mar. 22, 2017, 2:23 PM), https://theintercept.com/2017/03/22/real-time-face-recognition-threatens-to-turn-cops-body-cameras-into-surveillance-machines/ [http://perma.cc/6Z62-ACCM]; Patrick Tucker, *Facial Recognition Coming to Police Body Cameras*, DEFENSE ONE (July 17, 2017), https://www.defenseone.com/technology/2017/07/facial-recognition-coming-police-body-cameras/139472/ [http://perma.cc/QF35-ALKU].

[164] *Carpenter v. United States*, 138 S. Ct. at 2219 ("The Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years.").

[165] As a parallel, this type of investigative surveillance parallels police use of "Stingray" IMSI cellphone catchers.[165] IMSI technology allows police to find a particular cell phone out of the world of cell phone signals. Using a Stingray device, a police detective could find a particular phone in a particular apartment. The Department of Justice has issued guidance requiring a probable cause warrant before using these devices. Before using IMSI catchers, police must now go before a judge and obtain a warrant to target a particular phone at a particular location. The rationale is the same as it might be for a facial recognition search – in order to find the suspect's phone you need to search through all of the other signals out there, increasing the attendant privacy harms. To minimize that collection, a high standard like probable cause was adopted. *See* Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA Today (Aug. 24, 2015); Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, BALT. SUN (Apr. 9, 2015). DOJ. https://www.justice.gov/opa/file/767321/download.

iii. Face Tracking: Third Party-Controlled Image Searches

The scope and scale of third-party image datasets (Facebook, Google, YouTube, Instagram) are vast and growing, now including billions and billions of images and videos.[166] Police acquisition of some subset of these images to run face tracking matches for identified suspects offer a new investigatory power. If police wished to investigate a suspect by acquiring third-party images of a suspect, they would be able to located and identify more people in a fraction of the time.

Applying the future proofing principles to the problem of police acquisition of third-party images for face tracking purposes is unsatisfying. On the one hand, the request for images (or the ability to search images) will reveal much more personal data than mere identity. All of the times a face is on the platform will be shown which will include information about when the photo was taken, where, and with whom. Unlike cell-site signatures, photos reveal a host of associational information because of the contextual nature of the photos (we can see the subject matter of the photo for example). The aggregation problem exists as well as the permanence problem since the collection of images can be searched in perpetuity. In fact, the situation is more like *Riley* than *Jones*, because the harm comes from the revealing nature of stored digital content and inferences about interests and less pure locational tracking.[167]

On the other hand, all that is being revealed is a photograph (or video and photographs) that seek to confirm identity. Social media images are not a complete catalogue of movement, but a curated, many times inauthentic collection of human activities.[168] Complicating the analysis is the quasi-public nature of the shared photographs as well as any privacy filters that might apply. A single photograph in a third-party image database would not raise concerns, but the open question is whether thousands of photos mapped to location, activity, date, and time might be different.

There is no clear answer to whether police could obtain private images from third party providers without a warrant. *Carpenter* certainly suggests that acquisition of third-party records (that retain an expectation of privacy) raises Fourth Amendment privacy issues. Many of social media third-party images may fall into that category, but some might not, and one might imagine the Supreme Court requiring a similar warrant to acquire some

[166] More than 300 million photos are uploaded every day just on Facebook. https://zephoria.com/top-15-valuable-facebook-statistics/

[167] The Supreme Court in *Riley* was concerned less with the tracking data embedded in a smartphone than with the personal information and interests in the smartphone. The aggregation concern involved more than just locational inferences that invaded privacy, but also interpersonal and informational inferences.

[168] Your Instagram friends are not always in beautiful places taking perfect photos.

forms of private or quasi-private digital content from the photographs themselves (like photo metadata). But the current Fourth Amendment does not resolve the question.

4. Non-Law Enforcement Purposes

The foregoing analysis all presupposed a law enforcement purpose either in the form of surveillance or investigation. But facial recognition technology may also be used for non-law enforcement purposes. Face verification will be utilized in a host of situations requiring proof of identity. In these non-law enforcement situations, like international borders, or entry into secure buildings, the Fourth Amendment analysis is quite different because the purpose of the use is not focused on traditional policing.

The Supreme Court has had an inconsistent relationship with "purpose" when it comes to Fourth Amendment questions.[169] On one hand, the Court tries to avoid any "subjective" considerations of purpose that could entangle the Court in sorting through the individual decisions of officers.[170] In *Whren v. United States*, Justice Scalia stated that the officer's purpose (good or bad) was irrelevant to the Fourth Amendment analysis.[171] At the same time, purpose does matter when it comes to programmatic decisions. In *Edmond* the Court held that because the "primary purpose" of a warrantless checkpoint was for ordinary law enforcement work, the checkpoint was unconstitutional.[172] In doing so the Court distinguished other checkpoint stops where the "purpose" was not traditional law enforcement.[173] And, in the community caretaker cases like *Brigham City, Utah v. Stuart*, the Court stated that because the primary purpose of the responding officers was to offer aid (and not investigate) the ordinary Fourth Amendment principles did not apply.[174] Similar exceptions exist when police are not acting as investigators but under a "special needs" exception.[175] Finally, the Court's new exclusionary rule jurisprudence in *Herring* also seems to muddy the water around purpose because Chief Justice Roberts requires courts to evaluate "objective culpability by looking at whether the officer acted in a

[169] *See generally,* Nirej Sekhon, *Purpose, Policing, and the Fourth Amendment*, 107 J. CRIM. L. & CRIMINOLOGY 65, 66–67 (2017)

[170] *See generally*, Kit Kinports, *Veteran Police Officers and Three-Dollar Steaks: The Subjective/Objective Dimensions of Probable Cause and Reasonable Suspicion*, 12 U. Pa. J. Const. L. 75, 776 (2010).

[171] *See* Whren v. United States, 517 U.S. 806, 813 (1996) ("[T]he constitutional reasonableness of [a] traffic stop[] [does not] depend[] on the actual motivations of the individual officers involved.").

[172] *City of Indianapolis v. Edmond*, 531 U.S. 32, 33 (2000).

[173] *See e.g., Illinois v. Lidster*, 540 U.S. 419, 427 (2004).

[174] *Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006).

[175] Ric Simmons, *The Mirage of Use Restrictions*, 96 N.C. L. REV. 133, 155 (2017) ("A "special needs" search is (in theory) a type of government surveillance which is undertaken for a non-law enforcement purpose. Such purposes have included ensuring the safety of railway passengers, maintaining a positive learning environment in schools, or securing the country's borders.").

"deliberate," 'reckless," or "grossly negligent" manner.[176] As Justice Ginsburg commented in her *Herring* dissent, evaluating deliberateness or culpability necessarily raises issues of subjective purpose and intent.[177]

Facial recognition for non-law enforcement tasks runs right into this "purpose" issue. If police wish to use face surveillance for public safety monitoring (protests, events, special secure places), they could argue that their purpose was not for ordinary law enforcement.[178] Similarly, if police wish to use face tracking to locate a lost child, they could argue for an emergency exception or that there was an "opt-in" choice (almost like consent) to put the child's face in the matching system.[179] Purpose thus could create a workaround for police wishing to use facial recognition technologies, although as in *Edmond* the courts will have to examine the true purpose of the systems.

While purpose is a decidedly imperfect way to distinguish facial recognition uses, it might provide a way out of the Fourth Amendment problems discussed earlier. If explicitly used for non-investigatory purposes with clear *ex ante* guidelines and rules or in emergency situations or particular locations, one might imagine that the Supreme Court would view the problem with a different lens. The clearest examples will be the use of face verification in established points of entry like the international border, although one can imagine how this use could expand to other areas of transport, employment, stadiums, and public schools. In these cases the Fourth Amendment will not offer any check on the development of the technology.

D. Conclusion: Facial Recognition and a Continuum of Systemic Searches

The current Fourth Amendment offers only limited help in acting as a privacy bulwark against expanding networks of facial recognition. The Supreme Court's current emphasis on systems of surveillance certainly maps on to some types of face surveillance and face tracking, but leaves other uses completely unprotected. Networks of face surveillance and face tracking likely require a probable cause warrant, but more limited types of face identification using databases of stored mugshots or DMV photographs might

[176] Kit Kinports, *Veteran Police Officers and Three-Dollar Steaks: The Subjective/Objective Dimensions of Probable Cause and Reasonable Suspicion*, 12 U. PA. J. CONST. L. 751, 776 (2010) ("[T]he very notion of culpability seems to be a subjective one, and in fact the Court drew a distinction in *Herring* between a 'negligen[t] or innocent mistake' and one that is 'deliberate' or 'knowing[],' a distinction phrased explicitly in subjective terms." (second and third alterations in original) (internal quotation marks omitted)).

[177] Herring, 129 S. Ct. at 710 n.7 (Ginsburg, J., dissenting) ("It is not clear how the Court squares its focus on deliberate conduct with its recognition that application of the exclusionary rule does not require inquiry into the mental state of the police.").

[178] Of course, the line between general public safety and policing is a blurry one to define and does not necessarily resolve the Fourth Amendment questions.

[179] But, as might be obvious, in order to find the child, you need to scan everyone else.

not. On a continuum, a line does exist between allowance of some types of police surveillance and a too permeating system of police surveillance, but drawing the line is simply a constitutional guessing game. While the future proofing principles do offer valuable guideposts for Fourth Amendment analysis along the continuum, gaps remain. It is these gaps that necessitate the legislative framework suggested in Part IV.

III. THE FOURTH AMENDMENT AND THE LEGITIMACY PROBLEM OF FACIAL RECOGNITION

Criticism directed at facial recognition is not just about privacy, but also the legitimacy of police tools and strategies. Police legitimacy is at the core of modern Fourth Amendment debates. The use of stop and frisk policies and the use of force have caused a reexamination of structural problems of bias, fairness, transparency, and mistakes. The same issues spill over to the introduction of new surveillance technologies.[180] After all, even if the Fourth Amendment "search" issues could be resolved, facial recognition technology also raises difficult questions about error rates, racial bias, transparency, and fairness that need to be resolved.

The open question is whether the Fourth Amendment offers any answers to these core police legitimacy issues. If facial recognition becomes a preferred policing tool, does the Fourth Amendment offer any constitutional protection? Somewhat troublingly, the Fourth Amendment has little to say about these core police legitimacy issues. In fact, a deep dive into current Fourth Amendment doctrine shows that the Fourth Amendment largely fails to regulate policing around those subjects.

This Part briefly discusses four core "ethical AI" issues: (1) error, (2) bias, (3) transparency, and (4) fairness, asking first why these issues are concerns for facial recognition technology and then what if anything the Fourth Amendment has to say about them. The conclusion, like the conclusion around privacy is that the Fourth Amendment is an imperfect and unsatisfactory protection against expanding facial recognition technology, again suggesting that legislation is needed to counteract these systemic weaknesses.

A. Ethical AI and Concerns About Error, Bias, Fairness, and Transparency

[180] Alvaro M. Bedoya, *The Color of Surveillance*, Slate (Jan. 18, 2016), http://www.slate.com/articles/technology/future_tense/2016/01/what_the_fbi_s_surveillance_of_martin_luther_king_says_about_modern_spying.html; Dorothy Roberts & Jeffrey Vagle, *Racial Surveillance Has a Long History*, Hill (Jan. 4, 2016), http://thehill.com/opinion/op-ed/264710-racial-surveillance-has-a-long-history; Alex Vitale, THE END OF POLICING (2017).

In the computer science and data analytics fields, ethical use of artificial intelligence is now a topic of serious conversation.[181] Hard questions about error, bias, fairness, and transparency are increasingly part of the ongoing conversation about how to build "better" facial recognition technologies.[182] This is all for the good, because correcting the naïve assumption that big data policing systems will not replicate human bias is a necessary first step.[183] The common thread of these critiques is that the perceived objectivity arising from computer code is both false and dangerous, and computer models can be as biased as any other human enterprise.[184] Further, without oversight, artificial intelligence systems could similarly reify existing structural bias or exacerbate inequalities, all-the-while claiming to be data-driven, neutral, and objective.[185] In the specific context of facial recognition technology, the questions become even more pointed.

First, face surveillance does not always work as intended. Real concerns have been demonstrated about the accuracy of face surveillance matches.[186] Early testing of facial recognition has had a poor track record for error. Face surveillance tests in public spaces have bordered on embarrassing with error rates that dwarf success.[187] But, even in more controlled environments there have been errors resulting in false matches – one notable story being how 28 members of Congress were falsely matched with arrestee mugshots using commercially available face identification software.[188] Even the National Institute of Standards and Technology (NIST) found significant

[181] Fairness, Accountability, Transparency Conference. https://fatconference.org/2019/; https://fatconference.org/2018/program.html; Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671, 683–84 (2016) ("Because data mining relies on training data as ground truth, when those inputs are themselves skewed by bias or inattention, the resulting system will produce results that are at best unreliable and at worst discriminatory.").

