2021

Facial Recognition and the Fourth Amendment

Andrew Guthrie Ferguson

Article

Facial Recognition and the Fourth Amendment

Andrew Guthrie Ferguson†

Introduction 1106
I. Facial Recognition Technology 1109
A. The Technology 1110
B. Police Use of Facial Recognition Technology 1115
1. Face Surveillance 1116
2. Face Identification 1119
3. Face Tracking 1122
4. Non-Law Enforcement Purposes 1124
II. The Fourth Amendment and the Privacy Problem of Facial Recognition 1126
A. Pre-Digital Face Searches 1127
B. Future-Proofing the Fourth Amendment: A Theory 1129
1. Anti-Equivalence Principle 1132
2. Anti-Aggregation Principle 1134
3. Anti-Permanence Principle 1135
4. Anti-Tracking Principle 1136
5. Anti-Arbitrariness Principle 1137
6. Anti-Permeating Surveillance Principle 1139
7. Systems of Surveillance 1140
C. Analysis: How the Fourth Amendment Fits Facial Recognition Surveillance Technology 1141
1. Face Surveillance 1142
2. Face Identification 1150
3. Face Tracking 1152

† Professor of Law, American University Washington College of Law. Thank you to Professors 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 to Professor Andrew Selbst for providing the insight about how *Carpenter* forces a conversation about broad versus deep surveillance technologies. Thank you also to the ABA/AALS Criminal Justice Scholars workshop for terrific feedback.

4. Non-Law Enforcement Purposes 1161
D. Conclusion: Facial Recognition and a Continuum of Systemic Searches 1164
III. The Fourth Amendment and the Legitimacy Problem of Facial Recognition 1164
A. Ethical AI and Concerns About Error, Bias, Fairness, and Transparency 1167
B. The Fourth Amendment and Error, Bias, Transparency, and Fairness 1173
1. Error and Policing 1173
2. Bias 1181
3. Fairness 1185
4. Transparency 1188
C. Conclusion on Error, Bias, Transparency, and Fairness in Facial Recognition and the Fourth Amendment 1191
1. Human v. Programmatic Error/Bias 1191
2. Isolated v. Recurring Error/Bias 1193
3. A Fourth Amendment Framework for Surveillance Systems 1195
IV. A Legislative Framework for Facial Recognition 1197
A. Facial Recognition & Privacy: Legislative Principles 1197
1. Ban Generalized Face Surveillance 1197
2. Require a Probable Cause Warrant for Face Identification 1199
3. Ban or Require a Probable Cause-Plus Standard (akin to the Wiretap Act) for Face Tracking 1202
4. Limit Face Verification to International Border Crossings 1205
5. Require Accountability Around Error, Bias, Fairness, and Transparency 1207
Conclusion 1210

INTRODUCTION

Artificial intelligence systems are edging into policing.[1] Massive troves of sensor data, unstructured video surveillance feeds, and many other digital clues allow artificial intelligence to make sense of

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, 15–16 (2016).

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

2. *See generally* ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017).

3. CLARE GARVIE, ALVARO M. BEDOYA & JONATHAN FRANKLE, GEORGETOWN L. CTR. ON PRIV. & TECH., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 1 (2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf [https://perma.cc/S48P-PL53].

4. *See, e.g.*, Declan McCullagh, *Call It Super Bowl Face Scan I*, WIRED (Feb. 2, 2001), https://www.wired.com/politics/law/news/2001/02/41571 [https://perma.cc/BS67-UJVA]; 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/7GHK-UDZH]; Benjamin Powers, *Eyes over Baltimore: How Police Use Military Technology To Secretly Track You*, ROLLING STONE (Jan. 6, 2017), https://www.rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885 [https://perma.cc/F3RK-CDCK].

5. John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 134 (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*, 7 INFO. TECH. & PEOPLE 6, 34 (1994))); *see also* Malkia Devich-Cyril, *Defund Facial Recognition*, ATLANTIC (July 5, 2020), https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771 [https://perma.cc/9P29-JD63].

6. U.S. CONST. amend. IV.

technology. But current doctrine and constitutional theory offer 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.[7] Issues of error, bias, unfairness, and opacity in policing more generally become magnified when trying to design a new surveillance system for law enforcement.[8]

Understanding the limitations of the Fourth Amendment in the face of new law enforcement technology is important for three independent reasons. First, analysis shows that the Fourth Amendment will not save us from the privacy threat created by facial recognition surveillance.[9] The Supreme Court's recent Fourth Amendment jurisprudence only goes so far, leaving significant privacy gaps to fill.[10] Second, the planned designs for facial recognition systems raise core police legitimacy issues around error rates, racial bias, fairness, and transparency, and the current Fourth Amendment largely ignores these issues.[11] 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.[12]

Part I of this Article describes how facial recognition technology will be used by police. This Part looks at the surveillance capabilities of the technology as well as how police might use different versions to conduct face surveillance, tracking, 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.[13] The discussion reveals the gaps in

7. *See infra* Part III.
8. *See infra* Part III.
9. *See infra* Part II.
10. *See* Carpenter v. United States, 138 S. Ct. 2206 (2018); Riley v. California, 573 U.S. 373 (2014); United States v. Jones, 565 U.S. 400 (2012).
11. *See infra* Part III.A.
12. *See infra* Part IV.
13. *See infra* Part II.A.

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 proposes a legislative framework to regulate facial recognition in a manner consistent with existing Fourth Amendment law. This Part examines the core principles that any legislative response to facial recognition should include—principles that prohibit law enforcement access to some face surveillance and tracking technology, tighten the legal protections for access to face identification 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 that 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.[14] 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.[15] To work, a computer

14. *See, e.g.*, Matt Cagle & Nicole A. Ozer, *Amazon Teams Up with Law Enforcement To Deploy Dangerous New Face Recognition Technology*, ACLU 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 [https://perma.cc/T64R-SS94]; GARVIE ET AL., *supra* note 3.

15. 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

program is run on existing digital photographs or video surveillance cameras turning images into a digital network of identifiable objects and faces.[16] 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.[17] In practice, digital images of faces are broken down into identifiable component parts.[18] Traditionally, facial recognition technology has been "feature-based," which utilizes identifying measures like one's eyes, nose, and mouth and the distances between these features,[19] or "appearance-

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].

16. JOY BUOLAMWINI, VICENTE ORDÓÑEZ, JAMIE MORGENSTERN & ERIK LEARNED-MILLER, FACIAL RECOGNITION TECHNOLOGIES: A PRIMER 8–13 (2020), https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTs PrimerMay2020.pdf [https://perma.cc/X8CH-JAV3].

17. 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.

18. *See* Note, *In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 HARV. L. REV. 1870, 1871 n.14 (2007).

19. Jagdish Chandra Joshi & K.K. Gupta, *Face Recognition Technology: A Review*, 8 IUP J. TELECOMMS. 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 J. MECHATRONICS & 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, Simi Angelic Shavit & Thaier Hayajneh, *A Review of Facial Biometrics Security for Smart Devices*, 7 MDPI COMPUTS. 37, at 3 (2018) ("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.").

based," which attempts to match the whole face image.[20] In recent years, other forms of identification have emerged that look at skin textures,[21] shadows,[22] three-dimensional models,[23] or some combination of all of these types.[24]

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.[25] 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."[26] These digitized images are stored in large datasets so that a computer model can train itself on what constitutes a match.[27] In many systems, returned matches involve more than one image and may involve as many as twenty to fifty similar faceprints.[28] These face images are provided in order of the closeness of an overlap of the fixed digital features. So, for example, a police

20. Joshi & Gupta, *supra* note 19, at 53–54 ("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."); Petrescu, *supra* note 19, at 240 ("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.").

21. Petrescu, *supra* note 19, at 241 ("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.").

22. Galterio et al., *supra* note 19, 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.").

23. Petrescu, *supra* note 19, at 240–41 ("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.").

24. Petrescu, *supra* note 19, at 241.

25. *See generally* Levashov, *supra* note 15.

26. *See* BUOLAMWINI ET AL., *supra* note 16, at 10–14.

27. *See* GARVIE ET AL., *supra* note 3, at 9 (describing how face recognition algorithms train themselves to identify matches).

28. *See* BUOLAMWINI ET AL., *supra* note 16, at 12 (describing how faceprints with a similarity score higher than a set threshold are considered matches).

officer who seeks a match for a probe photograph of a suspect may receive twenty to fifty faceprints back as possible matches.[29]

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.[30] After the system returns a list of matching faceprints, an analyst will review the images to select a final suspect for investigation (if any).[31]

Facial recognition technology comes in different forms and can be used for different purposes.[32] As will be discussed in more detail below, one use is *face surveillance* which involves the generalized mass identification of individuals using face matching technology.[33] Face surveillance has been used in China as a means to identify people on busy streets or in train stations.[34] 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).[35] Face identification is being piloted by police as a revolutionary

29. GARVIE ET AL., *supra* note 3, at 9 ("Most police face recognition systems will output either the top few most similar photos or all photos above a certain similarity threshold.").

30. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 3–4 (2015), http://www.gao.gov/assets/680/671764.pdf [https://perma.cc/U9GG-J7NS].

31. Teresa Wiltz, *Facial Recognition Software Prompts Privacy, Racism Concerns in Cities and States*, PEW STATELINE (Aug. 9, 2019), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2019/08/09/facial-recognition-software-prompts-privacy-racism-concerns-in-cities-and-states [https://perma.cc/4RJU-CV88] ("[A]fter the software identifies a possible match, two analysts trained in biometrics by the FBI study the photograph.").

32. *See* Galterio et al., *supra* note 19, at 3–4 (describing the different forms of facial recognition technology and the purposes for which it can be used).

33. "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.

34. Simon Denyer, *China's Watchful Eye: Beijing Bets on Facial Recognition in a Big Drive for Total Surveillance*, WASH. POST (Jan. 7, 2018), https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance [https://perma.cc/YT62-RXTC]; Josh Chin, *Chinese Police Add Facial-Recognition Glasses to Surveillance Arsenal,* WALL ST. J. (Feb. 7, 2018, 6:52 AM), https://www.wsj.com/articles/chinese-police-go-robocop-with-facial-recognition-glasses-1518004353 [https://perma.cc/9J3S-VKFG].

35. 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 [https://perma.cc/U2F3-LT4T] ("Facial identification . . . involves trying to match a face to a person of interest in an existing database of faces.").

investigative tool akin to DNA matching[36] and is also being piloted in some commercial venues to enhance private security.[37] Third, there is *face tracking*, which is a hybrid of face surveillance and face identification.[38] Face tracking involves police use of stored or real time video to track a targeted suspect.[39] For example, after a bank robbery, police could search city video feeds to find the path of the fleeing suspect.[40] The main difference between face tracking and face identification is that face tracking provides locational information about the suspect. Finally, there is *face verification*, which involves confirming that a particular human face present before the camera matches a preset digital image of that face.[41] Face verification is already being piloted at international borders to confirm identity with stored passport photographs[42] and in airports to replace airplane boarding passes.[43]

36. *See, e.g.*, Asha Barbaschow, *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/L9RY-NE3F].

37. *See, e.g.*, Lisa Respers France, *Taylor Swift Reportedly Used Facial Recognition to Try to ID Stalkers*, CNN (Dec. 13, 2018), https://www.cnn.com/2018/12/13/entertainment/taylor-swift-facial-recognition/index.html [https://perma.cc/F9PW-NMQ3].

38. I am using the term "face tracking" in the context of facial recognition to distinguish it from generalized surveillance and identification. Tracking allows locational data to be uncovered as a result of a facial recognition match.

39. *See* GARVIE ET AL., *supra* note 3, at 12 (describing how facial recognition programs can compare faceprints to live video feeds).

40. *See id.*

41. Buolamwini, *supra* note 35 ("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.").

42. Mallory Locklear, *DHS Will Use Facial Recognition To Scan Travelers at the Border*, ENGADGET (June 5, 2018), https://www.engadget.com/2018/06/05/dhs-facial-recognition-scan-travelers-at-border [https://perma.cc/V4E8-7N7M]; Petrescu, *supra* note 19, at 238 ("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.").

43. Lori Aratani, *Your Face Is Your Boarding Pass at This Airport*, WASH. POST (Dec. 4, 2018, 1:25 PM), https://www.washingtonpost.com/nation/2018/12/04/your-face-is-your-boarding-pass-this-airport [https://perma.cc/9WW3-ZEG4] ("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.").

Of the four types of facial recognition, *face verification* tends to be the 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.[44] 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).[45] On the other hand, *face identification* requires searching through thousands (or millions) of images for the appropriate match and finding the "best" match.[46] 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.[47] *Face surveillance* and *face tracking* are the most complicated to 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.[48] Issues of age, race, clothing, facial hair, hair style, hats and other accessories all can impact the accuracy of the identification done at scale.[49]

44. Eisa Anis Ishrat Ullah & M. Akheela Khanum, *A Comparative Study of Facial Recognition Systems*, 9 INT'L J. ADVANCED RSCH. COMPUT. SCI. (SPECIAL ISSUE NO. 2) 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.").

45. Marcy Mason, *Biometric Breakthrough: How CBP Is Meeting Its Mandate and Keeping America Safe*, U.S. CUSTOMS & BORDER PROT., https://www.cbp.gov/frontline/cbp-biometric-testing [https://perma.cc/GZM6-KJ2Y] (stating that when a passenger has their picture taken, it is compared to "his or her gallery of photos").

46. *See* Drew Harwell, *Oregon Became a Testing Ground for Amazon's Facial-Recognition Policing. But What if Rekognition Gets It Wrong?*, WASH. POST (Apr. 30, 2019, 4:19 PM) https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police [https://perma.cc/LA3C-JD8K] (describing how police departments use facial-recognition algorithms to search through hundreds of thousands of images to find a match).

47. *See* Levashov, *supra* note 15, at 169 (stating that "[e]ven slight changes, like adding makeup," can make finding a match difficult).

48. Ullah & Akheela Khanum, *supra* note 44 ("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.").

49. BUOLAMWINI ET AL., *supra* note 16, at 12 ("Variations in many factors, such as hairstyle, camera angle, image resolution, lighting, and make-up, can all have significant impacts on faceprints, resulting in the faceprints of a single individual having significant variability.").

To work as intended, facial recognition needs at least two sets of images:[50] a photograph or collection of known faces digitized to their faceprint and a second digital dataset to match those faceprints against.[51] The set of faceprints can come from still images (e.g., driver's license photos, mugshot photos, Facebook photos), and once digitized can be matched to other still photos or live or stored video stream (e.g., surveillance cameras, police-worn body cameras, private surveillance cameras).[52] 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.[53]

B. POLICE USE OF FACIAL RECOGNITION TECHNOLOGY

Facial recognition surveillance technology is a tool that has many possible uses for law enforcement.[54] 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.[55] Each potential use raises different Fourth Amendment questions. This Section provides a brief overview of the types of facial recognition technology that will be of most interest to law enforcement.[56]

---

50. *See* BUOLAMWINI ET AL., *supra* note 16.

51. *See id.*

52. GARVIE ET AL., *supra* note 3, at 10–12.

53. *Police Unlock AI's Potential To Monitor, Surveil and Solve Crimes*, WALL ST. J. VIDEO (May 30, 2019, 5:30 AM), https://www.wsj.com/video/police-unlock-ai-potential-to-monitor-surveil-and-solve-crimes/819D5F78-22BC-4A41-9517AE31BE3C5E7E.html [https://perma.cc/HX8A-ZJ5J] (showing how police departments employ face-recognition technology).

54. Galterio et al., *supra* note 19 ("Using facial recognition software for surveillance purposes would assist government authorities in locating certain criminals, extremists, and missing children."); Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019, 2:54 PM), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches [https://perma.cc/KDM2-6YJQ].