[182] *Id.*

[183] *See* Safiya Noble, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM (2018); Virginia Eubanks, AUTOMATING INEQUALITY 37 (2018); Cathy O'Neil, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016); Frank Pasquale, THE BLACK BOX SOCIETY (2015). Leading the movement have been scholars and public intellectuals who have called out the dangers of trusting the technology as unbiased, or accurate, or accountable. Joy Buolamwini, *How I'm Fighting Bias in Algorithms*, Ted (Nov. 2016), https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms/transcript?language=en;

[184] Danielle Keats Citron & Frank A. Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014); Paul Ohm, *The Underwhelming Benefits of Big Data*, 161 U. Pa. L. Rev. Online 339, 340 (2013), https://www.pennlawreview.com/online/161-U-Pa-L-Rev-Online-339.pdf [https://perma.cc/U3FS-B9M8]

[185] Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 GA. L. REV. 109, 113 (2017); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. Rev. 93, 94 (2014).

[186] Clare Garvie, *Flawed Face Data* (May 2019) https://www.flawedfacedata.com/; Jeremy C. Fox, "Brown University student mistakenly identified as Sri Lanka bombing suspect." Boston Globe (April 2019), https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-su

[187] Charlotte Jee, *London police's face recognition system gets it wrong 81% of the time,* MIT TECHNOLOGY REVIEW (July 4, 2019) https://www.technologyreview.com/f/613922/london-polices-face-recognition-system-gets-it-wrong-81-of-the-time/

[188] Jacob Snow, ACLU, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, July 26, 2018, https://www.aclu.org/blog/privacytechnology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

errors in early facial recognition vendor tests, especially in attempting to identify women of color.[189] The problems involve both intrinsic and extrinsic problems involving the way in which photos are captured and the complexities of facial features and human movement.[190] This error/accuracy problem, however, may be relatively short-lived as improvements in big data pattern matching will allow companies to improve their error/accuracy rates year by year.

Error for facial recognition has real consequences as a match can lead to investigations, arrests, and prosecution. The danger of false positive hits is real and the consequence for such a false match means a coercive and potentially dangerous encounter with police. In the context of face surveillance with tens of thousands of faces being scanned every day, the reality of inaccurate matching technology will create significant practical problems.[191] In the field, it will be hard for an individual officer to override the suspicion of the algorithm, leading to some erroneous stops and some missed investigations. While police would be wise to never solely rely on the technology, the ease of use and the perceived technical precision might overcome common sense human judgment.

Second, there are issues of bias and the structural inequities that infect the data being used in the facial recognition models. Bias is partly due to the fact that the facial recognition systems were initially designed on homogeneous populations of white men and thus do a poor job of identifying faces of other races,[192] especially black women,[193] and non-conforming individuals.[194] The systemic bias in the datasets[195] is coupled with

[189] Face Recognition Vendor Test (FRVT) from National Institute of Standards and Technology (NIST), https://www.nist.gov/sites/default/files/documents/2019/04/04/frvt_report_2019_04_04.pdf

[190] Jagdish Chandra Joshi and K K Gupta, *Face Recognition Technology: A Review*, 1 THE IUP JOURNAL OF TELECOMMUNICATIONS, 53, 59 (2016) (recognizing intrapersonal problems such as "age, facial expression and facial details/equipment used (facial hair, glasses, cosmetics, veil, etc."); *see also id.* (recognizing extrinsic issues such as "illumination, pose, scale and imaging parameters (e.g., resolution, focus, imaging, noise, etc.").

[191] Joy Buolamwini, *Artificial Intelligence Has a Problem with Gender and Racial Bias. Here's How to Solve It*, TIME (Feb. 7. 2019), http://time.com/5520558/artificial-intelligence-racial-gender-bias/; Clare Garvie & Jonathan Frankle, *Facial Recognition Software Might Have a Racial Bias Problem*, Atlantic (Apr. 7, 2016).

[192] *Artificial Intelligence Has a Problem With Gender and Racial Bias. Here's How to Solve It*, Time Magazine http://time.com/5520558/artificial-intelligence-racial-gender-bias/; Tom Simonite, *Photo Algorithms ID White Men Fine - Black Women, Not So Much*, Wired (Feb. 6, 2018), https://www.wired.com/story/photo-algorithms-id-white-men-fineblack-women-not-so-much/; Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, Wired (July 22, 2019) https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/?verso=true

[193] https://medium.com/@Joy.Buolamwini/when-ai-fails-on-oprah-serena-williams-and-michelle-obama-its-time-to-face-truth-bf7c2c8a4119; Joy Buolamwini & Timnit Gebru, Gender Shades, 81 Proceedings of Machine Learning Research 1, 11 (2018).

[194] Cynthia M. Cook et al., *Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*," in *IEEE Transactions on Biometrics, Behavior, and Identity Science* (February 2019), https://ieeexplore.ieee.org/document/8636231

[195] IBM Research, Diversity in Faces (April 2019), https://arxiv.org/pdf/1901.10436.pdf ("Face recognition systems that are trained within only a narrow context of a specific data set will inevitably acquire bias that skews learning towards the specific characteristics of the dataset.)"

incomplete, incorrect, and fragmented data[196] which leads to a system that discriminates against anyone but white men, and almost completely erases transgender, non-conforming, or non-binary individuals.[197] As the bias tracks along race and gender lines the mistakes could also follow those patterns.[198] In some cases, it will mean that darker skin people will be missed by the system, but in others the matches will be less accurate.[199]

Third, there are issues of fairness in application and whether a facial recognition system is fair to use across a diverse population. In computer science there are complex debates about the first principles of fairness.[200] For example, one could think of "fairness" as non-discrimination (based on a particular characteristic), or "fairness" as choosing equally among groups, or "fairness" as preferring false positives to false negatives, or "fairness" as random selection or a host of other definitions all of which can shape how a machine learning model is developed.[201] All of these differing definitions of fairness offer some measure of a fair process, but they result in decidedly different outcomes if coded into a facial recognition model. In a computer design situation, the model's outcome can be directly impacted by the type of fairness deemed optimal. In the real world, this design might lead to unfair application.

Finally, there are issues of transparency as "black box" technologies require overcoming complaints of proprietary trade secrets and a lack of accountability.[202] The artificial intelligence and machine learning

[196] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data* (May 16, 2019), https://www.flawedfacedata.com/

[197] Joy Buolamwini, Testimony Before United States House Committee on Oversight and Government Reform, May 22, 2019, *Hearing on* Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties ("when evaluating error rates for the the facial analysis task of binary-gender classification (which does not account for gender nonconforming people, nonbinary people, agender people, and/or transgender people), our 2018 Gender Shades audit showed women with skin types associated with blackness had error rates as high as 47%. In the same study for men with skin-types perceived as white, error rates were no more than .08% in aggregate."); 78 Concerned Researchers, *On Recent Research Auditing Commercial Facial Analysis Technology*, Medium (Mar. 26, 2019) https://medium.com/@bu64dcjrytwitb8/on-recent-research-auditing-commercial-facial-analysis-technology-19148bda1832 ("[C]urrent gender classification methods use only a "male" and "female" binary — non-binary genders are not represented in these systems.")

[198] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81:1(15, 2018)

[199] Claire Garvie & Jonathan Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, THE ATLANTIC (Apr. 7, 2016).

[200] https://towardsdatascience.com/a-tutorial-on-fairness-in-machine-learning-3ff8ba1040cb

[201] *See e.g.*, Andrew Selbst, et.al., *Fairness and Abstraction in Sociotechnical Systems*, FAT Conference, http://delivery.acm.org/10.1145/3290000/3287598/p59-Selbst.pdf?ip=38.105.72.65&id=3287598&acc=NO%20RULES&key=EA62C54EFA59E1BA%2E39CF5184832A1C04%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1563903354_22c64486ae263e3b34b412a6cff5ea38; Richard Berk, et.al., *Fairness in Criminal Justice Risk Assessments: The State of the Art* https://arxiv.org/pdf/1703.09207.pdf

[202] *See e.g.*, Elizabeth E. Joh , *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. Rev. Online 101, 119-20 (2017); Brent Mittelstadt, *Explaining Explanations in AI*, http://delivery.acm.org/10.1145/3290000/3287574/p279-Mittelstadt.pdf?ip=38.105.72.65&id=3287574&acc=NO%20RULES&key=EA62C54EFA59E1BA%2E39CF5184832A1C04%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1563903557_868d56c751ad0a639fd16cc9d20b3b98

community has long confronted issues of transparency, secrecy, accountability, inscrutability,[203] interpretability, and explainability.[204] The same is obviously true with the machine learning systems fueling facial recognition technology. As machines get more sophisticated and as artificial intelligence and machine learning companies entering the policing space, it may be difficult to obtain any measure of transparency among the complex models and competing proprietary interests.

B. The Fourth Amendment and Error, Bias, Transparency, and Fairness

In the face of such questions about facial recognition technology, one might hope that the Constitution, in the form of the Fourth Amendment's limits on policing might provide a substantial counterweight. Unfortunately, the Fourth Amendment has little to say about the matter, offering almost no response to the problems of error, bias, fairness or transparency in policing more generally, and facial recognition in particular.

This section addresses how the Supreme Court has ignored issues of error, bias, fairness, and transparency in traditional Fourth Amendment cases. Thus, if offered as a design guide to computer engineers interested in designing a constitutionally compliant facial recognition system, the Fourth Amendment would be decidedly unhelpful.

1. Error and Policing

Error is part of policing. The Supreme Court has crafted Fourth Amendment rules to forgive error when seizing individuals, arresting individuals, and when considering the suppression of evidence for merely negligent errors.[205] The only time the Supreme Court appears to punish police error is if it is intentional, reckless, grossly negligent or systemic or recurring – a high bar to clear.[206] This section examines the extent of error allowed in Fourth Amendment doctrine to show how limited the Fourth

[203] Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085, 1091 (2018)

[204] *Id.*

[205] Kit Kinports, *Illegal Predicate Searches and Tainted Warrants After Heien and Strieff*, 92 TUL. L. REV. 837, 880 (2018) ("The definitions of probable cause and reasonable suspicion already give the police room to make reasonable errors in applying those standards to the facts of a particular case."); Herring v. United States, 129 S. Ct. 695, 702 (2009) ("To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system. As laid out in our cases, the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.").

[206] Davis v. United States, 131 S. Ct. 2419, 2427–28 (2011) ("When the police exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs. But when police act with an objectively 'reasonable good-faith belief' that their conduct is lawful, or when their conduct involves only simple, 'isolated' negligence, the 'deterrence rationale loses much of its force'").

Amendment would be as a guide to regulating error in facial recognition design.

a. Error & Reasonable Suspicion

The legal standard of "reasonable suspicion[207] which constrains police from stopping or seizing an individual suspected of criminal activity is a clear acknowledgment that police will err in their judgments on the streets.[208] The rule stated in *Terry v. Ohio* and controlling in thousands of cases is: "[I]n justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion."[209] In subsequent cases, the Court has acknowledged that reasonable suspicion can involve completely innocent conduct,[210] can be based on less than perfectly reliable information, and should be evaluated under a "totality of circumstances" test.[211] It can also be wrong. Suspicion does not equal certainty.

The Supreme Court has never quantified just how mistaken an officer can be or how low the threshold for error should be set. In fact, the Supreme Court has been emphatic in refusing to quantify the certainty of reasonable suspicion. Commentators and judges, however, have not been so reticent and have opined on the rough parameters of what percentage likelihood would look like for reasonable suspicion. Generally, the estimated range runs between a 30%-20% level of "certainty."[212] Although, one survey of judges had a broader range from 50%-10%.[213] Generally speaking, we know that

[207] The rule comes from *Terry v. Ohio*, 392 U.S. 1, 19 (1968) a case involving an experienced police officer watching the unusual behavior of John Terry and two associates outside a store in downtown Cleveland, Ohio. *Id.* 5-6. Officer McFadden believed the men were "casing" the store in preparation for a robbery and so he approached them, stopped, frisked, and found an illegal handgun on John Terry. In justifying Officer McFadden's stop of Terry on less than probable cause, the Supreme Court credited McFadden's interpretation that the behaviors of the men were suspicious.

[208] *Heien v. North Carolina*, 135 S. Ct. 530, 536 (2014) ("To be reasonable is not to be perfect, and so the Fourth Amendment allows for some mistakes on the part of government officials, giving them "fair leeway for enforcing the law in the community's protection."); see also id. ("[I]f officers with probable cause to arrest a suspect mistakenly arrest an individual matching the suspect's description, neither the seizure nor an accompanying search of the arrestee would be unlawful.").

[209] *Id.* at 21.

[210] United States v. Arvizu, 534 U.S. 266, 277 (2002) ("A determination that reasonable suspicion exists . . . need not rule out the possibility of innocent conduct.").

[211] *United States v. Sokolow, 490 U.S. 1, 7 (1989)* ("Reasonable suspicion is a less demanding standard than probable cause not only in the sense that reasonable suspicion can be established with information that is different in quantity or content than that required to establish probable cause, but also in the sense that reasonable suspicion can arise from information that is less reliable than that required to show probable cause.").