55. Nila Bala & Caleb Watney, *What Are the Proper Limits on Police Use of Facial Recognition?*, BROOKINGS INST. (June 20, 2019), https://www.brookings.edu/blog/techtank/2019/06/20/what-are-the-proper-limits-on-police-use-of-facial-recognition [https://perma.cc/2HGB-BFRY]; Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020) https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html [https://perma.cc/3UXM-3E5W].

56. Some portions of this Article were originally written as testimony to the House Oversight Committee on how best to regulate facial recognition technologies. *See Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties:*

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.[57] Police could use "face surveillance" in three ways: (1) scanning stored video footage to identify all faces in the stored data; (2) real-time scanning of video surveillance to identify all faces passing by the cameras; and (3) 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 video footage from networked surveillance cameras.[58] Imagine the ability to sort through stored digital video surveillance to identify particular people as they travel through public streets or on public transportation.[59] These cameras can be government-owned, private, or from mobile devices such as police-worn body cameras.[60] As digital

Hearing Before the H. Comm. on Oversight & Reform, 115th Cong. (2019) (written testimony of Professor Andrew Guthrie Ferguson), https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-FergusonA-20190522.pdf [https://perma.cc/L8YX-Q4UM].

57. *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.").

58. *See* Clare Garvie & Laura Moy, *America Under Watch: Face Surveillance in the United States*, GEO. CTR. ON PRIV. & TECH.: AM. UNDER WATCH (May 16, 2019), https://www.americaunderwatch.com [https://perma.cc/P6RF-56EB] (describing how various police departments use a network of surveillance cameras to conduct face surveillance).

59. *See* Allie Gross, *Experts: Duggan's Denial of Facial Recognition Software Hinges on 3 Words*, DET. FREE PRESS (July 16, 2019, 12:24 PM), https://www.freep.com/story/news/local/michigan/detroit/2019/07/16/duggan-war-of-words-surveillance-tech/1701604001 [https://perma.cc/9N2H-U7HW] (describing how the Detroit Police Department's facial recognition technology takes still images from videos to find a match).

60. *See* Chris Burt, *Motorola Could Offer Facial Recognition with Police Body Cameras with WatchGuard Acquisition*, BIOMETRIC UPDATE (July 23, 2019), https://www.biometricupdate.com/201907/motorola-could-offer-facial-recognition-with-police-body-cameras-with-watchguard-acquisition [https://perma.cc/6RQG-EHGP]. *But see* Madeline Purdue, *Axon Body-Camera Supplier Will Not Use Facial Recognition in Its Products – For Now*, USA TODAY (July 1, 2019, 2:17 PM), https://www.usatoday.com/

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.[61] 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.[62] 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.[63]

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.[64] Imagine a TV monitor of a city street with every human figure digitally framed by a box around his/her/their face. As they pass by cameras, personal information displays because the surveillance system has matched a prepopulated faceprint to their real-time presence.[65] Again, in this type of monitoring there is no individualized suspicion of criminal wrongdoing. Generally, the justification for use is a form of public safety or social control, for example, to identify all of the people

story/tech/2019/07/01/axon-rejects-facial-recognition-software-body-cameras-now/1601789001 [https://perma.cc/324C-AALN].

61. *Police Unlock AI's Potential To Monitor, Surveil and Solve Crimes*, *supra* note 53.

62. Garvie & Moy, *supra* note 58 ("With such a system, all people caught on camera . . . are scanned, their faces compared against the face recognition database on file.").

63. *Id.* ("If deployed pervasively, real-time video surveillance threatens to create a world where, once you set foot outside, the government can track your every move.").

64. *See* Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. To Profile a Minority*, N.Y. TIMES (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html [https://perma.cc/Z9QR-PG6F]; *Chinese Man Caught by Facial Recognition at Pop Concert*, BBC NEWS (Apr. 13, 2018), https://www.bbc.com/news/world-asia-china-43751276 [https://perma.cc/9DFT-5H3C].

65. Paul Mozur, *Inside China's Dystopian Dreams, A.I. Shame and Lots of Cameras*, N.Y. TIMES (July 8, 2018), https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html [https://perma.cc/8J37-2NEK] ("China has an estimated 200 million surveillance cameras.").

jaywalking,[66] or frequenting a sporting event, or entering a gun show.[67] 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.[68] Acquiring those images and matching them would allow law enforcement to build dossiers of individuals in a community.[69] Again, this type of face surveillance match would not be done for a particularized law enforcement purpose but rather to gather intelligence about individuals in the community.[70] The resulting identifications could involve locational details (both in metadata of the photos and from the context or content of the photos themselves), personal connections, likes, interests, and

66. Christina Zhao, *Jaywalking in China: Facial Recognition Surveillance Will Soon Fine Citizens via Text Message*, NEWSWEEK (Mar. 27, 2018, 9:34 AM), https://www.newsweek.com/jaywalking-china-facial-recognition-surveillance-will-soon-fine-citizens-text-861401 [https://perma.cc/H99T-NZAZ].

67. *See generally* Chris Burt, *NEC Facial Biometrics to Be Deployed for Rugby World Cup and Busiest International Airport in Japan*, BIOMETRIC UPDATE (Nov. 7, 2018), https://www.biometricupdate.com/201811/nec-facial-biometric-to-be-deployed-for-rugby-world-cup-and-busiest-international-airport-in-japan [https://perma.cc/VAJ9-Z236]; Dave Gershgorn, *Carnival Cruises, Delta, and 70 Countries Use a Facial Recognition Company You've Never Heard of*, MEDIUM: ONEZERO (Feb. 18, 2020), https://onezero.medium.com/nec-is-the-most-important-facial-recognition-company-you've-never-heard-of-12381d530510 [https://perma.cc/6BDD-E8WJ].

68. *See, e.g.*, Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Feb. 10, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/G895-W3LJ] (describing a facial recognition app reportedly supported by three billion images from Facebook, YouTube, and other websites); Petrescu, *supra* note 19, at 242 (describing a "deep learning facial recognition system created by a Facebook research group" trained on four million Facebook photos that is said to be "97% correct").

69. Heather Kelly & Rachel Lerman, *America Is Awash in Cameras, a Double-Edged Sword for Protesters and Police*, WASH. POST (June 3, 2020, 6:00 AM), https://www.washingtonpost.com/technology/2020/06/03/cameras-surveillance-police-protesters [https://perma.cc/F4GX-XDBJ]; Aaron Boyd, *ICE Outlines How Investigators Rely on Third-Party Facial Recognition Services*, NEXTGOV (June 2, 2020), https://www.nextgov.com/emerging-tech/2020/06/ice-outlines-how-investigators-rely-third-party-facial-recognition-services/165846 [https://perma.cc/SL4J-DHUK].

70. *Cf. Map: Social Media Monitoring by Police Departments, Cities, and Counties*, BRENNAN CTR. FOR JUST. (July 10, 2019), https://www.brennancenter.org/analysis/map-social-media-monitoring-police-departments-cities-and-counties [https://perma.cc/TC22-49A3] (describing how law enforcement has used social media monitoring software to monitor protests).

activities.[71] For example, the latest fabulous photo of your family beach vacation not only shows your family, associations, and activities, but also the day, time, and location of the photo.[72] 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.[73] A composite of locational metadata can thus reveal interests, activities, and travel patterns through still digital photographs.

2. Face Identification[74]

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 (e.g., surveillance tape, witness's iPhone video) or they might have a suspect's photograph and wish to match it with different photo datasets.[75]

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.[76] These databases could be drivers' license

71. *See* Richard Matthews, *How Law Enforcement Decodes Your Photos*, CONVERSATION (June 22, 2017, 4:04 PM), http://theconversation.com/explainer-how-law-enforcement-decodes-your-photos-78828 [https://perma.cc/7RQ8-MX5C]; Thomas Germain, *How a Photo's Hidden 'Exif' Data Exposes Your Personal Information*, CONSUMER REPS. (Dec. 6, 2019), https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data [https://perma.cc/YPG7-54AS].

72. *See* Matthews, *supra* note 71; Germain, *supra* note 71.

73. Germain, *supra* note 71.

74. Note that in past discussions of the subject, I have used the term "face recognition" to cover the categories of "face identification" and "face tracking." *See, e.g.*, *Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties: Hearing Before the H. Comm. on Oversight & Reform*, *supra* note 56. In this Article, I use the terms "face identification" and "face tracking" instead of "face recognition" for greater clarity and precision.

75. *See* Jon Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC NEWS (May 11, 2019, 3:19 AM), https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251 [https://perma.cc/P3A4-KYJR]; Harwell, *supra* note 46.

76. *See* James O'Neill, Opinion, *How Facial Recognition Makes You Safer*, N.Y. TIMES (June 9, 2019), https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html [https://perma.cc/HDY6-FJ35] ("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 . . . ."); *see also* Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial

photos (state DMV records), mugshot arrest photos (police-generated photos), or other more informal suspect identification systems (e.g., gang databases, jail photographs, prosecution data management systems).[77] In this scenario, police have an identified suspect and want to confirm the identity of the suspect through existing photo datasets.[78]

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 and 2019, the FBI conducted 152,500 searches for law enforcement investigations.[79] In New York City, NYPD conducted 7,024 searches in 2018.[80] *The Washington Post* reported that one small Oregon police department used commercial software created by Amazon to conduct investigatory searches in a variety of cases.[81] Police in Detroit, Michigan, have also admitted to using this type of facial recognition matching to track down violent suspects.[82]

-recognition-arrest.html [https://perma.cc/458E-SR99]; Ella Torres, *Black Man Wrongfully Arrested Because of Incorrect Facial Recognition*, ABC NEWS (June 25, 2020, 1:01 PM), https://abcnews.go.com/US/black-man-wrongfully-arrested-incorrect-facial-recognition/story?id=71425751 [https://perma.cc/JF9M-3C8E].

77. Amy Harmon, *As Cameras Track Detroit's Residents, a Debate Ensues over Racial Bias*, N.Y. TIMES (July 8, 2019), https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html [https://perma.cc/B5L2-9MS7] (describing a Detroit program that compares faces on video to "50 million driver's license photographs and mug shots contained in a Michigan police database"); *see also* Andrew Guthrie Ferguson, *Big Data Prosecution and* Brady, 67 UCLA L. REV. 180, 185–215 (2020) (describing various prosecution databases filled with photos of suspects).

78. *See* Schuppe, *supra* note 75 (describing how police use facial recognition to identify suspects from surveillance videos).

79. *Facial Recognition Technology (Part II): Ensuring Transparency in Government Use: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. 21 (2019) (statement of Kimberly J. Del Greco, Deputy Assistant Director, Criminal Justice Information Services, FBI).

80. O'Neill, *supra* note 76 ("[I]n 1,851 cases possible matches were returned, leading to 998 arrests.").

81. Harwell, *supra* note 46.

82. Harmon, *supra* note 77 ("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."). *But see* Robert Williams, Opinion, *I Was Wrongfully Arrested Because of Facial Recognition. Why Are Police Allowed to Use It?*, WASH. POST (June 24, 2020, 2:04 PM), https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology [https://perma.cc/XRD7-JFVR] (describing an innocent man's experience of being arrested for a non-violent crime based on Detroit police's use of facial recognition technology).

Face identification, as defined here, is limited to static photographs (not streaming video) and is used only after a crime has been committed to identify people. In the near future, however, this type of database matching could even be used during an ongoing investigation or during a police traffic stop.[83] Private companies are already selling the capabilities to do the search on a mobile phone.[84] Especially in a situation involving a suspect unwilling or unable to provide identification, the ability to quickly identify someone by their photo would be useful.[85]

One private company, Clearview AI, was revealed to have scraped billions of face images off public facing Internet and social media sites and created its own database for law enforcement.[86] Clearview AI had developed partnerships with hundreds of law enforcement and local police departments and conducted facial recognition searches to identify suspects.[87] Because Clearview scraped the images for its database from sites like Twitter—in violation of their policies—the company's practices were of dubious legality, but using its database was as

83. *See* Marco della Cava, *California Could Become First to Limit Facial Recognition Technology; Police Aren't Happy*, USA TODAY (June 17, 2019, 9:15 AM), https://www.usatoday.com/story/news/nation/2019/06/16/california-could-limit-how-police-use-facial-recognition-technology/1456448001 [https://perma.cc/9AZS-8P5F] ("State law enforcement officials here do not now employ the technology [facial recognition in body cameras] . . . . But some police officials oppose the bill on the grounds that a valuable tool could be lost.").

84. *See, e.g.*, FACEFIRST, http://web.archive.org/web/20200620203318/https://www.facefirst.com/industry/law-enforcement-face-recognition.

85. *See* Harwell, *supra* note 46 ("[T]he sheriff's office sets its own rules for facial-recognition use and allows deputies to use the tool to identify dead bodies, unconscious suspects and people who refused to give their name.").

86. Hill, *supra* note 68; Ina Fried, *Clearview Brings Privacy Concerns from Facial Recognition into Focus*, AXIOS (Feb. 10, 2020), https://www.axios.com/clearview-facial-recognition-law-enforcement-ac069290-b83e-4934-a9f0-0b782af82588.html [https://perma.cc/X4S6-QJFG] (chronicling the fallout from an exposé in *The New York Times*).

87. Hill, *supra* note 68; Fried, *supra* note 86; *see also* Corinne Reichert, *Clearview AI Is Looking to Expand Globally, Report Says*, CNET (Feb. 5, 2020), https://www.cnet.com/news/clearview-ai-reportedly-looking-to-expand-globally [https://perma.cc/4UXM-6SRH] (reporting that the company wants to sell its technology to law enforcement in Australia, Dubai, Sweden, Nigeria, and other countries).

simple as running a Google search.[88] Clearview AI is not alone, however, in selling facial recognition to law enforcement.[89]

3. Face Tracking

"Face tracking" is a term I will be using to describe 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 what I am terming "face tracking" in three different ways: (1) scanning stored video footage to identify a targeted face in the crowd; (2) scanning real-time video feeds to identify a targeted face; and (3) 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.[90] The same matching technology can be used to search months of stored surveillance footage, networks of video feeds, or growing image databases for images to compare with the target's face.[91] For example, searching stored video footage from a network of cameras could reveal the location of the "target" over time, including time, date, place,

88. Louise Matsakis, *Scraping the Web Is a Powerful Tool. Clearview AI Abused It*, WIRED (Jan. 25, 2020, 7:00 AM), https://www.wired.com/story/clearview-ai-scraping-web [https://perma.cc/7VTF-KS66]; Gisela Perez & Hilary Cook, *Google, YouTube, Venmo and LinkedIn Send Cease-and-Desist Letters to Facial Recognition App that Helps Law Enforcement*, CBS NEWS (Feb. 5, 2020, 6:15 AM), https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app [https://perma.cc/UE64-UZBA]; Jon Porter, *Facebook and LinkedIn Are Latest to Demand Clearview Stop Scraping Images for Facial Recognition Tech*, VERGE (Feb. 6, 2020), https://www.theverge.com/2020/2/6/21126063/facebook-clearview-ai-image-scraping-facial-recognition-database-terms-of-service-twitter-youtube [https://perma.cc/AX4H-A9BJ].

89. Nicolás Rivero, *The Little-Known AI Firms Whose Facial Recognition Tech Led to a False Arrest*, QUARTZ (June 26, 2020), https://qz.com/1873731/the-unknown-firms-whose-facial-recognition-led-to-a-false-arrest [https://perma.cc/8MMN-H9V6] (describing the companies that developed and sold the facial recognition technology that Detroit police used when they arrested an innocent man).

90. Garvie & Moy, *supra* note 58.

91. *Id.*

and patterns of movement.[92] 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.[93] 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 (i.e., 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.

b. Face Tracking: Real-Time Scans

Networked video systems also create the potential to track suspects in real-time.[94] A networked system of real-time face tracking would be able to provide the specific location of a "wanted" suspect.[95] The "hit" or "match" would alert police to the location of a particular person at a particular time in the city.[96] In January 2020, the London Metropolitan Police rolled out a facial recognition surveillance tool that seeks to match faces with a stored "watch list."[97] Of course, 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)

92. *Id.*

93. *Id.*

94. *Id.*

95. *Id.*; *see* Harmon, *supra* note 77 ("Although the [Detroit Police D]epartment 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.").