[212] Stephen E. Henderson, *A Rose by Any Other Name: Regulating Law Enforcement Bulk Metadata Collection*, 94 TEX. L. REV. SEE ALSO 28, 39 (2016) (positing that "reasonable suspicion is something akin to being 30% confident"); Christopher Slobogin, *Let's Not Bury Terry: A Call for Rejuvenation of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053, 1083 (1998) (reasonable suspicion "to be something like a 20% to 30% chance of success).

[213] L. Song Richardson, *Police Efficiency and the Fourth Amendment*, 87 IND. L.J. 1143, 1156–57 (2012) ("When 164 judges were asked to quantify how much evidence they felt was required to sustain

reasonable suspicion is more than a hunch, but less than probable cause, and no matter what "number" is chosen within this accepted range, it has a huge margin of error (again taking the average -- somewhere between 70%-80% getting it wrong).

For a facial recognition system, this uncertainty means that the error rate for a match could be significant (and yet constitutional).[214] Both false positives and false negatives may occur, and within the existing percentages many individuals could be incorrectly stopped based on erroneous matches.[215] If mapped to the reasonable suspicion standard, a facial recognition system could be more wrong than right and still be constitutional (or at least not violative of the Fourth Amendment).

b. Error & Probable Cause

Probable cause that a person's face matches the face of a person with an open felony warrant could be sufficient to arrest them on the spot. Probable cause is the legal standard that constrains police from arresting or searching individuals.[216] The standard originates from the text of the Fourth Amendment, but despite this provenance its meaning has never been established in any single definition. The Supreme Court has articulated several formulations over the years, but has generally agreed that probable cause should be determined under "the totality of circumstances" "defined in terms of facts and circumstances 'sufficient to warrant a prudent man in believing that the (suspect) had committed or was committing an offense"[217] or when "there is a fair probability that contraband or evidence of a crime will be found in a particular place."[218] The Court has gone on to emphasize that "probable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully,

a reasonable suspicion, their estimates ranged from 50% at the high end to 10% at the low end."); Ric Simmons, *Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in Our Criminal Justice System*, 2016 MICH. ST. L. REV. 947, 1005 (2016) ("Judges appear to have widely divergent views as to this question, with survey results varying widely but averaging at 30.8% for reasonable suspicion and 44.5% for probable cause.").

[214] The human equivalent of this process would be an officer erroneously believing the person who just walked past him has an open warrant, but he misidentifies the person.

[215] The variables that can be factored into the matching system (creating reasonable suspicion of a match) are wide open. The "totality of circumstances" does not exclude many factors, leaving design parameters open.

[216] Andrew Crespo, Probable Cause Pluralism, Yale L. J. (forthcoming 2020); https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3342902; 5 Am. Jur. 2d Arrest § 9 ("Under the Fourth Amendment, the standard for arrest is probable cause, defined in terms of facts and circumstances sufficient to warrant a prudent person in believing that the suspect has committed or is committing an offense; this standard, like those for searches and seizures, represents a necessary accommodation between the individual's right to liberty and the state's duty to control crime.").

[217] *Gerstein v. Pugh*, 420 U.S. 103, 111 (1975)

[218] *Illinois v. Gates*, 462 U.S. 213, 238 (1983) ("[T]he task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the "veracity" and "basis of knowledge" of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.").

reduced to a neat set of legal rules."[219] Because the standard is meant to be used in the real world, the Supreme Court has emphasized its "practical, common-sense" application,[220] and specifically refused to offer any quantification.[221] Generally, the objective test is whether a "man of reasonable caution" or "reasonably prudent person" would judge that a crime had been committed.[222] Reasoned probability, not certainty is the requirement, meaning that mistakes are baked into the standard.[223]

Scholars, judges, and law enforcement agents examining probable cause in practice have attempted to quantify this probability with some general consensus.[224] As Professor Ric Simmons has written, "Most commentators also agree that probable cause is something close to but just less than 50%,—while scattered evidence from prosecutors and law enforcement point to numbers between 40% and 51%."[225] The quantum of

[219] *Id.* at 232; Brinegar v. United States, 338 U.S. 160, 175 (1949) ("In dealing with probable cause, however, as the very name implies, we deal with probabilities."); Max Minzner, *Putting Probability Back into Probable Cause*, 87 Tex. L. Rev. 913, 915–16 (2009) ("[T]he probable-cause determination is explicitly and exclusively a statement about the probability of a particular outcome—namely, the odds of recovering evidence from a particular location.")

[220] Illinois v. Gates, 462 U.S. 213, 244 (1983) ("[W]e think it suffices for the practical, common-sense judgment called for in making a probable-cause determination.").

[221] Maryland v. Pringle, 540 U.S. 366, 371 (2003) ("The probable-cause standard is incapable of precise definition or quantification into percentages because it deals with probabilities and depends on the totality of the circumstances.")

[222] Safford Unified Sch. Dist. No. 1 v. Redding, 557 U.S. 364, 370 (2009) ("'Probable cause exists where the facts and circumstances . . . warrant a man of reasonable caution in the belief that' an offense has been or is being committed,' and that evidence bearing on that offense will be found in the place to be searched."); Florida v. Harris, 568 U.S. 237, 247–48 (2013) ("The question—similar to every inquiry into probable cause—is whether all the facts . . . viewed through the lens of common sense, would make a reasonably prudent person think that a search would reveal contraband or evidence of a crime.").

[223] Hill v. California, 401 U.S. 797, 804 (1971) ("[S]ufficient probability, not certainty, is the touchstone of reasonableness under the Fourth Amendment . . . .").

[224] Ric Simmons, *Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in Our Criminal Justice System*, 2016 MICH. ST. L. REV. 947, 987–88 (2016) ("Forty-five years ago, one law professor surveyed 166 federal judges to ask them to quantify the concept of probable cause, and the results ranged from ten percent to ninety percent.") (citing C.M.A. McCauliff, *Burdens of Proof: Degrees of Belief, Quanta of Evidence, or Constitutional Guarantees?*, 35 VAND. L. REV. 1293, 1327 (1982)) (The vast majority of the judges were between the 30% and 60% range--16% answered 30%, 27% answered 40%, 31% answered 50%, and 15% answered 60%--still indicating a wide range of disagreements. *Id.); but see* Kiel Brennan-Marquez, *"Plausible Cause": Explanatory Standards in the Age of Powerful Machines*, 70 VAND. L. REV. 1249, 1251 (2017) (arguing against quantification and for an explainable context for suspicion).

[225] Ric Simmons, *Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in Our Criminal Justice System*, 2016 MICH. ST. L. REV. 947, 1005 (2016); *see also* Ronald J. Bacigal, *Making the Right Gamble: The Odds on Probable Cause*, 74 MISS. L.J. 279, 338-39 (2004) (using an imprecise range of 40-49%); Daniel A. Crane, *Rethinking Merger Efficiencies*, 110 MICH. L. REV. 347, 356 (2011) (noting that practitioners and commentators estimate probable cause to be "in the 40-45 percent range"); Stephen E. Henderson, *A Rose by Any Other Name: Regulating Law Enforcement Bulk Metadata Collection*, 94 TEX. L. REV. SEE ALSO 28, 38–39 (2016) ("Some think probable cause requires a preponderance of the evidence, whereas I think it a slightly less, albeit inarticulable, measure."); Christopher Slobogin, *Let's Not Bury Terry: A Call for Rejuvenation of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053, 1083 (1998) (probable cause at about 50%); Lawrence Rosenthal, *The Crime Drop and the Fourth Amendment: Toward an Empirical Jurisprudence of Search and Seizure*, 29 N.Y.U. REV. L. & SOC. CHANGE 641, 680 (2005) (anecdotal account of a prosecutor stating probable cause is about 40%); Daniel Richman, *Prosecutors and Their Agents, Agents and Their Prosecutors*, 103 COLUM. L. REV. 749, 783 (2003) (anecdotal account of FBI agent probable cause is 51%).

evidence is certainly greater than reasonable suspicion.[226] A variation along a spectrum around 40% to 51% provides a general sense of the certainty required for an arrest or full search. Similar to reasonable suspicion, police have no obligation to consider exculpatory or innocent conduct,[227] can base their decisions on inferences,[228] and their judgment can be mistaken.[229]

The consequences of a 50% error rate for a facial recognition matching system are quite serious. An automated match (correct or not) will mean the identified suspect could be handcuffed, searched, and forcibly detained. The person may be incarcerated pending resolution of the warrant allegation. Absent unusual circumstances, police officers will have little discretion on whether or not to arrest an individual matched by the computer system. In fact, four fairly recent Supreme Court cases have involved errors arrest warrants.[230] And, again under a totality of circumstances many different inputs can be used to make the match.

c. Negligent Error

The doctrines of reasonable suspicion and probable cause forgive error at high rates. But even those percentages underestimate the permissible amount of Fourth Amendment error tolerated in policing. Adding to the calculus is the fact that the Supreme Court has both narrowed the scope of the exclusionary rule to obtain a remedy in the criminal justice system and raised the bar for qualified immunity for Fourth Amendment violations in the civil legal system.[231] By restricting both civil and criminal remedies for police mistakes, the consequence for errors drops.

For purposes of suppression the Supreme Court now forgives police error that was not intentional, reckless, grossly negligent, or the product of

[226] *United States v. Sokolow, 490 U.S. 1, 7 (1989)* ("We have held that probable cause means 'a fair probability that contraband or evidence of a crime will be found,' ... *and the level of suspicion required for a *Terry* stop is obviously less demanding than that for probable cause ....").

[227] Ahlers v. Schebil, 188 F.3d 365, 371 (6th Cir. 1999) ("Once probable cause is established, an officer is under no duty to investigate further or to look for additional evidence which may exculpate the accused.");

[228] Illinois v. Wardlow, 528 U.S. 119, 124-25 (2000) ("In reviewing the propriety of an officer's conduct, courts do not have available empirical studies dealing with inferences drawn from suspicious behavior, and we cannot reasonably demand scientific certainty from judges or law enforcement officials where none exists."); L. Song Richardson, Police Efficiency and the Fourth Amendment, 87 IND.L.J.1143, 1155 (2012) (noting that "courts consistently fail to determine whether the inferences drawn by the officer conducting the stop are actually entitled to any weight").

[229] Sherry F. Colb, *Probabilities in Probable Cause and Beyond: Statistical Versus Concrete Harms*, Law & Contemp. Probs., Summer 2010, at 69 ("'[P]robable cause' necessarily contemplates that official action may be undertaken in situations under which there is some probability that the action will prove to have been 'correct' (it will accomplish the objective for which it was initiated), and some probability that the action will prove to have been 'incorrect' (it will cause harm that, ex post, was not justified).").

[230] *See* Florence v. Bd. of Chosen Freeholders, 132 S. Ct. 1510 (2012); Herring v. United States, 555 U.S. 135 (2009); Rothgery v. Gillespie Cty., 554 U.S. 191 (2008); Arizona v. Evans 514 U.S. 1 (1995).

[231] *See e.g.*, Jennifer E. Laurin, *Trawling for Herring: Lessons in Doctrinal Borrowing and Convergence*, 111 COLUM. L. REV. 670, 684 (2011).

systemic or recurring problems.[232] In other words, merely negligent error will not result in the suppression of evidence.

In a series of recent cases, the Supreme Court has signaled that mere negligent error – a misjudgment or mistake – will not be sufficient to warrant use of the exclusionary rule.[233] As Chief Justice John Roberts wrote in *Herring v. United States*:[234]

> To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system. As laid out in our cases, the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.[235]

In practical effect, this means that the negligent error of a police officer or police employee will not result in suppression.[236]

For purposes of a facial recognition pattern matching technologies, *Herring* solidifies the reality that negligent errors in application will not undermine the constitutionality of the system.[237] Only intentional or reckless or systemic instances of error will warrant an exclusionary rule remedy. While rights and remedies are certainly different, this forgiving of error certainly allows a greater freedom for mistakes. If merely negligent, an error

[232] Andrew Guthrie Ferguson, *Constitutional Culpability: Questioning the New Exclusionary Rules*, 66 FLA. L. REV. 623, 639 (2014)

[233] *Utah v. Strieff*, 136 S. Ct. 2056 (2016); *Davis v. United States*, 131 S. Ct. 2419 (2011); *Herring v. United States*, 555 U.S. 135 (2009).

[234] 555 U.S. 135, 137 (2009).

[235] *Herring*, 555 U.S. at 144.

[236] *Id.* at 137 (holding that "the error was the result of isolated negligence attenuated from the arrest"); Four relatively recent Supreme Court cases involved arrests based on police errors. *See* Florence v. Bd. of Chosen Freeholders, 132 S. Ct. 1510 (2012); Herring v. United States, 555 U.S. 135 (2009); Rothgery v. Gillespie Cty., 554 U.S. 191 (2008); Arizona v. Evans 514 U.S. 1 (1995). *See also Baker v. McCollan*, 443 U.S. 137, 144-46 (1979), where the Court held that a mistaken arrest based on a facially valid warrant is not itself a Fourth Amendment violation, and that police have no duty "to investigate independently" claims of mistaken identity.; *see generally* Andrew D. Selbst, *Negligence and AI's Human Users*, Boston University Law Review (Forthcoming 2020) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3350508.

[237] Interestingly *Herring*, itself, was a case about data error. About how a mistake in a computer database did not justify suppression because there was no evidence of systemic or recurring problems. In the case, Bennie Dean Herring was arrested because a database search erroneously stated that he had an open felony arrest warrant. It turned out that the database had not been updated, but by the time the investigating agent realized the mistake, drugs and a gun were recovered on Mr. Herring's person. In refusing to exclude the evidence, the Court suggested that merely negligent data error would not be the subject of constitutional remedy. This general acceptance of police error and data error in the criminal justice system has been well cataloged in prior work. Wayne A. Logan & Andrew Guthrie Ferguson, *Policing Criminal Justice Data*, 101 MINN. L. REV. 541, 542–43 (2016) (detailing how there are "significant quality problems with criminal justice databases" and a "blasé acceptance of data error and its negative consequences for individuals"); Herring v. United States, 555 U.S. 135, 155–56 (2009) (Ginsburg, J., dissenting) ("Inaccuracies in expansive, interconnected collections of electronic information raise grave concerns for individual liberty. 'The offense to the dignity of the citizen who is arrested, handcuffed, and searched on a public street simply because some bureaucrat has failed to maintain an accurate computer data base is evocative of the use of general warrants that so outraged the authors of our Bill of Rights.'" (quoting Arizona v. Evans, 514 U.S. 1, 23 (1995) (Stevens, J., dissenting))).

in a facial recognition match will have no consequence for police investigation.[238]

2. Bias

Implicit and explicit biases exist in all human endeavors, but systemic racial bias has been revealed in policing practices at a discomforting level.[239] Yet, intentional or unintentional racial bias does not factor into the Fourth Amendment calculus (although it may raise equal protection or due process concerns).[240] The Fourth Amendment regulates police actions, but it does so within the social, economic, and racial realities of modern America. Those realities are not comforting to advocates of racial equity because they reveal a policing structure that has repeatedly demonstrated racial bias toward communities of color.[241] In hundreds of investigations, lawsuits, media stories, and personal anecdotes the reality of racial bias in policing has been made plain.[242] Especially in urban areas with higher crime rates, the problems of explicit and implicit bias and structural racism persist.[243]

Despite this reality, the Supreme Court has refused to allow the Fourth Amendment to be a vehicle to address racial bias in individual cases.[244] In *Whren*,[245] the Court held in response to a claim of a racially biased pretextual traffic stop: "[T]he constitutional basis for objecting to intentionally discriminatory application of laws is the Equal Protection Clause, not the Fourth Amendment."[246] This understanding that racial bias is largely

[238] Similarly, civil remedies ordinarily effectuated by lawsuits against police officers have also been limited by an expanded qualified immunity doctrine. Civil lawsuits claiming that a police officer made an error in applying the Fourth Amendment regularly lose in court, and have been restricted by the Supreme Court in a series of cases. Moreover, the layers of legal rules scaffolding the qualified immunity doctrine and section 1983 doctrine make individual civil rights cases rare to bring and even rarer to win. Most false stop or arrests cases do not get litigated.

[239] L. Song Richardson, *Police Efficiency and the Fourth Amendment,* 87 IND. L.J. 1143, 1170 (2012); L. Song Richardson, *Arrest Efficiency and the Fourth Amendment*, 95 MINN. L. REV. 2035, 2061-63 (2011).

[240] Whren, 517 U.S. at 813 ("We of course agree with petitioners that the Constitution prohibits selective enforcement of the law based on considerations such as race. But the constitutional basis for objecting to intentionally discriminatory application of laws is the Equal Protection Clause, not the Fourth Amendment.").

[241] *See generally,* Alex Vitale, THE END OF POLICING (2017); Paul Butler, CHOKEHOLD: POLICING BLACK MEN, 59–61 (2017).

[242] *See e.g.,* Paul Butler, *Stop and Frisk and Torture-Lite: Police Terror of Minority Communities,*12 OHIO ST. J. CRIM. L. 57, 66–69 (2014); R. Richard Banks, *Beyond Profiling: Race, Policing, and the Drug War*, 56 STAN. L. REV. 571 (2003); CHARLES J. OGLETREE, JR. ET AL., BEYOND THE RODNEY KING STORY: AN INVESTIGATION OF POLICE CONDUCT IN MINORITY COMMUNITIES 24, 52–53 (1995); s*ee also* CIVIL RIGHTS DIV., U.S. DEP'T of JUSTICE, INVESTIGATION OF THE FERGUSON POLICE DEPARTMENT 2–3 (Mar. 15, 2015), https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_report.pdf [https://perma.cc/W7NS-9CSB]; CIVIL RIGHTS DIV., U.S. DEP'T OF JUSTICE, INVESTIGATION OF THE BALTIMORE CITY POLICE DEPARTMENT 24 (Aug. 10, 2016), https://www.justice.gov/crt/file/883296/download [https://perma.cc/U4CT-49ZN]

[243] Cedric Merlin Powell, *The Structural Dimensions of Race: Lock Ups, Systemic Chokeholds, and Binary Disruptions*, 57 U. LOUISVILLE L. REV. 7, 8 (2018); Professor Scott Holmes, *Resisting Arrest and Racism - the Crime of "Disrespect"*, 85 UMKC L. REV. 625, 637–38 (2017)

[244] Gabriel J. Chin & Charles J. Vernon, *Reasonable but Unconstitutional: Racial Profiling and the Radical Objectivity of Whren v. United States*, 83 GEO. WASH. L. REV. 882, 884 (2015)

[245] 517 U.S. 806 (1996)

[246] Whren v, 517 U.S. at 813.

irrelevant to policing decisions has largely foreclosed Fourth Amendment claims based on racial discrimination.[247] While race, alone, would not constitute an appropriate justification for a stop, search, or arrest the Court will likewise not declare a stop unconstitutional because it is racially motivated.[248] In the pattern matching context, this would mean that a system programed to encourage pretextual race-based stops would not necessarily run into Fourth Amendment problems.

In addition, proxies for racial bias about certain groups or in certain areas would be permissible to include in the matching model. The Supreme Court has allowed proxies for race, poverty, and nationality to impact reasonable suspicion and probable cause in a series of Fourth Amendment cases.[249] "High crime areas,"[250] "drug courier profiles"[251] incongruity,[252] and immigration-related stops[253] all rely on proxies for individuals who have historically been targeted by police. The result has been that inputs that stand in for race can be used to justify a stop or arrest (at least in the human policing context).[254]

[247] Utah v. Strieff, 136 S. Ct. 2056, 2069 (2016) (Sotomayor, J., dissenting) ("[An officer's] justification must provide specific reasons why the officer suspected you were breaking the law, but it may factor in your ethnicity, where you live, what you were wearing, and how you behaved. The officer does not even need to know which law you might have broken so long as he can later point to any possible infraction--even one that is minor, unrelated, or ambiguous." (citations omitted)).

[248] Ric Simmons, *Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in Our Criminal Justice System*, 2016 MICH. ST. L. REV. 947, 971 (2016) ("Fourth Amendment jurisprudence has little to say about whether race can be used as a factor in determining reasonable suspicion or probable cause. Courts are unanimous in holding that race alone can never be the basis for a stop or a search, for the obvious reason that a person's race alone can never create probable cause or even reasonable suspicion that criminal activity is occurring." *See, e.g.*, United States v. Brignoni-Ponce, 422 U.S. 873, 886-87 (1975) ("[Mexican ancestry] alone ... does not justify stopping all Mexican-Americans to ask if they are aliens."); State v. Kuhn, 517 A.2d 162, 165 (N.J. Super. Ct. App. Div. 1986) ("No rational inference may be drawn from the race of [a person] that he may be engaged in criminal activities.").

[249] Ric Simmons, *Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in Our Criminal Justice System*, 2016 MICH. ST. L. REV. 947, 976 (2016); K. Babe Howell, *Broken Lives From Broken Windows: The Hidden Costs of Aggressive Order-Maintenance Policing*, 33 N.Y.U. REV. L. & SOC. CHANGE 271, 276–80 (2009).

[250] Illinois v. Wardlow, 528 U.S. 119, 124 (2000); Ric Simmons, *Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in Our Criminal Justice System*, 2016 MICH. ST. L. REV. 947, 976 (2016) ("No doubt in many instances, higher-crime neighborhoods will tend to be inner city neighborhoods with higher proportions of certain minority groups (or at least this will be the perspective of many police officers and judges). And this formal use of proxies for race under the current system is likely only the tip of the iceberg. The unconscious (or conscious) racial biases of police officers and magistrates permeate every aspect of the front end of the criminal justice system.").

[251] Tracey Maclin, *The Decline of the Right of Locomotion: The Fourth Amendment on the Streets*, 75 CORNELL L. REV. 1258, 1299 (1990) ("In the drug courier profile cases, the Court accorded police officials broad discretionary powers that do not implicate the fourth amendment. Mendenhall and Royer demonstrated that questioning citizens does not trigger fourth amendment scrutiny.").

[252] Sheri Lynn Johnson, *Race and the Decision to Detain A Suspect*, 93 YALE L.J. 214, 226 (1983) ("Police manuals often instruct officers to become familiar with their beat and question persons who do not "belong.").

[253] *United States v. Brignoni-Ponce*, 422 U.S. 873, 880 (1975).

[254] L. Song Richardson, *Arrest Efficiency and the Fourth Amendment*, 95 MINN. L. REV. 2035, 2080 (2011) ("[C]ourts currently allow officers to rely on race and proxies for race (such as consideration of high-crime neighborhoods) to justify Terry seizures."); David Rudovsky, *Law Enforcement by Stereotypes and Serendipity: Racial Profiling and Stops and Searches Without Cause*, 3 U. PA. J. CONST. L. 296, 304 (2001).

In the facial recognition pattern matching context, such proxy inputs might also be allowed. So, while a machine would not code for race, it might code for hairstyle, or facial composition, which in turn might stand in to represent (accurately or inaccurately) a particular race. Depending on what information was collected, some matching might include geographic areas (where the photograph is taken) which also could easily substitute as a neighborhood proxy for race or ethnicity[255] or the system could be programed for tattoo recognition as a proxy for gang involvement (and thus criminality).[256] At least from a Fourth Amendment perspective, there is nothing stopping facial recognition designers from creating and relying on these proxies to do the work that race might do in the algorithm. If a correlation for suspicion can be found, the Fourth Amendment would not preclude its use. This is a problem since, as discussed, early tests of facial recognition identification systems have been shown to be discriminatory toward African Americans,[257] and especially African American women.[258]

3. Fairness

Fairness presents an equally complex principle for policing. On one hand fairness defined as equality under the law and equal application of the law remain aspirational goals for police. Police are supposed to enforce the law the same regardless of race, class, age, gender, or neighborhood.[259] In actual practice, this has not been the case, as differences in race, class, gender, and place have impacted every facet of the policing process.[260] As a matter

[255] Margaret Raymond, *Down on the Corner, Out in the Street: Considering the Character of the Neighborhood in Evaluating Reasonable Suspicion*, 60 OHIO ST. L.J. 99, 138 (1999) ("Using the character of the neighborhood as a factor in the determination of reasonable suspicion results in the consideration by proxy of the impermissible factors of race and poverty. Even if the factor is not consciously used in this fashion, using this criterion will have a disproportionate impact on such communities.").

[256] *See generally* Aaron Mackey, Dave Maass & Soraya Okuda, *5 Ways Law Enforcement Will Use Tattoo Recognition Technology*, Electronic Frontier Foundation (June 2, 2016), www.eff.org/deeplinks/2016/05/5-ways-law-enforcement-will-use-tattoo-recognition-technology

[257] *See supra* note xx.

[258] *Id.*

[259] Tracey L. Meares, Tom R. Tyler, *Justice Sotomayor and the Jurisprudence of Procedural Justice*, 123 YALE L.J. FORUM 525, 539 (2014) (distinguishing between fairness of decisionmaking and the fairness of treatment); Stephen D. Mastrofski et al., *Compliance on Demand: The Public's Response to Specific Police Requests*, 33 J. Res. Crim. & delinq. 269 (1996) (personal experience procedural fairness increases compliance with police).

[260] *See generally* Andrew Kahn & Chris Kirk, *What it's like to be Black in the Criminal Justice System*, Slate (Aug. 9, 2015), http://www.slate.com/articles/news_and_politics/crime/2015/08/racial_disparities_in_the_criminal_justice_system_eight_charts_illustrating.html; Brad Heath, *Racial Gap in U.S. Arrest Rates: "Staggering disparity"*, USA Today (Nov. 19, 2014), http://www.usatoday.com/story/news/nation/2014/11/18/ferguson-black-arrest-rates/19043207/

of procedural fairness,[261] or procedural justice,[262] or just common experience, police treat different people differently.[263] And sadly, from a Fourth Amendment perspective, "fairness" defined as equal treatment of people, groups, and places has never been constitutionally required by the Fourth Amendment.