96. *See Police Unlock AI's Potential To Monitor, Surveil and Solve Crimes*, *supra* note 53 (demonstrating how police can use artificial intelligence to track a suspect).

97. Natasha Lomas, *London's Met Police Switches on Live Facial Recognition, Flying in the Face of Human Rights Concerns*, TECHCRUNCH (Jan. 24, 2020, 7:07 AM), https://techcrunch.com/2020/01/24/londons-met-police-switches-on-live-facial-recognition-flying-in-face-of-human-rights-concerns [https://perma.cc/Y9QR-L7E6]; Jason Douglas & Parmy Olson, *London Police to Start Using Facial Recognition Cameras*, WALL ST. J. (Jan. 24, 2020, 2:49 PM), https://www.wsj.com/articles/london-police-to-start-using-facial-recognition-cameras-11579895367 [https://perma.cc/A3AZ-DARA].

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.[98] Police access to this dataset (via informal request, subpoena, warrant, or purchase) can help identify suspects, groups, and associates.[99] Third-party datasets of photos not only provide images and identification but also locational data from metadata that can reveal where and when the photos were taken.[100] While unstructured, this long-term, aggregated locational information could be revealed from 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.[101]

4. Non-Law Enforcement Purposes

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.[102] While the lines

98. Facebook users alone upload 350 million photos per day. Salman Aslam, *Facebook by the Numbers: Stats, Demographics & Fun Facts*, OMNICORE (Apr. 22, 2020), https://www.omnicoreagency.com/facebook-statistics [https://perma.cc/936W-4Z9G].

99. O'Neill, *supra* note 76 (describing how police could "find social media images of a person at a birthday party wearing the same clothing as the suspect in a robbery" using facial recognition technology, leading to a break in a case).

100. Matthews, *supra* note 71 (explaining metadata and noting that Facebook "typically removes metadata from uploaded images"); Germain, *supra* note 71 ("If you upload pictures to Craigslist, Facebook, Imgur, Instagram, Twitter, or WhatsApp, the Exif data won't be available to the people who see them. That doesn't mean social media companies don't find any use for it, however.").

101. *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), https://www.nytimes.com/2014/01/08/nyregion/seeking-clues-to-gangs-and-crime-detectives-monitor-internet-rap-videos.html [https://perma.cc/E2FC-XYN9] (describing how police and prosecutors listen to local rap videos to understand recent crimes); Ben Austen, *Public Enemies: Social Media Is Fueling Gang Wars in Chicago*, WIRED (Sept. 17, 2013, 6:38 AM), https://www.wired.com/2013/09/gangs-of-social-media [https://perma.cc/MD29-DC4N] (explaining how police monitor social media to anticipate and respond to crimes).

102. *See* Joshi & Gupta, *supra* note 19, at 58 (articulating a variety of uses for facial recognition technology).

between security, policing, and public safety are blurry, some non-law enforcement uses include monitoring high security areas[103] or government-controlled areas such as public or rent-controlled housing.[104]

In other cases, facial recognition can be used to identify victims of crime or lost children, where police focus on their emergency response, not their investigation.[105] 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. Regardless of how systems collect images, how their algorithms match faces, or why users conduct a search, these systems 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, races, face types, and then match the target face to all the other identified faces. This mass surveillance capability also exists if the dataset consists of Facebook images. Once we build the architecture of surveillance that supports non-law enforcement matching, we have by necessity also created the capabilities for police use.

---

103. *See* Jon Schuppe, *Secret Service Tests Facial Recognition Surveillance System Outside White House*, NBC NEWS (Dec. 4, 2018, 11:43 AM), https://www.nbcnews.com/news/us-news/secret-service-tests-facial-recognition-surveillance-system-outside-white-house-n943536 [https://perma.cc/965K-DA4B] (describing the Secret Service's efforts to identify persons of interest outside the White House compound quickly using facial recognition).

104. Mutale Nkonde, *Automated Anti-Blackness: Facial Recognition in Brooklyn, New York*, HARV. KENNEDY SCH. J. AFR. AM. POL'Y, 2019–2020, at 30, 31, 34 (critiquing the proposal to install facial recognition technology in Atlantic Towers, a rent-controlled apartment complex); Yasmin Gagne, *How We Fought Our Landlord's Secretive Plan for Facial Recognition—and Won*, FAST CO. (Nov. 22, 2019), https://www.fastcompany.com/90431686/our-landlord-wants-to-install-facial-recognition-in-our-homes-but-were-fighting-back [https://perma.cc/ZV48-864C] (interviewing residents of Atlantic Towers); Lola Fadulu, *Facial Recognition Technology in Public Housing Prompts Backlash*, N.Y. TIMES (Sept. 24, 2019), https://www.nytimes.com/2019/09/24/us/politics/facial-recognition-technology-housing.html [https://perma.cc/ET3D-E4Y2] (reporting on the installation of video surveillance around a Detroit public housing complex that enables police to capture footage and use facial recognition technology).

105. Aarti Shahani, *ICE Turned to DMV Driver's License Databases for Help with Facial Recognition*, NPR (July 8, 2019, 4:45 PM), https://www.npr.org/2019/07/08/739643786/ice-turned-to-dmv-drivers-license-databases-for-help-with-facial-recognition [https://perma.cc/CWY5-P4PH] ("[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 [sic] them with their families.").

The next Part addresses the privacy-invading powers of facial recognition surveillance technology and how the Fourth Amendment might act as a constitutional check on growing police surveillance power. Later, Part III will tackle the equally fundamental questions arising from 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 into the puzzle of facial recognition technology? There is not an easy answer because the Fourth Amendment has largely ignored surveillance techniques that police use early in an investigation[106] and failed to regulate information seemingly exposed to the public.[107] But a new understanding of policing as more programmatic and systemic has shifted recent thinking about this traditional view,[108] 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 that 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 (e.g., surveillance, identification, tracking, or non-law enforcement purposes) and whether the Supreme

106. *See* Joh, *supra* note 1, at 33 (summarizing how the Fourth Amendment permits activities like following a suspect on the street).

107. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 574–76 (2009).

108. *See* Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1041–42 (2016) ("While our Fourth Amendment framework is transactional, then, surveillance is increasingly *programmatic*. . . . [T]he system of searches is designed en masse."); Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 93–97 (2016) ("[T]he concrete rules governing panvasive techniques should be viewed through the entirely different prism of administrative law."); Tracey L. Meares, *Programming Errors: Understanding the Constitutionality of Stop-and-Frisk as a Program, Not an Incident*, 82 U. CHI. L. REV. 159, 162–63 (2015).

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.[109] This constitutional standard comes from the Supreme Court's interpretation of the Fourth Amendment in *Katz v. United States*.[110] 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.[111] 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.[112] The Supreme Court held that the electronic interception of Mr. Katz's conversation violated a reasonable expectation of privacy and thus the Fourth Amendment.[113]

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

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

110. *Id.*

111. *Id.* ("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.'").

112. *Id.* at 348 (majority opinion).

113. *Id.* at 359. 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. United States v. Jones, 565 U.S. 400, 427–28 (2012) (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." (footnote omitted)).

> 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*.[114]

This understanding has largely prevailed in the context of human observation of human faces.[115] As a result, one traditional way of looking at the Fourth Amendment doctrine is 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.[116] Large scale surveillance systems have already created a difficult puzzle for standing determinations.[117] While facial challenges to statutes are permissible,[118] and systems of Fourth Amendment violations have been litigated under civil rights law,[119] 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. After the Court's unanimous

114. United States v. Dionisio, 410 U.S. 1, 14 (1973) (emphasis added).

115. *See, e.g.*, Rowe v. Burton, 884 F. Supp. 1372, 1381 (D. Alaska 1994) ("Generally, one does not have a reasonable expectation of privacy as to his physical characteristics, including one's likeness.").

116. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 411–14 (2013) (denying standing for a lawsuit challenging mass surveillance under the Foreign Intelligence Surveillance Act); *see also* Christopher Slobogin, *Standing and Covert Surveillance*, 42 PEPP. L. REV. 517, 530 (2015) (describing justiciability requirements). *But see* Leaders of a Beautiful Struggle v. Balt. Police Dep't, No. RDB-20-0929, 2020 WL 1975380, at *1–2, *6 (D. Md. Apr. 24, 2020), *appeal docketed*, No. 20-1495 (4th Cir. Apr. 28, 2020) (finding standing for community activists to challenge Persistent Surveillance System planes flying over Baltimore, Maryland, and videotaping movements on the ground).

117. *See* Stephen I. Vladeck, *Standing and Secret Surveillance*, 10 I/S: J.L. & POL'Y INFO. SOC'Y 551, 552 (2014), https://kb.osu.edu/handle/1811/73361 [https://perma.cc/N8XA-DUPM] (describing standing difficulties in *Clapper* and considering congressional remedies).

118. City of Los Angeles v. Patel, 576 U.S. 409, 415 (2015) ("We first clarify that facial challenges under the Fourth Amendment are not categorically barred or especially disfavored.").

119. *See* Floyd v. City of New York, 959 F. Supp. 2d 540, 558 (S.D.N.Y. 2013) (examining New York City's stop-and-frisk policy under the Fourth and Fourteenth Amendments).

ruling in *Riley v. California*,[120] legal commentators have recognized that when it comes to new digital surveillance technologies, "digital is different" for Fourth Amendment purposes.[121] In addition, if interpreted broadly, the Supreme Court's analysis about particular cases may have application to generalized surveillance systems.[122] 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[123]

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.[124] 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.

---

120. Riley v. California, 573 U.S. 373, 403 (2014) ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

121. *See* 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, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1, 10 (2015) ("[C]omputer technologies can call for computer-specific rules."); *see also* Jennifer Stisa Granick, *SCOTUS & Cell Phone Searches: Digital Is Different*, JUST SEC. (June 25, 2014), https://www.justsecurity.org/12219/scotus-cell-phone-searches-digital [http://perma.cc/94RH-42EV].

122. Granick, *supra* note 121 ("The Court's reasoning [in *Riley*] also will influence Fourth Amendment jurisprudence and surveillance cases going forward.").

123. Andrew Guthrie Ferguson, *Future-Proofing the Fourth Amendment*, HARV. L. REV. BLOG (June 25, 2018), https://blog.harvardlawreview.org/future-proofing-the-fourth-amendment [https://perma.cc/MD79-G69G]; *see* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) ("[T]he rule the Court adopts 'must take account of more sophisticated systems that are already in use or in development.'").

124. *See* Susan Freiwald & Stephen W. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 216 (2018) ("*Carpenter* is the latest in a trilogy of decisions in which the Supreme Court has finally begun to confront modern surveillance tools used by law enforcement."); Margaret Hu, *Cybersurveillance Intrusions and an Evolving* Katz *Privacy Test*, 55 AM. CRIM. L. REV. 127, 132 (2018) (noting that "*Jones*, *Riley*, and other recent Fourth Amendment cases illuminate the limitations of the *Katz* privacy test in the face of developing big data law enforcement capabilities").

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" that violated the constitutional rights of the driver.[125] More importantly for our analytical purposes, five Justices concurred in the outcome, reasoning that long-term GPS location tracking violates a reasonable expectation of privacy in most cases.[126] 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.[127] 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*.[128]

In *Carpenter*, the Supreme Court held that police typically need a probable cause warrant to acquire digital cell-site location information (CSLI) held by third-party cell phone service providers.[129] 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.[130] Using a court order authorized under the Stored Communications Act, police obtained seven days of his CSLI.[131] This information provided police with a virtual map of Carpenter's whereabouts that corresponded with his presence during the robberies.[132] 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

125. *See* United States v. Jones, 565 U.S. 400, 402–08 (2012).

126. *See id.* at 414–15 (Sotomayor, J., concurring) ("I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'"); *id.* at 430 (Alito, J., concurring). In *Carpenter*, Chief Justice Roberts confirmed this consensus by positively citing the *Jones* concurrences and declaring, "A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements." *Carpenter*, 138 S. Ct. at 2215, 2217.

127. *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

128. *Carpenter*, 138 S. Ct. at 2217.

129. *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.").

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

131. *Carpenter*, 138 S. Ct. at 2212.

132. *See id.* at 2212–13.

warrant.[133] 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.[134] Chief Justice Roberts summarized the holding stating, "[i]n 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."[135] The focus on "depth," "breadth," scope, and scale makes it clear that the Court is concerned with systems of digital surveillance.[136] The reasoning again turned on the voluminous and personal nature of the locational data being sought by police without a warrant.[137]

Finally, in *Riley v. California*, the Court held that police must obtain a warrant before searching a suspect's smartphone incident to arrest.[138] The Court reasoned that sensitive data[139] in modern smartphones revealed too many of the "privacies of life" not to require a probable cause warrant before acquiring the information.[140] 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.[141] The quantitative difference involves the "immense storage capacity" that can, in a very small space, collect and maintain an almost infinite amount of personal data.[142] In addition, the nature and scope of digital

133. *See id.* at 2212.

134. *Id.* at 2217–19.

135. *Id.* at 2223.

136. *See* Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 399 (2019) (explaining the Court's decision in *Carpenter* reveals its concern with the modern proliferation of digital surveillance).

137. *See Carpenter*, 138 S. Ct. at 2223.

138. Riley v. California, 573 U.S. 373, 386 (2014).

139. *See, e.g.*, Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1133 (2015) (describing sensitive information as "information that can be used to enable privacy or security harm when placed in the wrong hands").

140. *Riley*, 573 U.S. at 403 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

141. *Id.* at 393 ("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 called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

142. *Id.* at 393–94 ("One of the most notable distinguishing features of modern cell phones is their immense storage capacity. . . . Most people cannot lug around every

information reveals much more qualitative information than citizens normally share with anyone else.[143]

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.[144] One can also intuit a new awareness of systems of mass surveillance as a distinct concern not traditionally acknowledged in Fourth Amendment cases.[145] The Court is not just talking about a particular defendant's rights *vis a vis* surveillance technologies, but everyone's rights.[146] Such a digitally-aware Fourth Amendment would, of course, apply to the mass deployment of facial recognition.[147]

The next six Subsections identify what I am calling the "future-proofing" principles, which are helpful to analyze new surveillance technologies.[148] Some of these principles are decidedly new, and some can trace their roots back to first principles, but combined, these principles help structure an otherwise disordered Fourth Amendment doctrine.[149] The final Subsection will then apply this future-proofing theory to the problem of facial recognition technology.[150] 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.[151] In its recent technologically-enhanced

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.").

143. *Id.* at 395–97.

144. *See* Ohm, *supra* note 136, at 399–401.

145. *See id.* at 401–03.

146. *See infra* notes 157–58 and accompanying text.

147. *See infra* notes 157–58 and accompanying text.

148. *See infra* Parts II.B.1–6.

149. *See infra* Parts II.B.1–6.

150. *See infra* Parts II.B.7, II.C.

151. *But see* United States v. Knotts, 460 U.S. 276 (1983) (illustrating such an awareness of technological dangers is not necessarily new, as the Supreme Court has recognized mass surveillance concerns in older beeper tracking cases); Olmstead v. United States, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting) (arguing 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).

surveillance cases, the Supreme Court has recognized that digital police capabilities are simply not the equivalent of traditional analog policing methods.[152]

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.[153] He said the same thing in *Riley* when comparing smartphone data recovered incident to arrest and traditional physical objects recovered incident to arrest.[154] Justice Sotomayor 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.[155] In this way, the Court has been conscious of future-proofing its holdings.[156] In both *Kyllo*[157] and *Carpenter*,[158] the Court explicitly acknowledged that its decisions were 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,[159] recognizing that Fourth Amendment principles are threatened by new surveillance technologies in ways they were not similarly threatened by existing analog counterparts.[160]

152. *See* Ohm, *supra* note 136, at 399–403.