In fact, explicit adoption of profiling, high crime areas, border searches, and a litany of poverty focused exceptions to the warrant requirement all speak to an unequal and unfair doctrine.[264] In addition, police tactics have not been the same for all communities and all people. Differences in terms of the impact of stop and frisk tactics,[265] use of force, and surveillance all undermine a claim of a fair (uniform and equal) application of the Fourth Amendment. Some communities bear the brunt of police tactics with no relief provided by the Fourth Amendment.[266] Focused simply on how the Fourth Amendment guides equal treatment in the real world, one might argue that it has no impact or worse reifies an unequal and unfair society that is riven by differences in race, class, gender, and neighborhood.[267]

For purpose of building a facial recognition matching system, the same tension between ideals and application arise. The ideal of fairness, meaning applying the same decision-making rules to similar problems is

[261] Joshua J. Reynolds, Victoria Estrada-Reynolds & Narina Nunez, *Development and Validation of the Attitudes Towards Police Legitimacy Scale*, 42 LAW & HUM. BEHAV. 119, 120 (2018) (citing Tankebe (2013)) ("*Procedural fairness*, which concerns the fairness of how the outcomes are reached, is based on the quality of decision-making (e.g., opportunities for error correction) and the quality of treatment (e.g., respect, dignity, and courtesy)".).

[262] Tom R. Tyler & Jeffrey Fagan, *Legitimacy and Cooperation: Why Do People Help the Police Fight Crime in Their Communities?*, 6 Ohio St. J. Crim. L. 231, 264-65 (2008); Tracey Meares, *The Legitimacy of Police Among Young African-American Men*, 92 Marq. L. Rev. 651, 657-66 (2009)

[263] Rachel Moran, *In Police We Trust*, 62 VILL. L. REV. 953, 992 (2017) ("When communities of color fear the police, believe they will receive unfair treatment, and question their legitimacy, the natural result is that they also attempt to avoid contact with the police. In many minority communities, these efforts go so far as to avoid even reporting crimes, from a fear that police officers will treat them as suspects rather than witnesses or victims--a concept foreign to most white people."); see id. ("A recent Chicago survey revealed that only 6% of African-Americans in the city believed that Chicago police officers treated everyone fairly."); *see also* Josh Bowers & Paul H. Robinson, *Perceptions of Fairness and Justice: The Shared Aims and Occasional Conflicts of Legitimacy and Moral Credibility*, 47 WAKE FOREST L. REV. 211, 229-31 (2012); Devon W. Carbado, *(E)Racing The Fourth Amendment*, 100 MICH. L. REV. 946, 952 (2002).

[264] Christopher Slobogin, *The Poverty Exception to the Fourth Amendment*, 55 FLA. L. REV. 391, 401 (2003) ("Fourth Amendment protection varies depending on the extent to which one can afford accoutrements of wealth such as a freestanding home, fences, lawns, heavy curtains, and vision- and sound-proof doors and walls.").

[265] Aziz Z. Huq, *The Consequences of Disparate Policing: Evaluating Stop and Frisk As A Modality of Urban Policing*, 101 MINN. L. REV. 2397, 2412 (2017) ("In particular, SQF [Stop, Question, Frisk] tends to be concentrated upon minority--i.e., African-American and Hispanic--neighborhoods. In New York, the district court in *Floyd* found that the racial composition of a neighborhood was a better predictor of the density of stops than its lagged crime rate.").

[266] Andrew Gelman, Jeffrey Fagan & Alex Kiss, *An Analysis of the New York City Police Department's "Stop-and-Frisk" Policy in the Context of Claims of Racial Bias*, 102 J. AM. STAT. ASS'N 813, 821 (2007) ("In the period for which we had data, the NYPD's records indicate that they were stopping blacks and Hispanics more often than whites, in comparison to both the populations of these groups and the best estimates of the rate of crimes committed by each group.").

[267] David Cole, NO EQUAL JUSTICE (2010).

present. AI systems are good at procedural fairness rules.[268] But systemic and structural inequities in society (the inputs) results in a system that will not be fair in fact or be perceived as fair (the outputs). For example, if the list of people with felony warrants was created in a way that replicates societal bias in policing priorities, then a matching system will replicate the societal bias. And, independent of the technology, the Fourth Amendment says nothing about the underlying reality and source of data. An AI system built around principles of Fourth Amendment fairness probably need not be very fair as long as it represents the unfair world around it.

Beyond unequal treatment, the Fourth Amendment also has little to say about unequal or disparate effects of policing. Policing resources have never been equally distributed across society.[269] Police respond to crime patterns, strategic assessments, and political pressure and those influences do not result in an equal distribution of police resources across a community. Some neighborhoods are over-policed and some under-policed, and in both police have been criticized as being unfair.[270] Distributive fairness has never been realized or really a priority.[271] The Fourth Amendment neither mandates equal policing resources nor freedom from policing attention.

For a facial recognition system, any unfairness in effect will not be a Fourth Amendment concern. Complaints then that facial recognition matching systems do not work equally well on different races or genders, because they are trained on datasets without sufficient diversity will not merit Fourth Amendment attention. Complaints about the placement of surveillance cameras in particular neighborhoods will not be heard. Complaints about the disproportionate number of people of color with felony arrest warrants which might skew the matching capabilities of the algorithm will not be heard. In short, fairness considerations, while important in principle are not required as a Fourth Amendment matter.

4. Transparency

[268] Machines, after all, follow the process designed by the computer engineers.

[269] Seth W. Stoughton, *The Blurred Blue Line: Reform in an Era of Public & Private Policing*, 44 AM. J. CRIM. L. 117, 149 (2017) ("Policing is widely viewed as redistributive; the communities that provide the lion's share of the tax revenue that funds public policing efforts are typically not where the majority of policing takes place. Or, to provide a more nuanced view, those communities may receive a different mix of policing services than poorer communities; more community policing and problem-oriented policing, for example, and less enforcement oriented or zero-tolerance policing."); Alexandra Natapoff, *Underenforcement*, 75 FORDHAM L. REV. 1715, 1724 (2006) (discussing the problem of under policing certain poor areas).

[270] John Cassidy, *The Statistical Debate Behind the Stop-and-Frisk Verdict*, NEW YORKER (Aug. 13, 2013), http://www.newyorker.com/news/john-cassidy/the-statistical-debate-behind-the-stop-and-frisk-verdict [https://perma.cc/FT7P-QZTZ].

[271] Joshua J. Reynolds, Victoria Estrada-Reynolds & Narina Nunez, *Development and Validation of the Attitudes Towards Police Legitimacy Scale*, 42 LAW & HUM. BEHAV. 119, 120 (2018) citations omitted) ("*Distributive fairness* is described as perceptions that people receive fair decisions (e.g., to arrest or not) and that the outcomes are distributed fairly (e.g., minorities or poor individuals are not disproportionally arrested)."

Police decision-making is decidedly not transparent.[272] At an officer level, one cannot see into the human brain to understand why an officer acted the way they did. Further, well-documented cognitive shortcomings, implicit biases, and other limitations of the human mind prevent an accurate understanding.[273] Police officers like everyone else see a distorted world without noticing the distortions.[274] While there are some *ex post* mechanisms for recording the observations of officers (police reports, testimony, recordings of body camera footage), these types of formal memorialization are limited in scope and value.[275]

As mentioned, the Supreme Court has stated that subjective reasoning of police officers is largely irrelevant for Fourth Amendment purposes.[276] In rejecting consideration of an officer's subjective motivations for stopping or arresting a suspect, the Court has signaled that it is fine leaving the actual decision-making process unexamined. The goal, instead, is to look for objective justifications for a stop, not actual reasons. And, while objective rules must be established for police, these rules do not have to control the actual decisions of police. Police officers are allowed to arrest based on a reasonable mistake of fact,[277] and a reasonable mistake of law,[278] as long as there are some objective justifications for their actions.[279]

Beyond individual human decisions, the larger context of policing is equally opaque. As a profession, policing traditionally has not been very transparent about subjects like training, experiences, or tactics.[280] More than occasionally police have been affirmatively secretive.[281] At both an operational and institutional level, local governments have avoided various

[272] Erik Luna, *Transparent Policing*, 85 IOWA L. REV. 1107, 1112 (2000) ("Hidden police abuses are at least as virulent as prosecutorial misconduct, with occasional revelations of uniformed lawlessness indicating the existence of a secret code of policing on the streets."); see also id. at 1156 ("Undemocratic opaqueness in law enforcement policy and practice … is never harmless.").

[273] Megan Quattlebaum, *Let's Get Real: Behavioral Realism, Implicit Bias, and the Reasonable Police Officer*, 14 STAN. J. CIV. RTS. & CIV. LIBERTIES 1, 10 (2018)

[274] *Id*. at 10-13.

[275] *But see* Sharad Goel et al., *Combatting Police Discrimination in the Age of Big Data*, 20 NEW CRIM. L. REV. 181 (2017) (using recorded data to understand police patterns.

[276] Kentucky v. King, 563 U.S. 452, 464 (2011) ("Our cases have repeatedly rejected a subjective approach, asking only whether the circumstances, viewed *objectively*, justify the action." (quoting Brigham City, Utah v. Stuart, 547 U.S. 398 (2006)); Whren v. United States, 517 U.S. 806, 813 (1996) ("We think these cases foreclose any argument that the constitutional reasonableness of traffic stops depends on the actual motivations of the individual officers involved.").

[277] Illinois v. Rodriguez, 497 U.S. 177, 185-86 (1990).

[278] *Heien v. North Carolina*, 135 S. Ct. 530, 537 (2014)

[279] Devenpeck v. Alford, 543 U.S. 146, 153 (2004) ("Our cases make clear that an arresting officer's state of mind (except for the facts that he knows) is irrelevant to the existence of probable cause.").

[280] Rachel Harmon, *Why Do We (Still) Lack Data on Policing?*, 96 MARQ. L. REV. 1119, 1129 (2013) ("In practice, police chiefs and other local government actors often limit rather than promote information availability. Cities and police departments sometimes actively inhibit the collection of information about police by, for example, requiring secrecy when they settle civil suits for police misconduct or discouraging citizens from filing complaints about officer conduct.")

[281] Barbara E. Armacost, *Organizational Culture and Police Misconduct*, 72 GEO. WASH. L. REV. 453, 533 (2004) ("[E]fforts by outside agencies to collect and analyze information in a potentially adversarial framework, such as a § 14141 lawsuit, may lead police officers to be defensive and uncooperative.").

transparency initiatives and have occasionally fought them.[282] When technology is added to the formula, the push for secrecy grows even stronger, as claims of proprietary systems and tactical advantage cause police to defend non-transparent strategies.[283] The result has been that the reasons for police decisions, the training standards, and protocols remain under-examined, if not completely opaque. What officers are taught about the Fourth Amendment, how they are instructed to enforce the law consistent with the Fourth Amendment, and how new technologies intersect with the Fourth Amendment are all quite unclear.

A facial recognition system built to such Fourth Amendment standards can be a true black box and still be constitutional under this thinking. The Fourth Amendment neither requires police to be transparent, nor asks for the true underlying reason for the stop (as long as there is an objective justification). So, for example, a facial recognition matching model might set forth explicit rules of how a match should occur, but if the model is actually finding another hidden correlation to make the match, this underlying correlation could not be challenged. All that has mattered to the Court has been that there was an objective justification, not the actual reason. The result would be that an objectively reasonable, but mistaken facial recognition algorithm might survive Fourth Amendment scrutiny because courts would not want to look under the hood of the model.

C. Conclusion on Error, Bias, Transparency and Fairness in Facial Recognition and the Fourth Amendment

Like the privacy problem, the Fourth Amendment offers little comfort to some of the longstanding challenges to police legitimacy. The question is why, and what can be done about it.

Examining the Fourth Amendment through the lens of facial recognition technology reveals two related insights helpful for future Fourth Amendment analysis. First, much of the Supreme Court's expansion of police power can be traced to deference to human decision-making and when decision-making is made at a programmatic or administrative level such

[282] Rachel Harmon, *Why Do We (Still) Lack Data on Policing?*, 96 Marq. L. Rev. 1119, 1133 (2013) ("[S]tates not only do little to encourage police departments to produce information about policing that does exist, they also often restrict public access to it through privacy laws and exemptions from open records statutes.").

[283] https://www.brennancenter.org/analysis/nypd-predictive-policing-documents; Ric Simmons, *Big Data, Machine Judges, and the Legitimacy of the Criminal Justice System*, 52 U.C. DAVIS L. REV. 1067, 1087 (2018) ("Unfortunately, big data algorithms are notoriously opaque and incomprehensible, sometimes even to those who are applying them. Two of the largest providers of predictive algorithms in the criminal justice system are corporations who claim that the inner workings of their software are trade secrets."); Elizabeth E. Joh, *Feeding the Machine: Policing, Crime Data, & Algorithms*, 26 WM. & MARY BILL RTS. J. 287, 293 (2017) ("An algorithm can also be a black box in another sense; the companies that create them often refuse to divulge information about them. From their developers' perspective, revealing how an algorithm works risks exposing valuable trade secret information to competitors.").

deference wanes. "Digital may be different," but "programmatic" may also be different for the Fourth Amendment (ratcheting up constitutional scrutiny). Second, while the Supreme Court seems to forgive isolated errors or pretextual biases of individual officers, the Court does not forgive recurring errors or systemically biased decisions.