153. Carpenter v. United States, 138 S. Ct. 2206, 2210–14 (2018) ("[T]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers.").

154. Riley v. California, 573 U.S. 373, 386 (2014) ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in [prior precedent]."); *see also Carpenter*, 138 S. Ct. at 2214 ("[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.").

155. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

156. Ferguson, *supra* note 123.

157. 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.").

158. *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.'" (quoting *Kyllo*, 533 U.S. at 36)).

159. *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 479–81 (2011).

160. *Carpenter*, 138 S. Ct. at 2214 ("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[]

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.[161] It is no longer an answer to say, "Well, police could have just done it without technology," so the surveillance technique is constitutional.[162] 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.[163]

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 Court's recent decisions looking at the concerns with data aggregation, data permanence, long-term tracking, arbitrary monitoring, and the permeation of surveillance technologies.[164]

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.[165] Both Justice Sotomayor and Justice Alito in *Jones* separately articulated the consequences of large-scale public data collection on individual liberty.[166] The principle was reaffirmed in *Carpenter* when the Court

preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" (quoting *Kyllo*, 533 U.S. at 34)).

161. *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."); *see also* Granick, *supra* note 121.

162. *See* Granick, *supra* note 121.

163. *See* Riley v. California, 573 U.S. 373, 393 (2014); *see also* Granick, *supra* note 121.

164. *See infra* Parts II.B.2–6.

165. Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1139–40 (2002) (describing the increased privacy concerns with compiling individual public records into comprehensive reports). *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (explaining the Fourth Amendment "mosaic theory" under which searches are analyzed as a collective sequence of steps rather than as individual steps).

166. United States v. Jones, 565 U.S. 400, 413–16 (2012) (Sotomayor, J., concurring); *id.* at 429–31 (Alito, J., concurring).

drew a clear line from *Jones* to the privacy-invading nature of aggregated cell-site tracking.[167] 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.[168] 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 constitutionally protected space.[169] In each of these cases, the Court found the mosaic of aggregated personal data collection a Fourth Amendment concern.[170]

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-site tracking.[171]

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

167. Carpenter v. United States, 138 S. Ct. 2206, 2225 (2018).

168. *Riley*, 573 U.S. at 394 ("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.").

169. *Id.* at 396–97 ("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.").

170. *See, e.g.*, Kerr, *supra* note 165.

171. *See infra* Parts II–III.

all time.[172] This "time-machine-like" capability to access permanently stored data produced a fear about the creation of overbroad and unlimited data systems that allow for retrospective searching.[173] 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.[174]

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.[175]

4. Anti-Tracking Principle

The Supreme Court in *Jones* and *Carpenter* was explicitly concerned about the locational tracking capabilities of new surveillance technologies. *Jones* was literally a case about GPS tracking[176] and *Carpenter* a case about a network of tracking capabilities.[177] The *Jones* Court expressed concern about the associational freedoms impacted and the revealing nature of the tracking technology:

> 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."[178]

172. United States v. Jones, 565 U.S. 400, 415 (2012) (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.

173. Henderson, *supra* note 121, at 939.

174. *Carpenter*, 138 S. Ct. at 2218.

175. *Id.*

176. *Jones*, 565 U.S. at 403–04.

177. *Carpenter*, 128 S. Ct. at 2216.

178. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

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.[179] Similarly, Chief Justice Roberts in *Carpenter* recognized how the tracking capabilities of cellphones dwarf the capabilities of GPS tracking,[180] allowing an "all-encompassing record of the holder's whereabouts"[181] and creating a much graver threat to personal privacy.[182] The Court has been adamant that locational data should receive some Fourth Amendment protection when threatened by tracking technologies.[183] Similarly, the intellectual tracking of ideas—as made manifest by the informational choices in our smartphone—also deserves protection under *Riley*.[184] As facial recognition can track and identify location and generate inferences from private locational details, the same privacy concerns arise.[185]

5. Anti-Arbitrariness Principle

A related theme in the cases involves the desire to prevent arbitrary police actions. In *Carpenter*, Chief Justice Roberts stated quite

179. *Id.* ("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) ("[S]ociety'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.").

180. *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.").

181. *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.'").

182. *Id.* 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*.").

183. *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) [hereinafter Gray, *A Collective Right*]; Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527 (2017).

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

185. *See infra* Parts II–III.

simply: "[t]he '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.'"[186]

This is, of course, the central principle animating much of constitutional criminal procedure involving checks to government power.[187] The Fourth Amendment's textual emphasis on warrants, probable cause, particularity, oaths, and other formalities speaks to a concern about unconstrained, arbitrary government authority.[188] But specific emphasis on arbitrariness echoed Justice Sotomayor's concurrence in *Jones* where she stated equally plainly, "the Fourth Amendment's goal [is] to curb *arbitrary* exercises of police power."[189]

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."[190]

This fear of arbitrary government power arose directly from a historical experience which amply demonstrated how unconstrained governmental police power could negatively impact liberty.[191] In the prerevolutionary war colonies, arbitrary invasions directly interfered

186. *Carpenter*, 138 S. Ct. at 2213 (emphasis added).

187. 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.*, Florida v. Riley, 488 U.S. 445, 462 (1989) (Brennan, J., dissenting) ("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.'").

188. U.S. CONST. amend. IV.

189. United States v. Jones, 565 U.S. 400, 416–17 (2012) (Sotomayor, J., concurring) (emphasis added).

190. *Carpenter*, 138 S. Ct. at 2213–14 (emphasis added).

191. 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.").

with private behavior, manifesting both as physical home invasions and indirect government surveillance.[192]

In our modern times, facial recognition technology gives police the power to conduct arbitrary digital searches of its citizens.[193] Governments can run pattern matching searches for any face.[194] They can target surveillance in particular places or to find particular people.[195] The power is arguably far broader than a general warrant.[196] Instead of having a constable empowered to find out revealing information, you have an entire city designed to expose the people in it.[197]

6. Anti-Permeating Surveillance Principle

Finally, in both *Carpenter* and *Jones*, the Court addressed the Fourth Amendment's foundational role in restricting invasive police surveillance.[198] In *Carpenter* the Court stated, "a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'"[199] 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."[200]

Admittedly, the "too permeating" language is both vague and oddly unhelpful in a world of growing omnipresent surveillance.[201]

192. *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.'").

193. *See supra* Part II.C.

194. *See supra* Part II.C.

195. *See supra* Part II.C.

196. *See infra* Parts II.D, III.

197. *See infra* Parts II–III.

198. 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.").

199. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

200. United States v. Jones, 565 U.S. 400, 416–17 (2012) (Sotomayor, J., concurring) (quoting *Di Re*, 332 U.S. at 595).

201. *See* Daniel de Zayas, Comment, Carpenter v. United States *and the Emerging Expectation of Privacy in Data Comprehensiveness Applied to Browsing History*, 68 AM. U. L. REV. 2209, 2246 & n.216 (2019) (comparing Justice Sotomayor's invocation of the Framers' goals for the Fourth Amendment with colonial conceptions of privacy as "safeguard[ing] personal autonomy, emotional release, self-evaluation, and limited and protected communication").

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 their particular cases involving particular technologies[202] and more about signaling that all new privacy-invading surveillance technologies will require greater scrutiny.[203] 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 that undermined personal liberty and security.[204]

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

202. *See, e.g.*, Amy Davidson Sorkin, *In* Carpenter *Case, Justice Sotomayor Tries To Picture the Smartphone Future*, NEW YORKER (Nov. 30, 2017), https://www.newyorker.com/news/our-columnists/carpenter-justice-sotomayor-tries-to-picture-smartphone-future [https://perma.cc/2Q8P-3LT4] ("If *Smith* can apply to long-term location data today, what might a decision for the government in *Carpenter* be used to justify forty years from now?"); Kade Crockford & Nathan Freed Wessler, *The Supreme Court's Big Privacy Ruling Sent a Message. Will Judges Hear It?*, ACLU: FREE FUTURE (Sept. 5, 2018, 1:30 PM), https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-big-privacy-ruling-sent-message-will-judges [https://perma.cc/D74K-XS68] ("While [*Carpenter*] concerned historical location data stored by cellphone companies, it provides a roadmap for the protection of all manner of location data.").

203. *See, e.g.*, Evan Caminker, *Location Tracking and Digital Data: Can* Carpenter *Build a Stable Privacy Doctrine?*, 2018 SUP. CT. REV. 411, 415 ("*Carpenter* means that a majority of the Justices are searching to find ways to better protect privacy in the modern age. And by retooling long-standing precedent to be more adaptive to privacy concerns . . . ."); Shaun B. Spencer, *Predictive Surveillance and the Threat to Fourth Amendment Jurisprudence*, 14 I/S: J.L. & POL'Y INFO. SOC'Y 109, 131 (2017) ("The *Carpenter* decision could significantly impact how future courts approach predictive surveillance."); *see also* Transcript of Oral Argument at 44, *Carpenter*, 138 S. Ct. 2206 (No. 16-402) ("JUSTICE SOTOMAYOR: That's today . . . we need to look at [the privacy of cellphone information] with respect to how the technology is developing.").

204. *See supra* text accompanying notes 191–92.

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.[205] The language chosen in *Carpenter* is about how a system of surveillance could impact everyone, not just the instant defendant.[206] The underlying argument is 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.[207]

Thus, to study the problem of facial recognition, this Article looks at issues of aggregation, permanence, locational tracking, arbitrariness, and pervasive surveillance through a "digital is different"[208] 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 different levels of protection from different types of facial recognition technology. Even more importantly, this analysis reveals the constitutional gaps in protective coverage requiring legislative action, which will be discussed in Part IV.

205. *See* Gray, *A Collective Right*, *supra* note 183, at 199–200 (connecting the Fourth Amendment's origin in protecting the colonial public against general warrants with the Court's ruling in *Jones*).

206. *Carpenter*, 138 S. Ct. at 2218 ("Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone.").

207. *See* Transcript of Oral Argument, *supra* note 202, at 48–49 ("JUSTICE SOTOMAYOR: . . . . do you really believe that people expect that the government will be able to [see and locate them anywhere they are at any point in time] without probable cause and a warrant?").

208. Henderson, *supra* note 121, at 951.

1. Face Surveillance

How does the Fourth Amendment apply to generalized face surveillance? Again, face surveillance is the scenario involving suspicionless, mass surveillance of all people in a public area or using a third-party records image set.[209] 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 of gathering information (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 deemed 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. In *Carpenter*, the Supreme Court made clear that the opinion did not cover "conventional surveillance techniques and tools, such as security cameras."[210]

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.[211] The combination of facial recognition software with the scope and scale of digital networks create a new scheme just too different to equate to older systems.[212] In terms of scope, generalized surveillance is troubling because everyone observed

209. *See supra* Part I.B.1.

210. *Carpenter*, 138 S. Ct. at 2220.

211. *See supra* Part II.B.1.

212. The addition of such software to existing networks could result in a rapid and dramatic increase in our government's surveillance capacity.

> The United States is, by various estimates, home to tens of millions of surveillance cameras. . . . [I]t has been widely understood that it would be unfeasible, if not impossible, for each device to be constantly monitored and its footage carefully categorized and documented . . . . But improvements to technology . . . are poised to change that, ensuring that every second of footage can be analyzed.

Niraj Chokshi, *How Surveillance Cameras Could Be Weaponized with A.I.*, N.Y. TIMES (June 13, 2019), https://www.nytimes.com/2019/06/13/us/aclu-surveillance-artificial-intelligence.html [https://perma.cc/EL49-3YAD]; *see also* Complaint at 4–5, ACLU v. U.S. Dep't of Just., No. 1:19-CV-12242 (D. Mass. Oct. 31, 2019) ("[Biometric identification and tracking] technologies have the potential to enable undetectable, persistent, and suspicionless surveillance on an unprecedented scale.").

becomes a target.[213] In order to identify every person on a given street, police would need to match those people against some identified list which, for surveillance purposes, could encompass nearly everyone in the country.[214] The scale of the search can also be a problem, depending on which datasets the targets are matched against. Public spaces or the extensive repositories of images in third-party databases provide a vast search field for potential matches.[215] Months' worth of stored video footage from surveillance cameras, or a database of years' worth of images uploaded to third-party social networks, would expand the scale of potential matches to cover millions (or even billions) of people.[216] This type of overbroad matching seems

213. *See* Randy E. Barnett, *The NSA's Surveillance Is Unconstitutional*, WALL ST. J. (July 11, 2013, 6:44 PM), https://www.wsj.com/articles/SB10001424127887323823004578593591276402574 [https://perma.cc/6G8S-3X5A] ("[T]he Foreign Intelligence Surveillance Court has apparently secretly approved the blanket seizure of data on every American . . . . Such indiscriminate data seizures are the epitome of 'unreasonable,' akin to the 'general warrants' issued by the Crown to authorize searches of Colonial Americans.").

214. *Compare* S. 744, 113th Cong. § 3101(c)(1)(F)(iii) (2013) ("The Secretary [of Homeland Security] shall develop and maintain a photo tool that enables employers to match the photo on a covered identity document . . . to a photo maintained by a U.S. Citizenship and Immigration Services database."), *and* David Kravets, *Biometric Database of All Adult Americans Hidden in Immigration Reform*, WIRED (May 10, 2013, 6:30 AM), https://www.wired.com/2013/05/immigration-reform-dossiers [https://perma.cc/XJ6V-JEG3] (suggesting that the database would contain "photographs of everyone in the country with a driver's license or other state-issued photo ID"), *with* VANESSA M. PEREZ, PROJECT VOTE, AMERICANS WITH PHOTO ID: A BREAKDOWN OF DEMOGRAPHIC CHARACTERISTICS 3 tbl.1 (2015), https://www.projectvote.org/wp-content/uploads/2015/06/AMERICANS-WITH-PHOTO-ID-Research-Memo-February-2015.pdf [https://perma.cc/KL4F-VZ99] (reporting the results of a survey finding that 93% of Americans possess a current government-recognized photo ID).

215. *See, e.g.*, *Google Photos: One Year, 200 Million Users, and a Whole Lot of Selfies*, GOOGLE: KEYWORD (May 27, 2016), https://blog.google/products/photos/google-photos-one-year-200-million [https://perma.cc/5N7S-UNCU] (disclosing that users of one phone application captured 24 billion self-taken photos of themselves in one year).

216. *See* FACEBOOK INV. RELS., FACEBOOK Q2 2020 RESULTS 3 (2020), https://s21.q4cdn.com/399680738/files/doc.financials/2020/q2/02-2020-FB-Earnings-Presentation.pdf [https://perma.cc/F8N9-KYZ4] (disclosing that Facebook has 2.7 billion monthly active users worldwide and 256 million such users in the United States and Canada); FACEBOOK, ERICSSON & QUALCOMM, A FOCUS ON EFFICIENCY 6 (2013) [https://web.archive.org/web/20130919062717/https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851575_520797877991079_393255490_n.pdf] (reporting figures which equate to the average user uploading approximately nine photos per month). Even this rough synthesis of uploads to Facebook would provide law enforcement 24.3 billion new photos each month.

to cut against the Fourth Amendment's preference for particularized, individualized suspicion.[217]

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 scope, scale, detail, personal data, locational data, and retrieval capabilities at play. Further, the other principles concerning aggregation, tracking, and permanence suggest that this type of constant, ongoing monitoring system would constitute a Fourth Amendment search, although the analysis for stored footage and real-time images differs slightly.

a. Face Surveillance: Stored Footage

The power of face surveillance is that it allows police to scan through stored footage and identify 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).[218] The future-proofing principles of anti-aggregation, anti-permanence, and anti-tracking all apply.[219] This suggests face surveillance would be considered a surveillance system of Fourth Amendment concern.

After all, this surveillance would be directed against everyone in public,[220] creating a pervasive sense of police power that could be arbitrarily used or abused.[221] If the Supreme Court was concerned with tracking a single car (*Jones*)[222] or a single cellphone (*Carpenter*),[223] the idea of tracking everyone without a warrant should also raise constitutional concerns. Certainly, a system that routinely scanned faces and identified everyone in public or allowed the searching of stored image data to identify someone would raise constitutional red flags.

217. *See* Thomas K. Clancy, *The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures*, 25 U. MEM. L. REV 483, 533 & n.206 (1995) ("Individualized suspicion of illegal activity is normally required as one element of that justification [for the interference of liberty that results from a seizure].").

218. *See supra* Part I.B.1.a.

219. See *supra* Parts II.B.2–4.

220. *See* Mozur, *supra* note 65 (discussing a Chinese face surveillance system that scans all crossers at an intersection to identify jaywalkers).

221. *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS COMPUTERS AND THE RIGHTS OF CITIZENS 75 (1973) ("The risk of abuse of intelligence records is too great to permit their use without *some* safeguards to protect the personal privacy and due process interests of individuals.").

222. United States v. Jones, 565 U.S. 400, 403 (2012).

223. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

Perhaps even more fundamentally, the operative limiting terms of "probable cause" and "warrants" in the Fourth Amendment make little sense in a world of generalized surveillance.[224] With generalized surveillance there is no cause at all. There can certainly be no probable cause warrant predicate for generalized surveillance of everyone, everywhere, at all times. The lack of a limiting principle and the overbroad nature of suspicionless surveillance highlight the unreasonable nature of this type of surveillance.

While there exist real issues of standing to challenge face surveillance under traditional Fourth Amendment law,[225] one can imagine that a surveillance system that identified and tracked everyone in a city environment would be challenged under § 1983 civil rights law as a facial matter[226] or could be litigated if a criminal defendant was stopped based on the technology.[227] 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.[228]

---

224. *See* Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 299 (2016) ("The inability to make sense of the Fourth Amendment in today's world has the practical result of causing vastly more police intrusion, widespread violations of constitutional rights, and racial profiling. Making matters worse, there is good evidence that these intrusions are simply inefficacious . . . ."). *See generally* BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 143–84 (2017) (discussing the evolution of jurisprudence on the issue of cause in warrantless searches).

225. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) ("To establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" (quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010))). The Court held that there was no standing to challenge an electronic surveillance program on grounds that an "objectively reasonable likelihood" of the respondents' information being searched was "inconsistent with [the] requirement that 'threatened injury must be certainly impending to constitute injury in fact.'" *Id.* at 410 (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

226. For example, a federal district court found that community activists in Baltimore, Maryland, had both First and Fourth Amendment standing to challenge aerial surveillance planes filming the entire city as part of a violent crime suppression effort. Leaders of a Beautiful Struggle v. Balt. Police Dep't, No. RDB-20-0929, 2020 WL 1975380, at *1–2 (D. Md. Apr. 24, 2020).

227. *Cf. Clapper*, 568 U.S. at 423 (Breyer, J., dissenting) ("[A] plaintiff has that standing . . . if the action or omission that the plaintiff challenges has caused . . . an injury that is 'concrete and particularized,' 'actual or imminent,' and 'redress[able] by a favorable decision.'" (second alteration in original) (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992))).

228. *See* Complaint, *supra* note 212, at 1–2 ("[S]urveillance [utilizing biometric identification and tracking technologies] would permit the government to pervasively track people's movements and associations in ways that threaten core constitutional values.").

b. 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 each time an identifiable face appears on the screen.[229] This would result in an equivalent tracking system marking where people are located, what they are doing, and when they are doing it. While a real-time system would only provide a snapshot of localized presence, the data could be stored and rendered searchable[230] (raising the stored footage issue).[231] Equally importantly, the system itself "runs against everyone" and creates a similar warrantless dragnet.[232] The future-proofing principles point to a Fourth Amendment search problem, as the system can aggregate personal location data, track individuals, and is permanent, pervasive, and arbitrary.[233]

Simultaneously, 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 necessarily deep or aggregated data collection.[234] If the system did not save the collected data, the retrospective harm principle might not apply. Similarly, if the system merely identified a particular person at a particular point in time but did not track them, the tracking and aggregation principles might be less important.[235] Under a *Carpenter* analysis, one might

229. *See* Mozur, *supra* note 65 (discussing the goals of police and artificial intelligence companies to create facial recognition scans capable of identifying individuals in real-time).

230. *See* Mozur, *supra* note 64 (discussing a Chinese facial-information database searchable by data tags identifying gender and ethnic minority status).

231. *See supra* Part II.C.1.a.

232. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018); *cf.* Press Release, ACLU Va., ACLU-VA Puts Law Enforcement on Notice That Warrantless Dragnet Surveillance Is Illegal (July 15, 2019), https://acluva.org/en/press-releases/aclu-va-puts-law-enforcement-notice-warrantless-dragnet-surveillance-illegal [https://perma.cc/JBG9-2EXE] (reporting the noticing of Virginia law enforcement agencies that "'passive' use of automated license plate readers" used to "collect data on people's whereabouts without it being related to a specific criminal investigation" is illegal).

233. *See supra* Part II.B.

234. *See* JAKE LAPERRUQUE, CONST. PROJECT, FACING THE FUTURE OF SURVEILLANCE (2019), https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance [https://perma.cc/S3DP-72C6] ("*Real-time surveillance* . . . involves scanning all faces during a video feed and running them against a watchlist that will identify certain individuals. The contents of such a list could . . . be as broad as all individuals with a prior arrest for a minor crime."). *But cf.* Mozur, *supra* note 65 ("The system remains more of a digital patchwork than an all-seeing technological network. . . . Systems that police hope will someday be powered by A.I. are currently run by teams of people sorting through photos and data the old-fashioned way.").

235. *See supra* Parts II.B.2, 4.

imagine the Supreme Court allowing real-time scans in certain locations, under certain circumstances (e.g., special events, targeted locations).[236] However, generalized use for suspicionless surveillance would run afoul of Fourth Amendment search principles.[237]

This distinction is important in order to show the gaps in Fourth Amendment coverage. The Court in *Carpenter* emphasized the "depth, breadth, and comprehensive reach"[238] of CSLI data, leaving open the question of what happens when surveillance is broad but not deep or comprehensive. This gap may need to be addressed by legislation as the Court's Fourth Amendment cases provide little guidance.

c. 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. These are situations where the scans are conducted without suspicion simply for monitoring purposes.[239] First, the fact that the images are held by third parties does not change the Fourth Amendment analysis.[240] The Supreme Court in *Carpenter* held that the Fourth Amendment applied to government acquisition of certain private third-party records that people have a reasonable expectation of privacy over.[241] While there may be an open question about whether images that individuals post publicly deserve any Fourth Amendment protection, the scans here would go beyond individual public posting. They would include billions of available photos[242] as well as the accompanying metadata (revealing location, time, etc.),[243] which is not generally thought to be publicly shared information.[244] All of the

236. *Carpenter*, 138 S. Ct. at 2222–23 ("Even though the Government will generally need a warrant to access CSLI, case-specific exceptions may support a warrantless search of an individual's cell-site records under certain circumstances.").

237. *See supra* notes 221–24 and accompanying text.

238. *Carpenter*, 138 S. Ct. at 2223.

239. *See supra* Part I.B.3.c.

240. *See supra* Part I.B.3.c.

241. *See Carpenter*, 138 S. Ct. at 2220.

242. *See supra* note 215.

243. *See* Matthews, *supra* note 71 (discussing the content of metadata embedded in digital photos, including the GPS coordinates of the location it was taken); *see also* Hanni Fakhoury, *A Picture Is Worth a Thousand Words, Including Your Location*, ELEC. FRONTIER FOUND. (Apr. 20, 2012), https://www.eff.org/deeplinks/2012/04/picture-worth-thousand-words-including-your-location [https://perma.cc/8MH6-6LYG] (discussing an FBI arrest made using metadata from photos posted to social media).

244. *Compare* Smith v. Maryland, 442 U.S. 735, 744–45 (1979) (holding that telephone customers have no legitimate expectation of privacy in phone numbers they

future-proofing principles apply to generalized suspicionless face surveillance of third-party images. Such images will reveal a great deal of information about individuals' associational connections and locations, available for search in a permanent capacity.[245] It would largely be an arbitrary use of government power to monitor all (or almost all) individuals with images in these datasets.[246] The quantity and quality of data shared is simply beyond what could ever have been found before, raising similar fears to the *Riley* case.[247]

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.[248] If the FBI decided

dial, as they were exposed to the telephone company's equipment in the ordinary course of business, thus falling outside of Fourth Amendment protections), *with* Jennifer Stisa Granick, *Debate: Metadata and the Fourth Amendment*, JUST SEC. (Sept. 23, 2013), https://www.justsecurity.org/927/metadata-fourth-amendment [https://perma.cc/3VGV-JEPT] ("While it may be obvious that phone companies have the numbers I dialed, the average consumer has no idea what a trunk identifier, IMEI or IMSI is [various types of telephone metadata], or that the phone company keeps time and duration records for toll free calls.").

245. *See* Jonah Engel Bromwich, Daniel Victor & Mike Isaac, *Police Use Surveillance Tool to Scan Social Media, A.C.L.U. Says*, N.Y. TIMES (Oct. 11, 2016), https://www.nytimes.com/2016/10/12/technology/aclu-facebook-twitter-instagram-geofeedia.html [https://perma.cc/9Q39-KDSP] (discussing a program that allowed law enforcement to access and retain user images and location data from social media platforms); Aimee Picchi, *OK, You've Deleted Facebook, but Is Your Data Still Out There?*, CBS NEWS: MONEYWATCH (Mar. 23, 2018, 5:00 AM), https://www.cbsnews.com/news/ok-you've-deleted-facebook-but-is-your-data-still-out-there [https://perma.cc/8P7F-CQ8B] (discussing certain data retained by Facebook even after users delete their accounts); Hill, *supra* note 68 ("But if your [social media] profile has already been scraped, it is too late. The [facial recognition] company keeps all the images it has scraped even if they are later deleted or taken down.").

246. *See supra* Part II.B.5.

247. *See* Riley v. California, 573 U.S. 373, 395 (2014) ("[M]any of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. . . . Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case." (citing Ontario v. Quon, 560 U.S. 746, 760 (2010))).

248. *See* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 156 (2018) (discussing how the requirement under *Clapper* that plaintiffs show "clear evidence they are being surveilled—a fact that, because of the secret nature of the surveillance" makes standing in mass surveillance cases "difficult to establish"). *But see* ACLU v. Clapper, 959 F. Supp. 2d 724, 738 (2013) (finding standing to challenge a mass surveillance program because the plaintiff's telephone metadata was in fact collected); *cf.* Rozenshtein, *supra*, at 132 (discussing the potential for technology companies to challenge mass surveillance programs based on their corporate standing).

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.[249] 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[250] but, in the general surveillance situation, it is not clear how the case would arise. That said, unlike the standing problem in *Clapper*,[251] there at least would be a digital trail linking the government action to a particular person (or group of persons),[252] 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 (albeit without using facial recognition) is already conducted regularly by law enforcement.[253] Because no Supreme Court Fourth Amendment ruling has addressed the practice of viewing non-

249. *See supra* note 225 and accompanying text.

250. Warrantless collection of a defendant's face data would meet the Court's requirement that harm "must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) (quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010)). The problem remains, however, of proving that it was in fact the facial recognition system which identified the defendant. *See* Rozenshtein, *supra* note 249, at 156 (highlighting the difficulty targets of surveillance might have in proving they were actually surveilled).

251. *See Clapper*, 568 U.S. at 409–11.

252. *See* Aaron Mak, *Facing Facts*, SLATE (Jan. 25, 2019, 12:49 PM), https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html [https://perma.cc/74NW-X3PQ] (reporting that discovery uncovered digital evidence that a criminal defendant had been identified by use of facial recognition software). Defendant Willie Allen Lynch's pro se requests and motions also found that the sheriff's office failed to disclose their use of "biometric software." Benjamin Conarck, *How an Accused Drug Dealer Revealed JSO's Facial Recognition Network*, FLA. TIMES UNION: JACKSONVILLE.COM (Nov. 11, 2016, 1:11 PM), https://www.jacksonville.com/public-safety/2016-11-11/how-accused-drug-dealer-revealed-jso-s-facial-recognition-network [https://perma.cc/7KXM-N62B]. Lynch appealed on *Brady* violation grounds, but his conviction was upheld because he could not prove he was misidentified as a result of the lower court denying him access to the other photos in the database. Mak, *supra*.

253. *See, e.g.*, Megan Behrman, *When Gangs Go Viral: Using Social Media and Surveillance Cameras to Enhance Gang Databases*, 29 HARV. J.L. & TECH. 315, 324 (2015) ("[P]olice in Cincinnati . . . created a gang database filled with information gleaned from monitoring suspects' social media accounts. Thanks to this database, the police possessed evidence that not only highlighted a given member's participation in certain crimes but also enabled them to link suspects together." (footnote omitted)).

private images[254] and because there are no clear laws on the subject,[255] this type of monitoring (at least through posted images) is a routine practice.[256] The open question is whether overlaying a facial recognition search program on top of this regular practice changes the Fourth Amendment calculus.

2. Face Identification

On the other end of the Fourth Amendment spectrum is face identification, involving the matching of digital faceprints.[257] Two types of facial recognition scans should be distinguished based on the type of dataset to be matched.[258] One type of image database consists of police-generated images (e.g., arrest photos, jail photos, suspect photos taken during investigations).[259] Another consists of larger

254. *See Cases – Search and Seizure*, OYEZ, https://www.oyez.org/issues/227 [https://perma.cc/CAS7-WSES]. *See generally* United States v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) ("When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment. . . . However, postings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected." (citation omitted)); United States v. Gatson, Crim. No. 13-705, 2014 WL 7182275, at *22 (D.N.J. Dec. 16, 2014) (denying defendant's motion to suppress evidence, gathered by police accessing his Instagram account through use of an undercover account with a false identity, on grounds that "[n]o search warrant is required for the consensual sharing of this type of information").

255. *See* Rachel Levinson-Waldman & Ángel Díaz, *How to Reform Police Monitoring of Social Media*, BROOKINGS INST.: TECHSTREAM (July 9, 2020), https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media [https://perma.cc/R3ZN-RJPU] ("[T]here are few laws that specifically constrain law enforcement's ability to engage in social media monitoring. In the absence of legislation, the strongest controls over this surveillance tactic are often police departments' individual social media policies and platform restrictions . . . ."); *see also State Social Media Privacy Laws*, NAT'L CONF. ST. LEGISLATURES, https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx [https://perma.cc/YP6X-4QAZ] (reporting no state laws shielding social media information from law enforcement).

256. *See* KIDEUK KIM, ASHLIN OGLESBY-NEAL & EDWARD MOHR, INT'L ASS'N CHIEFS POLICE & URB. INST., 2016 LAW ENFORCEMENT USE OF SOCIAL MEDIA SURVEY 3 fig.2 (2016), https://www.urban.org/sites/default/files/publication/88661/2016-law-enforcement-use-of-social-media-survey_5.pdf [https://perma.cc/9L7A-5NGA] (reporting that 70% of responding police agencies used social media for "[i]ntelligence gathering for investigations").

257. *See supra* Part I.B.2.

258. *See* Garvie & Moy, *supra* note 58 (distinguishing between the Detroit Police Department's agency-generated photo database and "Michigan's Statewide Network of Agency Photos" compiled from civil sources).

259. Schuppe, *supra* note 75 ("[F]acial recognition allows officers to submit images of people's faces, taken in the field or lifted from photos or video, and instantaneously

government image databases, like driver's license photos or passport photos, that include a large majority of the population.[260] While the two datasets raise different privacy concerns because of their respective sources and scales,[261] they share a similar Fourth Amendment analysis.