These two insights are not necessarily new, as scholars like Daphna Renan, Tracey Meares, and Christopher Slobogin have all made the argument that the Fourth Amendment should be thought of in a systemic light.[284] The insights do, however, offer a way forward to theorize how the Supreme Court might address new *systems* of surveillance like facial recognition. The common theme (like with privacy) is that the more programmatically designed and systematized a policing practice becomes, the higher level of Fourth Amendment scrutiny it should receive from the Court. As facial recognition technology is literally a construct of programmatic engineering and computer design, it would receive higher Fourth Amendment scrutiny.

1. Human v. Programmatic Error/Bias

One reason why the Supreme Court seems to forgive police error and bias turns on the fact that for most of the Court's history Fourth Amendment cases were decidedly human, with police officers on the front lines of quick discretionary decisions. Police, as ordinary people get things wrong.[285] As the Court recognized in *Heien v. North Carolina*, "To be reasonable is not to be perfect, and so the Fourth Amendment allows for some mistakes on the part of government officials, giving them 'fair leeway for enforcing the law in the community's protection.'"[286] The Supreme Court has forgiven mistakes of fact[287] and mistakes of law.[288] Within this "human" forgiveness, the Supreme Court emphasizes the quickness required for immediate decisions, the complexity of human behavior and observations, and the one-

[284] Daphna Renan, *The Fourth Amendment As Administrative Governance*, 68 STAN. L. REV. 1039, 1041 (2016); *see id.* at 1042 ("While our Fourth Amendment framework is transactional, then, surveillance is increasingly *programmatic*."); Christopher Slobogin, *Policing As Administration*, 165 U. PA. L. REV. 91, 97 (2016); Tracey L. Meares, *Programming Errors: Understanding the Constitutionality of Stop-and-Frisk as a Program, Not an Incident*, 82 U. CHI. L. REV. 159, 162 (2015).

[285] *Brinegar v. United States*,338 U.S. 160, 176 (1949) ("Because many situations which confront officers in the course of executing their duties are more or less ambiguous, room must be allowed for some mistakes on their part. But the mistakes must be those of reasonable men, acting on facts leading sensibly to their conclusions of probability.")

[286] *Heien v. North Carolina*, 135 S. Ct. 530, 536 (2014)

[287] *Heien*, 135 S. Ct. at 536 ("We have recognized that searches and seizures based on mistakes of fact can be reasonable.")(*citing Illinois v. Rodriguez,* 497 U.S. 177, 183–186 (1990); *Hill v. California,* 401 U.S. 797, 802–805, 91 S.Ct. 1106, 28 L.Ed.2d 484 (1971).

[288] *Id*. ("But reasonable men make mistakes of law, too, and such mistakes are no less compatible with the concept of reasonable suspicion. … There is no reason, under the text of the Fourth Amendment or our precedents, why this same result should be acceptable when reached by way of a reasonable mistake of fact, but not when reached by way of a similarly reasonable mistake of law.).

off nature of decision-making.[289] In addition, Court forgives error because Fourth Amendment law can be technical and hard to interpret.[290]

Yet, this human deference falls away when programmatic and thus systemic Fourth Amendment violations can be shown. Generally, when police administrators organize formalized, broad investigatory measures for ordinary policing purposes, the response of the Supreme Court is critical.[291] Dragnet sweeps, road blocks, and other types of broad-based suspicion-less searches for law enforcement purposes are not favored. The reason in part is because police administrators have the ability to craft constitutionally respectful rules before implementing the plans. Absent special needs or special circumstances, the Supreme Court has been reluctant to allow systems of general suspicionless searches for ordinary law enforcement purposes.[292] The more planned the practice is, the less deferential the Court appears.[293] In the case of a designed system of facial recognition technology, any deference would seem to drop away to a fully programmatic (computer programed) system.

2. Isolated v. Recurring Error/Bias

As stated, another reason for the Supreme Court's failure to address human error and bias arises from how Fourth Amendment cases come before the courts. Suppression hearings involve individualized cases with particular facts involving particular officers. Fourth Amendment rights are decided in one-off settings where systemic or structural error is not presented.[294] The result is that in criminal cases systemic constitutional violations are not litigated and thus not seen by courts. This practice hides systemic error and allows for a less holistic understanding of police misconduct.

Yet those systemic errors exist. Through investigations and litigation, clear evidence of systemic police error, misconduct, and Fourth Amendment

[289] *Kentucky v. King*, 563 U.S. 452, 466 (2011) ("The calculus of reasonableness must embody allowance for the fact that police officers are often forced to make split-second judgments—in circumstances that are tense, uncertain, and rapidly evolving."); *Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics,* 403 U.S. 388, 418, 91 S. Ct. 1999, 2016, 29 L. Ed. 2d 619 (1971) ("Inadvertent errors of judgment that do not work any grave injustice will inevitably occur under the pressure of police work.").

[290] Wayne A. Logan, *Police Mistakes of Law,* 61 EMORY L.J. 69, 83 (2011) ("A prime justification for forgiving police mistakes of law lies in the enormous number and often-technical nature of low-level offenses that commonly serve as bases to stop and arrest individuals. The expectation that the law is "definite and knowable"[86] is no more tenable for police today than it is for the lay public.").

[291] *City of Indianapolis v. Edmond*, 531 U.S. 32, 33 (2000).

[292] Barry Friedman, UNWARRANTED: POLICING WITHOUT PERMISSION, 143-184 (2017) (explaining the difference between cause based and suspicionless searches).

[293] *Ferguson v. City of Charleston*, 532 U.S. 67, 81, 121 S. Ct. 1281, 1290, 149 L. Ed. 2d 205 (2001) ("In looking to the programmatic purpose, we consider all the available evidence in order to determine the relevant primary purpose.").

[294] *But see*, Andrew Guthrie Ferguson, *The Exclusionary Rule in the Age of Blue Data,* 72 VAND. L. REV. 561, 591 (2019) (discussing the promise of litigating systemic or recurring error through the use of new data-driven technologies).

violations have been found in cities like Chicago,[295] Baltimore,[296] Philadelphia,[297] New York City,[298] and most famously Ferguson, Missouri.[299] The Department of Justice Civil Rights Division has opened 69 investigations and entered into 40 reform agreements.[300] Since 2012, the DOJ Civil Rights Division has "opened 11 new pattern-or-practice investigations and negotiated 19 new reform agreements."[301]

In recent cases, the Justices have acknowledged that recurring problems would impact Fourth Amendment decisions, including the suppression of evidence. For example, *Herring* turned on the lack of recurring errors in the arrest warrant database.[302] Similarly, in *Utah v. Strieff,* both the majority and dissent recognized that proof of systemic violations would have impacted the analysis.[303]

In fact, the flipside of *Herring's* limits on negligent error is that intentional or reckless error and/or systemic or recurring error may yet be remedied as a Fourth Amendment violation.[304] One would hope that

[295] CIVIL RIGHTS DIV., U.S. DEP'T OF JUSTICE, INVESTIGATION OF THE CHICAGO POLICE DEPARTMENT (Jan. 13, 2017), https://www.justice.gov/opa/file/925846/download [https://perma.cc/U8W6-6C9G] [hereinafter DOJ CHICAGO REPORT].

[296] CIVIL RIGHTS DIV., U.S. DEP'T OF JUSTICE, INVESTIGATION OF THE BALTIMORE CITY POLICE DEPARTMENT 24 (Aug. 10, 2016), https://www.justice.gov/crt/file/883296/download [https://perma.cc/U4CT-49ZN]

[297] *See* Plaintiffs' First Report to Court and Master on Stop and Frisk Practices at 7, Bailey v. City of Philadelphia, No. 10-5925 (E.D. Pa. filed Nov. 4, 2010), https://www.law.columbia.edu/sites/default/files/microsites/contract-economic-organization/files/Bailey%20First%20Report_final%20version.docx [https://perma.cc/T4HB-XQR7]; *see id.* at 8:

> In sum, over the first six months of 2011, based on the 1426 75-48a forms reviewed by counsel (a larger number were reviewed by law students with similar findings), 713 pedestrian stops were made with reasonable suspicion and 713 were made without reasonable suspicion. Of 355 frisks, 165 were with reasonable suspicion and 190 without reasonable suspicion.

[298] Floyd v. City of New York, 959 F. Supp. 2d 540, 562 (S.D.N.Y. 2013) ("The City acted with deliberate indifference toward the NYPD's practice of making unconstitutional stops and conducting unconstitutional frisks."); *Id.*; *see id.* at 660 ("The NYPD's practice of making stops that lack individualized reasonable suspicion has been so pervasive and persistent as to become not only a part of the NYPD's standard operating procedure, but a fact of daily life in some New York City neighborhoods."); *Ligon v. City of New York*, 925 F. Supp. 2d 478, 492–510 (S.D.N.Y. 2013) (nine independent police stops illustrating misconduct); Davis v. City of New York, 902 F. Supp. 2d 405, 412–30 (S.D.N.Y. 2012) (seven instances of NPYD misconduct); see also Jeffrey Fagan & Amanda Geller, *Following the Script: Narratives of Suspicion in* Terry *Stops in Street Policing*, 82 U. CHI. L. REV. 51, 69 (2015).

[299] *See* CIVIL RIGHTS DIV., U.S. DEP'T of JUSTICE, INVESTIGATION OF THE FERGUSON POLICE DEPARTMENT 2–3 (Mar. 15, 2015), https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_report.pdf [https://perma.cc/W7NS-9CSB] [hereinafter DOJ FERGUSON REPORT]

[300] CIVIL RIGHTS DIV., U.S. DEP'T OF JUSTICE, THE CIVIL RIGHTS DIVISION'S PATTERN AND PRACTICE POLICE REFORM WORK: 1994-PRESENT 3 (Jan. 2017), https://www.justice.gov/crt/file/922421/download [https://perma.cc/QC3S-A792]; *see also id.* at 15 ("Of 69 total investigations since Section 14141's enactment, the Division has closed 26 investigations without making a formal finding of a pattern or practice.").

[301] *Id.* at 1.

[302] *Herring*, 555 U.S. at 146 ("In a case where systemic errors were demonstrated, it might be reckless for officers to rely on an unreliable warrant system.").

[303] *Strieff*, 136 S. Ct. at 2063 ("Moreover, there is no indication that this unlawful stop was part of any systemic or recurrent police misconduct. To the contrary, all the evidence suggests that the stop was an isolated instance of negligence that occurred in connection with a bona fide investigation of a suspected drug house.").

[304] *Herring*, 555 U.S. at 146 ("We do not suggest that all recordkeeping errors by the police are immune from the exclusionary rule. In this case, however, the conduct at issue was not so objectively culpable as to require exclusion."); *id.* ("In a case where systemic errors were demonstrated, it might be reckless for officers to rely on an unreliable warrant system.").

intentionally choosing an 80% error rate in a facial recognition system (following reasonable suspicion rules) should qualify as recklessly promoting error. And, because *Herring* is talking about remedies and not rights, it might be an even stronger case to say that a system built around 80% error violates Fourth Amendment rights. Thus, civil rights investigations, civil rights lawsuits, and empirical studies that demonstrate systemic or recurring error could be the basis of finding Fourth Amendment violations.[305] A facial recognition program that systematically or regularly makes matching errors could be the subject of constitutional challenge (or a civil rights lawsuit).

If thought of as a system of policing rules, any design choice that results in reckless errors will be constitutionally suspect. While human police error can be common and forgiving, designed structural police error might not be treated the same way.

3. A Fourth Amendment Framework for Surveillance Systems

A silver lining thus might emerge from this analysis that offers a way forward for regulating systems of surveillance. Surveillance technologies like facial recognition are by design non-human, programmatically engineered, and meant to offer recurring and systemic information to police. Someone must *ex ante* sit down and program the choices made to provide information. These technologies, thus, should sit in a different space compared to traditional human policing decisions.

If seen in this light, courts may not afford these technologies the deference traditionally given to human police decisions. If an issue of error rate, bias, or fairness can be identified in the design stage, this systems problem should result in a colorable Fourth Amendment challenge that should not be dismissed by the courts.

If, as I have argued, digital systems are different, then the cases focused on the harms of systemic or recurring error, bias, or unfairness should open the door for a different legal analysis. A litigant should be able to bring a case showing the design flaw as a Fourth Amendment problem, and escape the traditional arguments about low standards of suspicion or the irrelevance of error or pretext. For example, if the face identification system routinely fails to identify women of color in comparison to white males, a suspect who

[305] CIVIL RIGHTS DIV., U.S. DEP'T OF JUSTICE, INVESTIGATION OF THE FERGUSON POLICE DEPARTMENT 3–4 (2015), https://www.justice.gov/sites/default/files/ opa/press-releases/attachments/2015/03/04/ferguson_police_department_report.pdf.; CIVIL RIGHTS DIV., U.S. Dep't of Justice, INVESTIGATION OF THE BALTIMORE CITY POLICE DEPARTMENT 24 (Aug. 10, 2016), https://www.justice.gov/crt/file/883296/download [https://perma.cc/U4CT-49ZN]; Floyd v. City of New York, 959 F. Supp. 2d 540, 562 (S.D.N.Y. 2013) ("The City acted with deliberate indifference toward the NYPD's practice of making unconstitutional stops and conducting unconstitutional frisks."); Jeffrey Fagan & Amanda Geller, *Following the Script: Narratives of Suspicion in* Terry *Stops in Street Policing*, 82 U. CHI. L. REV. 51, 69 (2015) (providing empirical data to demonstrate violations of the Fourth and Fourteenth Amendment);

was stopped based on a face identification match should be able to challenge the stop on Fourth Amendment grounds without being limited by *Whren's* suggestion that bias is irrelevant to the Fourth Amendment.[306] Or, if the error rate were revealed, the suspect should be able to challenge the stop based on the high error rate without being precluded by the rather forgiving reasonable suspicion standard.[307] While the Fourth Amendment has not traditionally worked this way, the move to systems of pre-programmed decision-making creates a new opportunity for a new analysis. In this way, the Fourth Amendment argument could build on insights of ethical AI critics who have demanded access to the decisions and data underlying AI systems to show its limitations.

The symmetry of this systems analysis around privacy and legitimacy reinforces my claim that the Supreme Court might treat systems of mass surveillance differently than traditional policing when it comes to the Fourth Amendment. In both analyses, the fact that there are programed systemic choices being made *ex ante* changes things. In both analyses, the fact that technology restructures police power changes things. And, in both analyses, the potential scope and scale of the societal change changes things. But, as might be clear, such a theory that digital systems – like facial recognition – are different for Fourth Amendment purposes would need to be adopted by the courts. This would take time and there is no guarantee that the Supreme Court would see the systems of surveillance the same way. More practically, facial recognition technology needs to be regulated now. If the Fourth Amendment largely fails to offer protections, a legislative fix is necessary.

The next Part addresses how legislation could be drafted to fill the gaps of Fourth Amendment protection in terms of privacy, error, bias, transparency, and fairness.

IV. A Legislative Framework for Facial Recognition

This last Part details the principles that should undergird any legislation around facial recognition. The Constitution provides the floor on which legislative bodies can scaffold further protections to protect privacy and enhance legitimacy. The first section examines the legal standards that should cover the different use cases for facial recognition technology with an eye toward those uses that threaten Fourth Amendment expectations of privacy. The second section examines the necessary accountability protections that will confront issues of bias, fairness, transparency, and error.

[306] *See supra* note xx.
[307] *See supra* notes xx, xx.

A. Facial Recognition & Privacy: Legislative Principles

Following the analysis detailed in Part II, legislation should remedy the concerns raised by the different potential police uses (surveillance, identification, tracking, and verification). Proposed legislation should mirror existing Fourth Amendment principles and also fill any gaps from the acknowledged failures of the Fourth Amendment.

Central to the regulation of facial recognition are three questions: (1) should any facial recognition uses be banned outright; (2) if not banned, what level of legal justification (probable cause, reasonable suspicion, etc.) should be required to use facial recognition matches; and (3) above the constitutional floor, what if any additional protections should be required as a better way to protect privacy and ensure legitimacy. The follow discussion attempts to interweave the technologies and legal analysis discussed in Part I & II to set out principles helpful for legislative action.

1. Ban Generalized Face Surveillance

Face surveillance should be banned for all ordinary law enforcement purposes. Whether stored, real-time, or through third party image searches, building a system with the potential to arbitrarily scan and identify individuals without individualized suspicion and to discover personal information about their location, interests, or activities should simply be banned by law.[308]

The justification for such a ban derives in large part from the Fourth Amendment principles discussed earlier. This type of suspicionless, warrantless, mass surveillance system runs straight into Fourth Amendment concerns, and – depending on the scope and scale – likely would be declared unconstitutional by the Supreme Court. The combination of digital capacity, mass collection, retrospective searching, long-term aggregation, tracking, and all without any individualized or particularized suspicion should trigger significant, if not fatal Fourth Amendment scrutiny.

But the constitutional concerns extend beyond the fact that suspicionless, mass surveillance runs afoul of Fourth Amendment principles. In addition, First Amendment principles are threatened.[309] In fact, underlying the Supreme Court's recent Fourth Amendment reasoning about privacy in public is a realization that surveillance chills First Amendment protected

[308] Separate rules can be designed for non-law enforcement purposes including public safety emergencies.

[309] *See e.g.,* Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. Rev. 741, 747 (2008) ("The potential chilling effect due to relational surveillance poses serious risks not only to individual privacy, but to the First Amendment rights to freedom of association and assembly…"); Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 Am. U. L. Rev. 21, 28-29 (2013)

activity.[310] Free expression, association, petitioning for redress, and political dissent all will be negatively impacted by face surveillance systems. Police have already shown a willingness to use surveillance technologies to monitor dissenting voices,[311] and face surveillance will only strengthen that power. In addition, individual choices to live free from government observation and participate in certain social and recreational activities, religious practices, or community groups will be curbed without a way to maintain some level of public obscurity.[312] By eroding what Woodrow Hartzog and Evan Selinger term the "practical obscurity" of public activity, face surveillance raises significant First and Fourth Amendment concerns and provides ample reason to ban its use.[313] In sum, generalized face surveillance should be banned under federal law, with the only exceptions being for emergency or non-law enforcement uses.

2. Require a Probable Cause Warrant for Face Identification

Police currently use face identification without any explicit legislative oversight or constitutional check. As detailed, in Part II, while a warrant requirement is not constitutionally required, legislatures would be wise to future-proof their legislation with a heightened standard. Face identification should be regulated by a probable cause warrant requirement because of the potential for abuse, and the important due process and transparency considerations around the use of new surveillance technologies.

The main reason for this warrant requirement involves the same "digital is different" fears articulated by the Supreme Court, namely that the quantitatively and qualitatively different capabilities of digital matching requires caution and greater court oversight.[314]

The argument here is two-fold: first, because of the growing scale and aggregation of digital images and the ease of automating face identification a heightened legal standard and additional legal process should be legislatively required. Second, this probable cause standard will be relatively

[310] Alex Abdo, *Why Rely on the Fourth Amendment to Do the Work of the First?,* 127 Yale L.J. Forum 444, 445 (2017)

[311] George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, INTERCEPT (July 24, 2015, 2:50 PM), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/; Darwin BondGraham, *Counter-Terrorism Officials Helped Track Black Lives Matter Protestors*, E. BAY EXPRESS (Apr. 15, 2015), http://www.eastbayexpress.com/oakland/counter-terrorism-officials-helped-track-black-lives-matter-protesters/Content?oid=4247605.

[312] Evan Selinger & Woodrow Hartzog, *Why You Can No Longer Get Lost in the Crowd, NY TIMES* (April 17, 2019).

[313] Woodrow Hartzog, *Body Cameras and the Path to Redeem Privacy Law*, 96 N.C. L. REV. 1257, 1259 (2018); Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 388 (2013); Woodrow Hartzog & Evan Selinger, *Obscurity: A Better Way To Think About Your Data Than 'Privacy,'* ATLANTIC (Jan. 17, 2013), http:// http://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283 [https://perma.cc/FA9K-B2TQ].

[314] *See supra* note xx.

straightforward to operationalize in the face identification context. Finally, because of the potential abuse and overuse, the technology should be limited to serious felony crimes.

First, the scale of digital images available to police is simply too great to allow unregulated face identification scans. Whereas today a police officer might just match a target's face to a local jail database, the ability tomorrow to search any other database of images needs to be regulated. Even the FBI's own image database has grown to now include access to a network of more than 400 million images.[315] The simple fact is that any government-controlled database can be expanded to include any number of images bought, scraped from the web, or developed organically.

In addition, the ease brought on by automation makes these searches something different in kind than traditional photo matches. It would be a mistake to mechanically equate past human search practices with the quantitatively and qualitative different capabilities of artificial intelligence powered pattern matching systems. Just because police officers once could match a target image with a paper mugshot book does not mean that the same officers should be able to run that image against 400 million images (or billions of Internet images) without any cause. Too many innocent people are caught in that web[316] and the capacity to search these millions of innocent facts is simply too powerful without regulation.[317]

Importantly, the requirement of probable cause will prevent warrantless face identification from becoming an automated and continuous process. If police need no cause or justification to run a search of an image against their growing image datasets, they could also automate this process. The result would be that every photograph in police possession, or every photo taken through police body cameras could be uploaded to see if a face identification match occurs (with all the images permanently stored for future searches). A probable cause warrant requirement, while not mandated by the current Fourth Amendment doctrine, allows for a balance of interests that would limit the use to particular crimes and particular cases.

Second, the requirement of probable cause threshold will not be burdensome to meet in the context of face identification. In many serious felony cases police have both probable cause a crime has occurred and a suspect's photo. They wish to run the image in a particular database because they have no other leads. They have a defined purpose, a defined image dataset, and probable cause to believe that the face they are searching for will

[315] GAO Report, https://www.gao.gov/assets/680/677098.pdf

[316] Kaveh Waddell, *Half of American Adults Are in Police Facial-Recognition Databases*, The Atlantic (Oct. 19, 2016) https://www.theatlantic.com/technology/archive/2016/10/half-of-american-adults-are-in-police-facial-recognition-databases/504560/.

[317] Evan Selinger & Woodrow Hartzog, *Amazon Needs to Stop Providing Facial Recognition Tech for the Government*, *MEDIUM* (June 21, 2018).

be in the dataset. Police have solved crimes long before the ability to do dragnet like face searches and likely should be encouraged to not overly rely on the technology. If all of these things are true, they would meet the requirements of a probable cause warrant to be signed by a judge.[318]

As an added benefit, the warrant process will generate a written record allowing for a measure of transparency, accountability, and the avoidance of abuse.[319] Probable cause warrants are not simply about justifying an intrusion into personal privacy, but also about documenting the use after the fact. Written records will reveal the scale, scope, and efficacy of the programs and also allow regular auditing and accountability. Stories have already begun to emerge about the consequences of an unregulated system of face identification used to target low level crimes and immigration enforcement.[320] Finally, the warrant process will provide a record to study if any alterations were made to the searched photos or any deviations made in the process of obtaining a match, and also create a formal record suitable to be provided to prosecutors and defense counsel consistent with due process protections including potential *Brady* material.[321]

3. Ban or Require a Probable Cause-Plus Standard (akin to the Wiretap Act) for Face Tracking

Face tracking presents the most difficult legislative decision. The danger, of course, is that face tracking is just face surveillance with a particularized purpose. The technological process and surveillance power is the same, but the purpose is about finding a particular person not general monitoring.

If police are given the power to search stored video footage and real time video monitors for their human target, a grave privacy threat exists. Such a capability could be misused by government authorities and once built could even be allowed by a change in legislation. It is for this reason that many advocates have pushed for a ban on all types of face tracking that uses the face surveillance capabilities of the video camera systems.[322] Trusting

[318] Such a process has been proposed for other new digital technologies. *See* Natalie Ram et al., *Genealogy Databases and the Future of Criminal Investigation*, 360 Science 1078 (2018) (discussing a Wiretap Act like requirement for genetic databases); David Gray, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE, 255-57 (2017) (proposing a Wiretap Act like process for tracking technologies); Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 497 (2012) (discussing a Wiretap Act like process for biometrics).

[319] US Courts, Wiretap Statistics, https://www.uscourts.gov/statistics-reports/wiretap-report-2017

[320] Drew Harwell, *Police Have Used Celebrity Look-alikes, Distorted Images to Boost Facial-Recognition Results, Research Finds*, WASH. POST (May 16, 2019).

[321] Ben Conarck, *Florida Courts Could Decide How Police Use Facial Recognition Tech*, The Florida Times-Union (March 12, 2018); Aaron Mak, *Facing Facts*, Slate, (Jan. 25, 2019) https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html

[322] Evan Selinger and Woodrow Hartzog, What Happens When Employers Can Read Your Facial Expressions?, NY Times (10/17/19).

police to use a judicial process or trusting that the legislative limits will not change is not a risk they are willing to take. The arguments for this type of ban of all forms of face surveillance (generalized and particularized) are compelling and should be taken seriously.

Legislators could respect this legitimate fear and ban both face surveillance (generalized) and face tracking (targeted) using stored footage and real time cameras. This would leave police with the capabilities to search through still photograph datasets (mugshots and DMV records) with a warrant, but not turn a network of surveillance cameras into a tracking system. A probable cause requirement could still be required for those mugshot/DMV photo searches, but it would be limited to the current practice of just searching through datasets of stored face images (not city-wide video surveillance streams).

If legislatures wished to allow police face tracking capabilities, legislation should authorize use of face tracking only on a probable cause-plus standard, requiring an assertion of probable cause in a sworn affidavit, plus declarations that care was taken to minimize unintended collection of other face images, that no other investigative tools were possible, and that proper steps have been taken to document and memorialize the collection.[323] This standard (akin to a Wiretap Act warrant) would apply to all face tracking, including stored surveillance scans, real-time scans, and third party image scans. As will be discussed below, this rule fills the gaps of Fourth Amendment protection, offers significantly more protection than the constitutional floor, and also responds to the different ways digital surveillance technologies will expand in scope and scale over time.