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.[262] Second, in terms of the future-proofing principles, the Supreme Court's concerns are not directly implicated,[263] thus leading to the conclusion that these are likely not Fourth Amendment searches. A facial recognition photo image match against a database of stored images would reveal an individual's identity,[264] but not necessarily their location, tracking history, or aggregated private details as it would if run against real-time surveillance or stored footage databases.[265] In addition, assuming there is some predicate level of suspicion (or internal police policy), the scan will not be arbitrary.[266] Combined with some control over their use, the scan will not be a form of pervasive surveillance. This is especially true when using already-compiled police-generated photographs (as opposed to DMV photos); there is less of a privacy harm because the photos already exist in

compare them to photos in government databases—mugshots, jail booking records, driver's licenses.").

260. *See* PEREZ, *supra* note 214, at 3 tbl.1 (finding that 93% of Americans possess a current government-recognized photo ID).

261. *Compare What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the S. Subcomm. on Priv. Tech. & the L. of the S. Comm. on the Judiciary*, 112th Cong. 3 (2012) (statement of Jerome M. Pender, Deputy Assistant Director, Criminal Justice Information Services Division, FBI) (testifying that the FBI's "national repository of photos consisting of criminal mug shots . . . contains approximately 12.8 million searchable frontal photos"), *with* PEREZ, *supra* note 214 (reporting survey results finding that 93% of Americans have a photo ID), *and U.S. and World Population Clock*, U.S. CENSUS BUREAU, https://www.census.gov/popclock [https://perma.cc/TLA5-7F3K] (estimating the U.S. population at 330.4 million). This rough estimate suggests that over 307 million Americans have their photos in civil government databases, twenty-four times as many as have their photos in the FBI's mugshot database.

262. *See, e.g.*, Jamali v. Maricopa Cnty., No. CV-13-00613, 2013 WL 5705422, at *2 (D. Ariz. Oct. 21, 2013) (holding that the Maricopa County Sheriff's "seizure and publication of Plaintiff's [mugshot] and personal information did not violate his Fourth Amendment rights").

263. *See supra* Parts II.B.1–6.

264. *See, e.g.*, Mak, *supra* note 252.

265. *See supra* Parts II.B.1–6; United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (warning of the deeply personal details that can be compiled by locational tracking information).

266. *See supra* Part II.B.5.

police custody.[267] Thus, under existing jurisprudence, it is unlikely that the Supreme Court would find Fourth Amendment harm in a face identification scenario.

As face identification is the most common use of facial recognition technology,[268] the lack of Fourth Amendment protection 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.[269] There is also no current legislation on police use of facial recognition technology,[270] raising the question, addressed in Part IV, of whether the gap should be filled with some form of legislation.

3. Face Tracking

Face tracking technology presents a more difficult Fourth Amendment analysis, but it is perhaps one of the most important. The potential capability to scan image databases or vast stores of stored video footage to find wanted suspects is quite attractive for law enforcement.[271]

Because stored video is generated by 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.[272] In addition, the ability to match target face images with the accumulated face images

267. *See Jamali*, 2013 WL 5705422, at *3 ("Plaintiff does not have a property interest in his likeness and personal information that would prevent the County from taking his picture and obtaining personal information incident to his arrest. Use of information seized incident to arrest should 'not be unduly restricted upon any fanciful theory of constitutional privilege.'" (citing Maryland v. King, 569 U.S. 435, 457 (2013))).

268. *See* GARVIE ET AL., *supra* note 3 (finding that "law enforcement face recognition affects over 117 million American adults" and "[a]t least one out of four state or local police departments has the option to run face recognition searches"); Jenni Bergal, *States Use Facial Recognition Technology To Address License Fraud*, GOVERNING (July 15, 2015), https://www.governing.com/topics/public-justice-safety/states-crack-down-on-drivers-license-fraud2.html [https://perma.cc/7ZEH-4ZMD] (reporting that "[a]t least 39 states now use [facial recognition] software in some fashion").

269. *See supra* text accompanying notes 261–67.

270. *See supra* note 254.

271. *See supra* Part I.B.3.

272. *See* Garvie & Moy, *supra* note 58 ("Thanks to face recognition technology, authorities are able to conduct biometric surveillance—pick you out from a crowd, identify you, trace your movements across a city with the network of cameras capturing your face—all completely in secret.").

contained in third-party social networks means that many more people can be identified for criminal prosecution.[273]

Again, targeted tracking is distinguishable from generalized surveillance because police are seeking to find a particular person's location, not that of all people.[274] Further, the predicate of alleged criminal activity justifies the law enforcement tracking action.[275] For example: imagine that a police department wishes to use an automated, ongoing facial recognition system to locate a "wanted" face in *stored* surveillance footage of a major city. The facial recognition system could be programmed to only identify the person with an open felony warrant while ignoring everyone else. To make that match, the system is potentially identifying all of the times the wanted face shows up in front of a camera on the streets of a city. So, the suspect's face might be observed dozens of times in a day as they are recorded by dozens of cameras in a city. This information could allow police to make an informed decision about when and how to apprehend the suspect, weighing factors such as imminence of further harm to the public, risk of escape, or further intelligence that could be gained by tracking the suspect.

To answer the open question about whether targeted face tracking is a search for Fourth Amendment purposes, one must apply the future-proofing principles discussed above.[276] As an initial matter, it should be noted that the police's ability to *manually* compare photos of targets to collected photobooks or other datasets does not end the analysis.[277] Again, "when it comes to the Fourth Amendment, digital is different."[278] As 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.[279] A manual search of all media uploaded to

273. *Cf.* Hill, *supra* note 68 (reporting that facial recognition technology was able to scan social media information to identify a suspect who did not have a driver's license and did not appear in law enforcement databases).

274. *See supra* notes 235–36 and accompanying text.

275. *See supra* Part II.B.5.

276. *See supra* Parts II.B.1–6.

277. *See* Riley v. California, 573 U.S. 373, 393–94 (2014) ("[T]he fact that a search in the predigital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery.").

278. Henderson, *supra* note 121, at 951.

279. United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring) ("In the precomputer 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.").

Facebook would take multiple lifetimes,[280] while a digital search can take mere seconds.[281] *Riley*'s "quantitative" and "qualitative" differences of digital technology is made even more obvious in the facial recognition context.[282] While a police officer could recognize a face from a "most wanted" poster while walking a city, that officer could never be able to manually examine the entire city's worth of faces over months or years.

The next three Subsections examine how the Fourth Amendment would apply to targeted investigations using three different types of face tracking. As will be clear, the analyses turn on the type of dataset being used to match faces with identities, taking in turn (1) stored footage of public areas, (2) real-time footage, and (3) third-party image datasets.

a. Face Tracking: Stored Footage

Face tracking scans using a network of stored video footage might constitute a Fourth Amendment search under *Carpenter*. Like a cell signal, such a scan would reveal where a person was over time.[283] A retrospective scan of stored video footage for a particular individual would involve police tracking a person's location over time, making inferences from the aggregated data, and keeping it for other uses,[284] thus creating the same type of Fourth Amendment harms as in *Carpenter*.[285] A mosaic of geolocational clues could be mapped to reveal a pattern of activity, tracking personal details, and exposing the privacies of one's life. Where one prays, loves, learns, and lives would all be trackable because of the identifying nature of their face. The datapoints could be aggregated and made permanently and continually

280. *See* FACEBOOK ET AL., *supra* note 216, at 6 ("More than 250 billion photos have been uploaded to Facebook, and more than 350 million photos are uploaded every day on average.").

281. Hill, *supra* note 68 (reporting that a facial recognition program scanning against social media data "was 'able to identify a suspect in a matter of seconds'").

282. *Riley*, 573 U.S. at 393–94 ("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.").

283. *See supra* Part I.B.3.a.

284. *See supra* Part I.B.3.a.

285. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("[T]ime-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.'" (quoting United States v. Jones, 565 U.S. 400, 403 (2012) (Sotomayor, J., concurring))).

searchable.[286] The requisite camera system would exert a pervasive surveillance power and, while targeted at individual suspects, would also capture information on innocent bystanders (even if they were not identified).

Again, the Supreme Court's jurisprudence has focused on the creation of systems of continuous, automatic surveillance that reveal location and personal details.[287] A stored-footage face-tracking system seems to raise the same issues. In both *Jones* and *Carpenter*, the Court was concerned with the potential tracking capabilities of the instant technologies as much as the actual details revealed about the particular defendants.[288] A face tracking system provides an even more powerful potential retrospective search system than GPS tracking or cell-site signals.[289]

Of course, open questions remain regarding 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.[290] In some cities, there

286. *See 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." (citing United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, C.J., dissenting) (mem.))).

287. In addition to Justice Sotomayor's elucidation on the personal information tracking technology can reveal, *id.* at 417–18, both concurrences in *Jones* expressed concerns with the length of the surveillance period, *id.* at 415; *id.* at 429–30 (Alito, J., concurring). *Contra id.* at 412 (majority opinion) ("[I]t remains unexplained why a 4-week investigation is 'surely' too long . . . ." (quoting *id.* at 431 (Alito, J., concurring))). Justice Alito specifically connected the ability to surveil a suspect in this manner with advancements in tracking technology. *Id.* at 429 (Alito, J., concurring).

288. 138 S. Ct. at 2210 ("[T]he rule the Court adopts 'must take account of more sophisticated systems that are already in use or in development.'" (quoting Kyllo v. United States, 544 U.S. 27, 36 (2001))). At oral arguments, Justice Sotomayor even mused about the possibility that "someday a [cellphone service] provider could turn on my cell phone and listen to my conversations." Transcript of Oral Argument, *supra* note 203, at 14.

289. *Compare* Garvie & Moy, *supra* note 58 ("Thanks to face recognition technology, authorities are able to . . . pick you out from a crowd, identify you, trace your movements across a city . . . completely in secret. [The technology] may now identify who is where, doing what, at any point in time."), *with Carpenter*, 138 S. Ct. at 2218 ("Unlike the . . . car in *Jones*, a cell phone . . . tracks *nearly* exactly the movements of its owner." (emphasis added)).

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

might be more locational details revealed than others.[291] The Fourth Amendment question might thus depend on the sophistication and scale of the technology, which offers an unsatisfying and rather happenstance constitutional answer.

b. Face Tracking: Real-Time

Real-time scans can identify whether a target is present as they pass by a facial recognition enabled camera,[292] representing a different Fourth Amendment analysis. Police could load a suspect's face image into a system and, in real-time, find their current location in a city.[293] Or the situation could involve a fixed camera outside a shooting range (preventing a wanted felon from entering and possessing a gun)[294] or a police-worn body camera automatically alerting the officer to a person with an open arrest warrant.[295]

> While the records in this case reflect the state of technology at the start of the decade, the accuracy of CSLI is rapidly approaching GPS-level precision. As the number of cell sites has proliferated, the geographic area covered by each cell sector has shrunk, particularly in urban areas. In addition, with new technology measuring the time and angle of signals hitting their towers, wireless carriers already have the capability to pinpoint a phone's location within 50 meters.

Carpenter, 138 S. Ct. at 2219 (citing Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Petitioner at 12, *Carpenter*, 138 S. Ct. 2206 (No. 16-402)).

291. *See* Paul Bischoff, *Surveillance Camera Statistics: Which Cities Have the Most CCTV Cameras?*, COMPARITECH (July 22, 2020), https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities [https://perma.cc/3NCD-42BQ] (comparing CCTV-camera-to-population ratios by city). The data upon which Comparitech researchers relied shows, for example, that Los Angeles has 49% more CCTV cameras per person than New York City. *CCTV Cameras by City and Country* (June 2020), https://docs.google.com/spreadsheets/d/1I-WpH2KOiguKy9JTQ9zC2JxBBhH2scdbSRI8lJVjzdo/edit#gid=979494433 [https://perma.cc/6DT5-WCUY].

292. *See supra* Part I.B.3.

293. *See supra* notes 72–74 and accompanying text.

294. *See, e.g.*, Mozur, *supra* note 65 (discussing a "building complex where [a] facial-recognition gate system has been installed" to keep criminals out).

295. *See* Ava Kofman, *Real-Time Face Recognition Threatens to Turn Cops' Body Cameras into Surveillance Machines*, INTERCEPT (Mar. 22, 2017, 1:23 PM), https://theintercept.com/2017/03/22/real-time-face-recognition-threatens-to-turn-cops-body-cameras-into-surveillance-machines [https://perma.cc/NFL8-HBEG] (quoting "[t]he captain of the Las Vegas Police Department" as "envision[ing] his officers someday patrolling the Strip with 'real-time analysis' on their body cameras and an earpiece to tell them, 'Hey, that guy you just passed 20 feet ago has an outstanding warrant'"); Patrick Tucker, *Facial Recognition Coming to Police Body Cameras*, DEF. ONE (July 17, 2017), https://www.defenseone.com/technology/2017/07/facial-recognition-coming-police-body-cameras/139472 [http://perma.cc/QF35-ALKU] (reporting Motorola's partnership with a startup "to build 'real-time learning for a person of interest search'").

From one perspective, the animating concerns of the future-proofing principles are somewhat mitigated. The suspect is tracked, but only to a particular location,[296] and their location need not necessarily be aggregated. The scan is not arbitrary to the target, even if it is arbitrary when directed to those innocents captured by the camera system.[297] Under this reading, the scope of privacy invasion would be real but limited, and it may not constitute a *Carpenter*-like Fourth Amendment violation.[298]

From another perspective, however, the privacy harms look less benign. In order to find one targeted suspect, a system of facial recognition tracking must be in place to cull out the non-matched.[299] Everyone is being surveilled, just not flagged. If police body cameras have the potential to scan every face,[300] vast numbers of innocent people would thus arbitrarily be included in the collection, as was the concern in *Carpenter*.[301] In addition, while the search is in real time, the images may still be stored and thus permanently accessible, undermining the limitation of the anti-aggregation principle.[302] Finally, other people accompanying a suspect will have their information collected incidental to a criminal investigation irrespective of any criminality on their part.[303] The net of associational and inferential connections will grow as never before,[304] reshaping the power the government has over individuals.[305] For this reason, real-time tracking technology is less constrained than one might think and may thus

296. *See supra* note 73 and accompanying text.

297. *See supra* Part II.B.5.

298. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) ("[W]hen the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.").

299. *See supra* note 231 and accompanying text.

300. *See* Kofman, *supra* note 295.

301. *See Carpenter*, 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 [defendant's] location but also everyone else's, not for a short period but for years and years.").

302. *See supra* Part II.B.2.

303. *See supra* note 232 and accompanying text.

304. *See supra* notes 244–46 and accompanying text.

305. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("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."); Mozur, *supra* note 65 ("China is reversing the commonly held vision of technology as a great democratizer, bringing people more freedom and connecting them to the world. In China, [facial recognition technology] has brought control.").

raise significant constitutional questions.[306] But, as may be clear, the Fourth Amendment principles do not resolve the question, and standing problems may forestall any actual Fourth Amendment litigation.[307] The issue remains open for debate and discussion until resolved by the Supreme Court or Congress.

c. Face Tracking: Third-Party-Controlled Image Searches

The scope and scale of third-party image datasets (e.g., Facebook, Google, YouTube, Instagram) are vast and growing, and now include billions and billions of images and videos.[308] Police acquisition of

306. As a parallel, this type of investigative surveillance parallels police use of "Stingray" cell-site simulators. Cell-site simulator technology allows police to find a particular cell phone among the world of cell phone signals. *See generally Cell-Site Simulators/IMSI Catchers*, ELEC. FRONTIER FOUND.: ST.-LEVEL SURVEILLANCE (Aug. 28, 2017), https://www.eff.org/pages/cell-site-simulatorsimsi-catchers [https://perma.cc/8US5-GKGR]. Using a Stingray device, police could find a particular phone in a particular apartment. *See, e.g.*, Courtney Mabeus, *Battlefield Technology Gets Spotlight in Maryland Courts: Secrecy and Defense Concerns Surround Cell Phone Trackers*, CAP. NEWS SERV. (May 3, 2016), https://cnsmaryland.org/interactives/spring-2016/maryland-police-cell-phone-trackers/index.html [https://perma.cc/H6JA-THZA] (describing a case where the location of a particular phone was tracked to a specific city bus). Baltimore police, for example, "have used the technology 4,300 times since 2007." Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, BALT. SUN (Apr. 9, 2015, 6:42 AM), https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html [https://web.achive.org/web/20201001173300/https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html]. However, the use of Stingrays in Baltimore only came to light in 2015, as police departments had been subject to "non-disclosure agreement[s] with federal authorities" that "explicitly instruct[ed] prosecutors to drop cases if pressed on the technology." *Id.* Previously, police did not seek warrants for the use of Stingrays, instead "obtain[ing] court orders under the state's 'pen register' statute . . . requir[ing] a lower standard of proof than a search warrant." *Id.* Subsequently, the Department of Justice issued guidance requiring a probable cause warrant before using these devices. *See* DEP'T OF JUST., DEPARTMENT OF JUSTICE POLICE GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 3 (2015), https://www.justice.gov/opa/file/767321/download [https://perma.cc/WU3V-XR73] ("[P]rosecutors should . . . either (1) obtain a warrant that contains all information required to be included in a pen register order . . . or (2) seek a warrant and a pen register order concurrently."). The rationale is much the same as it might be for a facial recognition search: in order to find the suspect's phone, the Stingray device searches all of the other signals in the area, increasing the attendant privacy harms. *See supra* notes 300–02 and accompanying text. To minimize the harms of collection, a higher probable cause standard was adopted. *See* DEP'T OF JUST., *supra*.

307. *See supra* notes 248–50 and accompanying text.

308. *See* FACEBOOK ET AL., *supra* note 216, at 6 ("More than 250 billion photos have been uploaded to Facebook, and more than 350 million photos are uploaded every day on average."); Anmar Frangoul, *With Over 1 Billion Users, Here's How YouTube Is Keeping Pace with Change*, CNBC (Mar. 14, 2018, 4:54 AM), https://www.cnbc.com/2018/

some subset of these images against which to run face tracking matches for identified suspects offers a new investigatory power. If police wished to investigate a suspect by acquiring third-party images of a suspect, they would be able to locate and identify more people in a fraction of the time.[309]

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.[310] Unlike cell-site signatures, photos reveal a host of associational information because of the contextual nature of the photos (e.g., what the subject matter of the photo reveals about the photographer).[311] The aggregation and permanence problems both exist since the collection of images can be searched in perpetuity.[312] 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 drawn therefrom, rather than from pure locational tracking.[313]

03/14/with-over-1-billion-users-heres-how-youtube-is-keeping-pace-with-change .html [https://perma.cc/7D86-GK6Q] (reporting a YouTube regional director's claim that the site "ha[s] over 500 hours of new content uploaded onto the platform every minute"); Olivia B. Waxman, *Here Are the 5 Most Popular Instagram Photos of All Time*, TIME (Oct. 6, 2015, 8:00 AM), https://time.com/4060078/instagram-5th-birthday -most-liked-photos [https://perma.cc/AY8N-N3K3] (reporting that over 40 billion photos were uploaded to Instagram in its first five years of existence).

309. *See supra* notes 280–81 and accompanying text.

310. *See supra* note 245 and accompanying text.

311. *See supra* notes 283–84 and accompanying text.

312. *See supra* note 243 and accompanying text; *cf.* United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, C.J., dissenting) (mem.) ("[GPS trackers] create a permanent electronic record that can be compared, contrasted and coordinated to deduce all manner of private information about individuals."), *cert. granted*, *vacated*, *remanded for consideration in light of* United States v. Jones, 565 U.S. 1189 (2012), *aff'd on remand*, 688 F.3d 1087 (9th Cir. 2012).

313. In *Riley*, the Court was concerned less with the tracking data emitted by a smartphone than with the personal information and interests contained within its memory.

> Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. . . . There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for

On the other hand, all that is being revealed are photographs or videos that confirm an individual's identity. Social media images are not a complete catalogue of movement, but instead a curated, many times inauthentic collection of human activities.[314] Complicating the analysis is the quasi-public nature of the shared photographs, as well as any privacy filters that might apply.[315] Scanning a single photograph in a third-party image database would not raise concerns,[316] 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.[317] Many social media third-party images may fall into that category,[318] but some might not,[319] and one might imagine the Supreme Court requiring a warrant similar to that in *Carpenter* in order to acquire some forms of private or quasi-private digital content from the photographs

> improving your romantic life. . . . The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life.

Riley v. California, 573 U.S. 373, 395–96 (2014) (citing Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) and Twenty-Four Technical Experts and Legal Scholars in Support of Petitioner at 9, *Riley*, 573 U.S. 373 (No. 13-132)).

314. Your Instagram friends are not always in beautiful places taking perfect photos. *See* Elspbeth Harris & Aurore C. Bardey, *Do Instagram Profiles Accurately Portray Personality? An Investigation into Idealized Online Self-Presentation*, FRONTIERS PSYCH., Apr. 2019, at 9, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6491845/pdf/fpsyg-10-00871.pdf [https://perma.cc/GV47-HURU] ("Many [participants in a study] thought that '*Instagram portrays what they* (account holders) *want their personality to be seen as*,' and that '*the best stuff is published, so there is always a false face in that respect, you know it does not show life as it is* . . . .'").

315. *See, e.g.*, United States v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) ("When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment. . . . However, postings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected." (citation omitted)).

316. *See supra* note 216 and accompanying text.

317. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) ("There is a world of difference between the limited types of personal information addressed in [other cases concerning business records] and the exhaustive chronicle of location information casually collected by wireless carriers today. . . . [M]echanically applying the third-party doctrine to this case . . . fails to appreciate that there are no comparable limitations on the revealing nature of CSLI.").

318. *See supra* notes 283–87 and accompanying text.

319. *See supra* note 252.

themselves (e.g., photo metadata).[320] But the current state of Fourth Amendment law does not resolve the question.

4. Non-Law Enforcement Purposes

The foregoing analysis all presupposes 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 in a host of situations requiring proof of identity. In these non-law enforcement situations, like international border crossings[321] or entry into secure buildings,[322] 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.[323] On one hand, the Court tries to avoid any subjective considerations of purpose that could entangle the Court in sorting through the decisions of individual officers.[324] In *Whren*, Justice Scalia stated that the officer's purpose (good or bad) was irrelevant to the Fourth Amendment analysis.[325] 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

320. *See supra* notes 243–44 and accompanying text.

321. *See* Paul S. Rosenzweig, *Functional Equivalents of the Border, Sovereignty, and the Fourth Amendment*, 52 U. CHI. L. REV. 1119, 1121 (1985) ("In exceptional circumstances, however, the government's interest may be strong enough to eliminate the warrant and probable cause requirements. The Supreme Court has held that border searches constitute such an exceptional circumstance . . . ." (footnote omitted)).

322. *See* Mozur, *supra* note 65 ("At a building complex in Xiangyang, a facial-recognition system . . . let[s] residents quickly through security gates . . . .").

323. *See* Nirej Sekhon, *Purpose, Policing, and the Fourth Amendment*, 107 J. CRIM. L. & CRIMINOLOGY 65, 66–69 (2017) (discussing inconsistencies in the Court's jurisprudence on "purpose" under the Fourth Amendment).

324. *See* Herring v. United States, 555 U.S. 135, 145 (2009) ("The pertinent analysis of deterrence and culpability is objective, not an 'inquiry into the subjective awareness of arresting officers.'" (quoting Reply Brief for Petitioner at 4–5, *Herring*, 555 U.S. 135 (No. 07-513))). *But see* 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) ("But it is difficult to reconcile that comment [in *Herring*] with the Court's acknowledgment just two sentences later that an officer's 'knowledge' is relevant in assessing good faith—as well as in evaluating probable cause." (quoting *Herring*, 555 U.S. at 145)).

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

enforcement work, the checkpoint was unconstitutional.[326] Meanwhile, the Court has distinguished other warrantless checkpoint stops where the purpose was not routine, untargeted law enforcement.[327] And, in the community caretaker cases like *Brigham City v. Stuart*, the Court stated that when the primary purpose of responding officers is to offer aid, and not investigate crimes, ordinary Fourth Amendment limitations do not apply.[328] Similar exceptions exist when police are not acting as investigators but instead under a valid "special needs" exception.[329] Finally, the Court's new exclusionary rule jurisprudence also seems to muddy the water around purpose. In *Herring*, Chief Justice Roberts required courts to evaluate objective culpability by looking at whether the officer acted in a "deliberate, reckless, or grossly negligent" manner.[330] As Justice Ginsburg argued in her dissent, evaluating deliberateness or culpability necessarily raises issues of subjective purpose and intent.[331]

Facial recognition for non-law enforcement tasks runs right into the purpose issue. If police wish to use face surveillance for public safety monitoring (e.g., at protests, events, special secure places), they could argue that their purpose was not for ordinary law

326. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000) ("The primary purpose of the Indianapolis narcotics checkpoints is in the end to advance 'the general interest in crime control' . . . . We decline to suspend the usual requirement of individualized suspicion where the police seek to employ a checkpoint primarily for the ordinary enterprise of investigating crimes." (quoting Delaware v. Prouse, 440 U.S. 648, 659 n.18 (1979))).

327. *See, e.g.*, Illinois v. Lidster, 540 U.S. 419, 427 (2004) ("The relevant public concern was grave. . . . No one denies the police's need to obtain more information at that time. And the stop's objective was to help find the perpetrator of a specific and known crime, not of unknown crimes of a general sort.").

328. *See, e.g.*, Brigham City v. Stuart, 547 U.S. 398, 403 (2006) ("Accordingly, law enforcement officers may enter a home without a warrant to render emergency assistance to an injured occupant or to protect an occupant from imminent injury." (citing Mincey v. Arizona, 437 U.S. 385, 392 (1978))).

329. *See* 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 [upheld] have included ensuring the safety of railway passengers, maintaining a positive learning environment in schools, or securing the country's borders." (footnotes omitted)).

330. Herring v. United States, 555 U.S. 135, 144 (2009); *see* Kinports, *supra* note 325, at 776 ("[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) (quoting *Herring*, 555 U.S. at 145)).

331. *Herring*, 555 U.S. at 157 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.").

enforcement.[332] Similarly, if police wished to use face tracking to locate a lost child, they could argue for an emergency exception[333] or that there was an "opt-in" choice (almost like consent) to put the child's face in the matching system.[334] Thus, purpose could create a workaround for police who wish to use facial recognition technologies, although—as in *Edmond*—the courts will have to examine the primary purpose of the systems.[335]

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, in emergency situations, or in particular locations, one might imagine that the Supreme Court could view the problem with a different lens. The clearest examples to come will be the use of face verification in established points of entry, like international borders,[336] although one can imagine how this use could expand to other areas of transport,[337] employment,[338]

332. *See* Simmons, *supra* note 329, at 155 ("In practice, the line between a search pursuant to a 'law enforcement purpose' and a search pursuant to a 'non-law enforcement purpose' can become blurred.").

333. *See, e.g.*, Kendall v. Olsen, 727 F. App'x 970, 973 (10th Cir.) (holding that a missing child justified a warrantless search on exigency grounds); United States v. Gilliam, 842 F.3d 801, 804 (2d Cir. 2016) (holding that exigency justified the warrantless GPS tracking of a suspect to locate a kidnapped minor).

334. But, as might be obvious, in order to find the child you would need to scan everyone else in the target area, *see supra* notes 293–95 and accompanying text, possibly running into the same broad versus particular distinction as in *Carpenter*. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) ("Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone."). Scholars have also critiqued the idea that any type of valid consent to facial recognition exists. *See generally* Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 101 (2020).

335. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 48 (2000) ("Because the primary purpose of the Indianapolis checkpoint program is ultimately indistinguishable from the general interest in crime control, the checkpoints violate the Fourth Amendment.").

336. *See* Rosenzweig, *supra* note 321, at 1121 ("The Supreme Court has held that border searches constitute such an exceptional circumstance [not requiring probable cause].").

337. *See* Geoffrey A. Fowler, *Why Airport Facial Recognition Raises Privacy Concerns*, WASH. POST (June 10, 2019, 3:51 PM), https://www.washingtonpost.com/technology/2019/06/10/your-face-is-now-your-boarding-pass-thats-problem [https://perma.cc/8DFY-C3XA] (reporting increased used of facial recognition technology at airports).

338. *See* S. 744, 113th Cong. § 3101(c)(1)(F)(iii) (2013) (requiring the Department

stadiums,[339] and public schools.[340] 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

Current Fourth Amendment jurisprudence 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. Face surveillance and face tracking networks likely require a probable cause warrant,[341] but more limited types of face identification using databases of stored mugshots or DMV photographs might not.[342] A continuum exists between permitting some types of police surveillance and creating "a too permeating police surveillance,"[343] but drawing the bright line is simply a constitutional guessing game. While the future-proofing principles do offer valuable guideposts for Fourth Amendment analysis along the continuum, gaps in the law 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 technology is not just about privacy but also the legitimacy of police tools and strategies.[344]

---

of Homeland Security to "develop and maintain a photo tool that enables employers to match the photo on a covered identity document . . . to a photo maintained by a U.S. Citizenship and Immigration Services database").

339. *See* Parmy Olson, *Facial Recognition's Next Big Play: The Sports Stadium*, WALL ST. J. (Aug. 1, 2020, 10:00 AM), https://www.wsj.com/articles/facial-recognitions-next-big-play-the-sports-stadium-11596290400 [https://perma.cc/A7LV-DVWZ] (reporting that "the New York Mets and the Los Angeles Football Club, are testing facial-recognition technology in stadiums").

340. *See* Tom Simonite & Gregory Barber, *The Delicate Ethics of Using Facial Recognition in Schools*, WIRED (Oct. 17, 2019, 6:00 AM), https://www.wired.com/story/delicate-ethics-facial-recognition-schools [https://perma.cc/733Q-YCS9] (reporting on schools installing facial recognition systems to "prevent major incidents such as shootings" and "to enforce school rules or simply as a convenient way to monitor students").

341. *See supra* Parts II.C.1, 3.

342. *See supra* Part II.C.2.

343. United States v. Jones, 565 U.S. 400, 416–17 (2012) (Sotomayor, J., concurring) (quoting United States v. Di Re, 332 U.S. 281, 595 (1948)).

344. *See* Geoffrey Fowler, *Black Lives Matter Could Change Facial Recognition Forever—if Big Tech Doesn't Stand in the Way*, WASH. POST (June 12, 2020, 10:13 AM),

Police legitimacy is at the core of modern Fourth Amendment debates.[345] Increased attention on stop-and-frisk policies and police use of force has caused a reexamination of structural problems of police bias, fairness, transparency, and mistakes.[346] National conversations about structural racism and policing as a mechanism of social control have exploded since George Floyd was killed by a Minneapolis police officer.[347] The same issues spill over to the introduction of new surveillance technologies like facial recognition.[348] After all, even if the

---

https://www.washingtonpost.com/technology/2020/06/12/facial-recognition-ban [https://perma.cc/26VB-YDVM] ("Ramping up [facial recognition technology] use . . . opens a slippery slope to a world of supercharged policing that's likely to disproportionately impact people of color through misidentification or just more surveillance of minority communities.").