The analogy here to the Wiretap Act is admittedly imperfect, but offers a working model for legislation.[324] Designed to address another form of valuable, but personally revealing information, the Wiretap Act provides law enforcement access to personal communications on a showing of probable cause plus a few other requirements.[325]

[323] David Gray, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE, 255-57 (2017).

[324] The suggestion is also not new. *See e.g.,* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 14 (2004) (describing the history of the Wiretap Act and how it can be adapted to new technologies); *see also* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 491 (2012); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 2 (2007); Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1280 (2004).

[325] 18 USC § 2518 reads in relevant part:

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify--

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

The Wiretap Act is built around several limitations. First, it is limited to specific enumerated crimes, most of which are serious felonies. Second, the Act itself has four requirements: (1) probable cause that a crime has been committed, (2) a minimization requirement to avoid unnecessary collection, (3) a declaration that other means of investigation have been exhausted, and (4) a particularized statement about the length of time and type of communication sought. Notably, this process has been used without significant complaint for decades by investigators and the courts in the context of communications evidence.

In the facial recognition context, a parallel process should be relatively easy because all that would be required is a showing of probable cause that a serious crime had been committed, a declaration that the face tracking search was necessary because there were no other ways to obtain an identification, a statement about how other images of innocent people would be minimized (images deleted), and the reason why police thought the target's image would be in the particular dataset. Like the Wiretap Act, this process could be formalized and standardized (but also limited to only certain more serious types of crime (maybe even limited to violent crime).

For some forms of targeted face tracking (stored footage scans, third-party images scans with metadata), this type of probable cause plus standard is not only preferable, but likely constitutionally necessary to survive a Fourth Amendment challenge. If the Supreme Court is going to require a probable cause warrant for systems of surveillance like cell-site data that can reveal location, patterns, interests, and identity, some forms of facial recognition matching should be regulated by an appropriately high constitutional standard (probable cause or probable cause-plus).

4. Limit Face Verification to International Border Crossings

Government face verification may actually be the hardest technology to regulate as it has the potential to be the most ubiquitous. From Apple iPhone log-ins, to the tests of face verification on the international border, the ability to substitute face verification for the myriad security checkpoints encountered as we travel, enter government buildings, conduct financial transactions, or enter other secure spaces will be quite tempting.[326]

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

18 U.S.C.A. § 2518(4) (West 2019)

[326] Jagdish Chandra Joshi and K K Gupta, *Face Recognition Technology: A Review*, 1 THE IUP JOURNAL OF TELECOMMUNICATIONS, 53, 58 (2016) (describing uses such as "electoral registration, banking, electronic commerce, identifying newborn babies, establishing national IDs, passports, driving licenses, employee IDs and so

As this is an article largely focused on domestic law enforcement use of facial recognition, the regulation of face verification is slightly misaligned, but related dangers remain. For example, in jurisdictions that have "stop and identify" statutes on the books which allow police to ask for identification after they have made a stop based on reasonable suspicion,[327] one could imagine that face verification could be used to confirm identity. In addition, as the dissenting Justices acknowledged in *Utah v. Strieff*, police have been known to use warrant checks as a pretext to stop individuals.[328] With face verification this warrant-check justification could lead to the use/abuse of facial recognition technology in pedestrian stops or car stops. Similarly, narcotics interdiction stops on busses and trains have become a routine practice.[329] The request to see identification and match it to a bus or train ticket could also now include a face verification match. Finally, one could imagine a facial recognition system in a police station to confirm identity in a routine booking situation.[330]

While none of these uses is all that different from what a human police officer can do, it also muddies the line between face identification and face verification. Police could simply assert they are doing face verification during a traffic stop when in truth they are attempting a warrantless face identification process. It is for this reason that legislation should also address the potential abuse of face verification. Face verification should be banned from ordinary domestic law enforcement. If there is a need to make a face match, then police can use the face identification procedures of a probable cause-plus warrant. If not, they should not have routine warrantless access to the technology.

The only exception might be on the international border where the interests of the government are the strongest,[331] the Fourth Amendment has little purchase,[332] and individuals are already presenting themselves with

on.").

[327] *Hiibel v. Sixth Judicial Dist. Court of Nevada, Humboldt Cty.*, 542 U.S. 177, 182 (2004)

[328] *Strieff*, 136 S. Ct. at 2068 (Sotomayor, J. dissenting) ("The States and Federal Government maintain databases with over 7.8 million outstanding warrants, the vast majority of which appear to be for minor offenses. … The county in this case has had a "backlog" of such warrants. … Justice Department investigations across the country have illustrated how these astounding numbers of warrants can be used by police to stop people without cause."); *see also Utah v. Strieff*, 136 S. Ct. 2056, 2073 (2016) (Kagan, J. dissenting) ("In other words, the department's standard detention procedures—stop, ask for identification, run a check—are partly designed to find outstanding warrants. And find them they will, given the staggering number of such warrants on the books.").

[329] *United States v. Drayton*, 536 U.S. 194, 197 (2002)

[330] *Maryland v. King*, 569 U.S. 435, 449 (2013)

[331] *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) ("Consistently, therefore, with Congress' power to protect the Nation by stopping and examining persons entering this country, the Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior. Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant and first-class mail may be opened without a warrant on less than probable cause.").

[332] Paul S. Rosenzweig, *Functional Equivalents of the Border, Sovereignty, and the Fourth Amendment*, 52 U. CHI. L. REV. 1119 (1985) ("The fourth amendment's restrictions on searches do not apply at the nation's borders. Law enforcement agents may search any individual entering the country even without a warrant or a showing of probable cause.").

government issued identification to prove identity. As currently designed the face verification systems on the border conduct a binary match of the passport photograph on file and a digital photo of the person presenting herself. After the match, the digital image is destroyed. While entry and exit records are maintained, the face image taken is not. Such a limited use could be allowed through carefully crafted legislation that would allow face verification in situations at international borders.

5. Require Accountability around Error, Bias, Transparency, Fairness

Legislation can also address the Fourth Amendment's inability to confront the legitimacy questions around how well facial recognition works or how it will be used. Legislation can be drafted to strengthen the weaknesses around accuracy, bias, fairness, and transparency.

To address issues of error rates, legislation can require testing, auditing, and third-party certification requirements. For example, as a precondition to utilizing facial recognition, police (or the technology companies) could be required to reveal results from testing about error rates. Such auditing should occur in product development and by independent researchers.[333] Similarly, after adoption, auditing measures to continue to test the technology could be required.[334] The auditing could focus on accuracy and error rates, and also how the technology was used in actual practice. Such audits will both offer a measure of practical accountability to prevent misuse, but also ensure that the technology is improving in accuracy and precision.[335]

To address concerns about bias, certification and auditing could include testing to track how facial recognition is used on people different races, ethnicities, genders, ages, or other demographic characteristics. Of particular importance is to reveal the training data and on-going data being fed into the system. One way to avoid past instances of biased data systems is to pay close attention to the types of data going into the system to train the system. Systems that cannot show through audits that the technology avoids bias should not be adopted.

In addition, legislation could require public reporting about how facial

[333] 78 Concerned Researchers, *On Recent Research Auditing Commercial Facial Analysis Technology*, Medium (Mar. 26, 2019) https://medium.com/@bu64dcjrytwitb8/on-recent-research-auditing-commercial-facial-analysis-technology-19148bda1832

[334] *See* U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 10-32 (May 2016), http://www.gao.gov/assets/680/677098.pdf (discussing the need for auditing). See also Testimony Before the Committee on Oversight and Reform, House of Representatives, FACE RECOGNITION TECHNOLOGY DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains. Statement of Gretta L. Goodwin, Director Homeland Security and Justice (June 4, 2019)https://www.gao.gov/assets/700/699489.pdf

[335] Inioluwa Deborah Raji & Joy Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products,* Association for the Advancement of Artificial Intelligence (2019).

recognition technologies are deployed. While surveillance technology tools, themselves, do not automatically raise discrimination concerns, if past is prologue the use of the technology will impact poor communities and communities of color more than other groups.[336] The history of policing in America supports an acute awareness of technology has been weaponized as mechanism of social control.[337] There is little reason to think that the development of face surveillance technology will be different than past uses of surveillance technology. Early adopters have targeted poor urban areas and communities of color.[338] The choices of where the cameras are placed, which datasets are used, how they are used, and who is targeted must be publicly reported in order to avoid implicit or explicit discriminatory uses.

Fairness is a hard concept to legislate because the initial fairness choices will all be baked into the design. The choices about how to deploy the technology are also harder to legislate, as they will be local choices and based around police necessity. But some forms of fairness can be legislated such as giving fair notice about the use of the technology before deployment and reporting on any inequities in use. In addition, enforcement provisions to ensure fairness can be included in legislation. Civil remedies, administrative remedies, and damages can all be included as a mechanism to check abuses.

Most importantly in terms of fairness, legislatures should ensure that due process protections are protected for criminal defendants.[339] Facial recognition produces matches that vary in accuracy and certainty thresholds. Some matches might be considered 99% accurate and some 27%, and the parties should know the difference. If the system returns 20 matches for a probe photograph in ranked order of certainty, the other photographs should be preserved as possible impeachment evidence. The images may be exculpatory, may impeach a witness, may undermine the government's investigation of the case, or might reveal an error in the software matching system itself. In the interest of fairness, these other photos and underlying system data need to be preserved, and if appropriate turned over as *Brady* material.

Finally, transparency concerns can be built in akin to the Wiretap Act which includes an annual public report of the types of warrants requested and

[336] Alvaro M. Bedoya, *The Color of Surveillance*, SLATE (Jan. 18, 2016), http://www.slate.com/articles/technology/future_tense/2016/01/what_the_fbi_s_surveillance_of_martin_luther_king_says_about_modern_spying.html; Dorothy Roberts & Jeffrey Vagle, *Racial Surveillance Has a Long History*, Hill (Jan. 4, 2016), http://thehill.com/opinion/op-ed/264710-racial-surveillance-has-a-long-history.

[337] *See* Alex Vitale, THE END OF POLICING (2017); Paul Butler, CHOKEHOLD: POLICING BLACK MEN, 59–61 (2017); Angela Davis, POLICING THE BLACK MAN: ARREST, PROSECUTION, AND IMPRISONMENT, 178–233 (Angela J. Davis ed., 2017).

[338] Clare Garvie & Laura Moy, *America Under Watch* (May 2019), https://www.americaunderwatch.com/.

[339] Jack Karp, Facial Recognition Software Sparks Transparency Battle, Law360.com (11/3/19); Jason Tashea, As Facial Recognition Software Becomes more Ubiquitous, Some Governments Slam on the Brakes, ABA Journal (9/24/19); Aaron Mak, Facing Facts, Slate (1/25/19).

issued.[340] A public report of how facial recognition was used, in what types of cases, by whom, and the results can be required by statute.[341] In combination with the auditing provision that recertify and protect against error and bias, these types of reporting requirements can generate a measure of public trust.

These ideas help ground a legislative framework to respond to the failures of the Fourth Amendment and take seriously the privacy and legitimacy concerns of the technology that might undermine it.

CONCLUSION

Surveillance technologies like facial recognition can monitor movements, transactions, families, and watch the religious and democratic habits of its populace raising serious liberty concerns. Even when not directed by police officers, omnipresent digital surveillance undermines human privacy and threatens personal liberty.

The harms associated with this type of surveillance are political, personal and corporal. Constant public surveillance chills associational freedom, inhibits expression, and undermines the freedom to protest or petition for redress.[342] The ability to carve out a private life, independent of government watchers is fundamental to modern American life.[343] Finally, the harm can be quite physical as surveillance can lead to police contact and control. The social control powers of surveillance do not always remain virtual but can have real world impacts, especially with those individuals with less political power and in already over policed communities.

Because of these dangers, facial recognition must be regulated by legislative action. As discussed throughout this article the Fourth Amendment largely fails to protect core issues of privacy, and ignores fundamental problems of error, bias, opacity, and unfairness. The framework set forth in this Article offers a compromise that acknowledges that not all facial recognition technology is the same, but that all such surveillance requires oversight and accountability. Legislative action is required to ensure that the liberty interests threatened by facial recognition remain secure.

[340] The Wiretap Act audits are all publicly available on a government website. *See* https://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports

[341] *Id*.

[342] Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 434 (2008) ("Government surveillance—even the mere possibility of interested watching by the state—chills and warps the exercise of this interest. This effect was understood by the drafters of the Fourth Amendment, who grasped the relationship between preventing government searches of papers and protecting religious and political dissent.").

[343] Woodrow Hartzog & Evan Selinger, *Obscurity: A Better Way To Think About Your Data Than 'Privacy,'* ATLANTIC (Jan. 17, 2013), http:// http://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283 [https://perma.cc/FA9K-B2TQ].