345. *See* 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, 252 (2008) (reporting the results of a study and regression analysis indicating that "public evaluations of the justice of police decision making and the justice of the manner that the police treat members of the public both shaped police legitimacy" to a statistically significant degree). Applying those findings to Fourth Amendment issues, one scholar suggested that:

> [p]olice/citizen encounters involving searches and seizures are just the kind of personal experiences that, according to Fagan and Tyler, shape public views of police legitimacy and, with it, the prevalence of law-abiding behavior by the public and its willingness to help police. Everyone wants public safety and less crime; the vitality of our cities and towns depends on it.

David A. Harris, *How Accountability-Based Policing Can Reinforce—or Replace—the Fourth Amendment Exclusionary Rule*, 7 OHIO ST. J. CRIM. L. 149, 164 (2009).

346. *See, e.g.*, Barry Friedman, *Amid Calls to 'Defund,' How to Rethink Policing*, WALL ST. J. (June 13, 2020, 12:01 AM), https://www.wsj.com/articles/amid-calls-to-defund-how-to-rethink-policing-11592020861 [https://perma.cc/SW9L-QZ4K]; Barry Friedman, *Disaggregating the Police Function*, U. PA. L. REV. (forthcoming 2020–21).

347. *See, e.g.*, Mariame Kaba, *Yes, We Mean Literally Abolish the Police*, N.Y. TIMES (June 12, 2020), https://www.nytimes.com/2020/06/12/opinion/sunday/floyd-abolish-defund-police.html [https://perma.cc/DBQ6-REDB]; Annie Lowrey, *Defund the Police*, ATLANTIC (June 5, 2020), https://www.theatlantic.com/ideas/archive/2020/06/defund-police/612682 [https://perma.cc/24CK-NE4U]; Jon Schuppe, *What Would It Mean to 'Defund the Police'? These Cities Offer Ideas*, NBC NEWS (June 11, 2020, 9:55 AM), https://www.nbcnews.com/news/us-news/what-would-it-mean-defund-police-these-cities-offer-ideas-n1229266 [https://perma.cc/VM4D-2WMC]; Alex S. Vitale, *The Only Solution Is to Defund the Police*, NATION (May 31, 2020), https://www.thenation.com/article/activism/defund-police-protest [https://web.archive.org/web/20200607032550/https://www.thenation.com/article/activism/defund-police-protest].

348. As a direct result of the protests arising from the police killing of George Floyd, some large technology companies have paused their development or deployment of facial recognition systems for police. *See* Brian Fung, *Microsoft Says It Won't Sell Facial Recognition Technology to US Police Departments*, CNN BUS. (June 11, 2020), https://www.cnn.com/2020/06/11/tech/microsoft-facial-recognition-police/index.html

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 answered.[349]

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 prohibition or legislation is needed to counteract these systemic weaknesses.

[https://perma.cc/DZF7-CUHE]; Nick Statt, *Amazon Bans Police from Using Its Facial Recognition Technology for the Next Year*, VERGE (June 10, 2020, 5:37 PM), https://www.theverge.com/2020/6/10/21287101/amazon-rekognition-facial-recognition-police-ban-one-year-ai-racial-bias [https://web.archive.org/web/20200610221350if_/https://www.theverge.com/2020/6/10/21287101/amazon-rekognition-facial-recognition-police-ban-one-year-ai-racial-bias]; Bobby Allyn, *IBM Abandons Facial Recognition Products, Condemns Racially Biased Surveillance*, NPR (June 9, 2020, 8:04 PM), https://www.npr.org/2020/06/09/873298837/ibm-abandons-facial-recognition-products-condemns-racially-biased-surveillance [https://perma.cc/2TR7-7CP7].

349. *See* Tawana Petty, *Defending Black Lives Means Banning Facial Recognition*, WIRED (July 10, 2020, 8:00 AM), https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition [https://perma.cc/7EHA-N8S9]; Devich-Cyril, *supra* note 5; *see also* Alvaro M. Bedoya, *The Color of Surveillance*, SLATE (Jan. 18, 2016, 5:55 AM), https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html [https://perma.cc/SH8R-EH6B]; Dorothy Roberts & Jeffrey Vagle, Opinion, *Racial Surveillance Has a Long History*, HILL (Jan. 4, 2016, 5:11 PM), http://thehill.com/opinion/op-ed/264710-racial-surveillance-has-a-long-history [https://perma.cc/Q32V-MBFB]. *See generally* ALEX S. VITALE, THE END OF POLICING (2017).

A. ETHICAL AI AND CONCERNS ABOUT ERROR, BIAS, FAIRNESS, AND TRANSPARENCY

In the computer science and data analytics fields, ethical use of artificial intelligence is now a topic of serious conversation.[350] Hard questions about error, bias, fairness, and transparency are increasingly part of the ongoing conversation about how to build "better" facial recognition technologies.[351] 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.[352] 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.[353] Further, without

350. *See, e.g.*, *ACM FAccT,* ASS'N FOR COMPUTING MACH. CONF. ON FAIRNESS, ACCOUNTABILITY & TRANSPARENCY, https://facctconference.org/index.html [https://perma.cc/5WLQ-DS86] ("Although these [algorithmic] systems may bring myriad benefits, they also contain inherent risks, such as codifying and entrenching biases; reducing accountability, and hindering due process; they also increase the information asymmetry between individuals whose data feed into these systems and big players capable of inferring potentially relevant information. ACM FAccT is an interdisciplinary conference dedicated to bringing together a diverse community of scholars from computer science, law, social sciences, and humanities to investigate and tackle issues in this emerging area."); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. 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.").

351. Barocas & Selbst, *supra* note 350; *see also* Irina Ivanova, *Why Face-Recognition Technology Has a Bias Problem*, CBS NEWS (June 12, 2020, 7:57 AM) https://www.cbsnews.com/news/facial-recognition-systems-racism-protests-police-bias [https://perma.cc/Q7ZU-4R33].

352. *See* SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM (2018) (discussing how search engine algorithms perpetuate bias by producing stereotypical, offensive, and stigmatizing results); VIRGINIA EUBANKS, AUTOMATING INEQUALITY 37 (2018); CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016) (discussing how bias that is written into algorithms has far-reaching, negative consequences); *cf.* FRANK PASQUALE, THE BLACK BOX SOCIETY 18 (2015) ("Corporations depend on automated judgments that may be wrong, biased, or destructive. The black boxes of reputation, search, and finance endanger all of us. Faulty data, invalid assumptions, and defective models can't be corrected when they are hidden."). 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 [https://perma.cc/32RE-CAYQ].

353. *See* Danielle Keats Citron & Frank A. Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014) (discussing how data ranking creates stigmatization in AI scoring systems); *cf.* RUHA BENJAMIN, RACE AFTER TECHNOLOGY:

oversight, artificial intelligence systems could similarly reify existing structural bias or exacerbate inequalities, all the while claiming to be data-driven, neutral, and objective.[354] In the specific context of facial recognition technology, the questions become even more pointed.[355]

First, face surveillance does not always work as intended. Real concerns have been demonstrated about the accuracy of face surveillance matches.[356] 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.[357] But, even in more controlled environments there have been errors resulting in false matches—in one notable story, twenty-eight members of Congress were falsely matched with arrestee mugshots using commercially available face identification software.[358] Even the National

ABOLITIONIST TOOLS FOR THE NEW JIM CODE 112–13 (2019) (discussing misguided use of electronic surveillance by private companies in the movement for decarceration); Paul Ohm, *The Underwhelming Benefits of Big Data*, 161 U. PA. L. REV. ONLINE 339, 340 (2012), https://www.pennlawreview.com/wp-content/uploads/2020/05/161-U-Pa-L-Rev-Online-339.pdf [https://perma.cc/U3FS-B9M8] ("But some Big Data projects will also lead to bad outcomes, like invasion of privacy and hard-to-detect invidious discrimination.").

354. *See* Selbst, *supra* note 1, at 115–16 (arguing that the use of AI systems in policing enhances racial disparities through discrimination in data mining); Pratyusha Kalluri, *Don't Ask If Artificial Intelligence Is Good or Fair, Ask How It Shifts Power*, NATURE (July 7, 2020), https://www.nature.com/articles/d41586-020-02003-2 [https://perma.cc/N9MY-M8G9] ("These [AI] systems sometimes mitigate harm, but are controlled by powerful institutions with their own agendas. At best, they are unreliable; at worst, they masquerade as 'ethics-washing' technologies that still perpetuate inequality."); *cf.* 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) ("Personal harms emerge from the inappropriate inclusion and predictive analysis of an individual's personal data without their knowledge or express consent.").

355. Devich-Cyril, *supra* note 5 (arguing that facial recognition technology is an inaccurate tool employed in discriminatory contexts and propagates disparities for communities of color); ERIK LEARNED-MILLER, VICENTE ORDÓÑEZ, JAMIE MORGENSTERN & JOY BUOLAMWINI, FACIAL RECOGNITION TECHNOLOGIES IN THE WILD: A CALL FOR A FEDERAL OFFICE 3–4 (2020), https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_FRTsFederalOfficeMay2020.pdf [https://perma.cc/5BGG-ML6V].

356. Garvie & Moy, *supra* note 58; BUOLAMWINI ET AL., *supra* note 16, at 14–16 (discussing how small differences in inputs can create dramatic accuracy issues in facial recognition technology).

357. Charlotte Jee, *London Police's Face Recognition System Gets It Wrong 81% of the Time*, MIT TECH. REV. (July 4, 2019), https://www.technologyreview.com/2019/07/04/134296/london-polices-face-recognition-system-gets-it-wrong-81-of-the-time [https://perma.cc/X4J6-TL3V].

358. Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018, 8:00 AM), https://www.aclu.org/blog/

Institute of Standards and Technology (NIST) found significant errors in facial recognition vendor tests,[359] especially in attempting to identify women of color.[360] The problems involve both intrinsic and extrinsic factors, including the way in which photos are captured and the complexities of facial features and human movement.[361] This error/accuracy problem, however, could be short-lived as improvements in big data pattern matching will allow companies to improve their error/accuracy rates year by year.[362]

Error for facial recognition has real consequences, as a match can lead to investigations, arrests, and prosecution. The danger of false positive hits leads to false arrests,[363] and the consequence for such a false match means a coercive and potentially dangerous encounter with police.[364] In the context of face surveillance, with tens of

privacytechnology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [https://perma.cc/9JS3-6TRM].

359. PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, NAT'L INST. STANDARDS & TECH., INTERNAL REP. 8280, FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 2–3 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf [https://perma.cc/4VEW-SD7F]; *see also* Sophie Bushwick, *How NIST Tested Facial Recognition Algorithms for Racial Bias*, SCI. AM. (Dec. 27, 2019), https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias [https://perma.cc/9JFT-GV22] ("NIST's tests revealed that many of these algorithms were 10 to 100 times more likely to inaccurately identify a photograph of a black or East Asian face, compared with a white one. In searching a database to find a given face, most of them picked incorrect images among black women at significantly higher rates than they did among other demographics.").

360. GROTHER ET AL., *supra* note 359, at 63; *see also* Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, WASH. POST (Dec. 19, 2019, 5:43 PM), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use [https://perma.cc/8967-B8VM].

361. Joshi & Gupta, *supra* note 20, at 59 (recognizing intrapersonal problems such as "age, facial expression and facial details/equipment used (facial hair, glasses, cosmetics, veil, etc.)" and extrinsic issues such as "illumination, pose, scale and imaging parameters (e.g., resolution, focus, imaging, noise, etc.)" as causing a myriad of challenges in algorithmic recognition techniques).

362. Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, WIRED (July 22, 2019, 7:00 AM), https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally [https://perma.cc/H8KP-AGPC] ("NIST said last year that the best algorithms got 25 times better at finding a person in a large database between 2010 and 2018 . . . .").

363. Hill, *supra* note 68; Torres, *supra* note 76; Kris Holt, *Facial Recognition Linked to a Second Wrongful Arrest by Detroit Police*, ENGADGET (July 10, 2020), https://www.engadget.com/facial-recognition-false-match-wrongful-arrest-224053761.html [https://perma.cc/KS46-YWGW].

364. Williams, *supra* note 82; *cf.* Jeremy C. Fox, *Brown University Student Mistakenly Identified as Sri Lanka Bombing Suspect*, BOS. GLOBE (Apr. 28, 2019, 5:42 PM), https://

thousands of faces being scanned every day, the reality of inaccurate matching technology will create significant practical problems.[365] In the field, it may be hard for an individual officer to override the suspicion of the algorithm, leading to some erroneous stops and some missed investigations.[366] 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.[367] 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

www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html [https://perma.cc/RZK4-WVXD] (describing the emotional distress of receiving death threats and calls for death of mistaken identity victim).

365. *See, e.g.*, Timothy B. Lee, *Detroit Police Chief Cops to 96-Percent Facial Recognition Error Rate*, ARS TECHNICA (June 30, 2020, 11:12 AM), https://arstechnica.com/tech-policy/2020/06/detroit-police-chief-admits-facial-recognition-is-wrong-96-of-the-time [https://perma.cc/DX2G-986E]; Tim Cushing, *Detroit Police Chief Says Facial Recognition Software Involved in Bogus Arrest Is Wrong '96 Percent of the Time*,' TECHDIRT (July 2, 2020, 3:30 AM), https://www.techdirt.com/articles/20200629/17423944814/detroit-police-chief-says-facial-recognition-software-involved-bogus-arrest-is-wrong-96-percent-time.shtml [https://perma.cc/9FC8-H2QU]; *see also* Joy Buolamwini, *Artificial Intelligence Has a Problem with Gender and Racial Bias. Here's How to Solve It*, TIME (Feb. 7, 2019, 7:00 AM), http://time.com/5520558/artificial-intelligence-racial-gender-bias [https://perma.cc/9USJ-K94C] ("[F]ailed machine learning systems . . . amplify, rather than rectify, sexist hiring practices, racist criminal justice procedures, predatory advertising, and the spread of false information."); Garvie & Frankle, *supra* note 15 ("[N]ot only are African Americans more likely to be misidentified by a facial-recognition system, they're also more likely to be enrolled in those systems and be subject to their processing.").

366. *See, e.g.*, *supra* note 363 (identifying examples of misidentification by police using facial recognition technology).

367. BENJAMIN, *supra* note 353, at 109 ("The power of the New Jim Code is that it allows racist habits and logics to enter through the backdoor of tech design, in which the humans who create the algorithms are hidden from view."); Buolamwini, *supra* note 352 (discussing how algorithmic bias amplifies discrimination); Sahil Chinoy, Opinion, *The Racist History Behind Facial Recognition*, N.Y. TIMES (July 10, 2019), https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html [https://perma.cc/DP34-4MWR] ("[N]ew applications of facial recognition—not just in academic research, but also in commercial products that try to guess emotions from facial expressions—echo the same biological essentialism behind physiognomy."); Joy Boulamwini, Opinion, *When the Robot Doesn't See Dark Skin*, N.Y. TIMES (June 21, 2018), https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html [https://perma.cc/UV8U-YV93] ("A.I. systems are shaped by the priorities and prejudices—conscious and unconscious—of the people who design them . . . .").

poor job of identifying faces of other races,[368] especially black women,[369] and non-conforming individuals.[370] The systemic bias in the datasets[371] is coupled with incomplete, incorrect, and fragmented data,[372] which leads to a system that discriminates against anyone but white men and almost completely erases transgender, non-conforming, or non-binary individuals.[373] As the bias tracks along race and

368. Buolamwini, *supra* note 365 ("[O]ne government dataset of faces collected for testing . . . contained 75% men and 80% lighter-skinned individuals and less than 5% women of color . . . ."); Tom Simonite, *Photo Algorithms ID White Men Fine—Black Women, Not So Much*, WIRED (Feb. 6, 2018, 6:21 PM), https://www.wired.com/story/photo-algorithms-id-white-men-fineblack-women-not-so-much [https://perma.cc/M5CM-JNXR] ("All the companies' [facial recognition] services had particular trouble recognizing that photos of women with darker skin tones were in fact women."); Simonite, *supra* note 362 ("The easiest place to gather huge collections of faces is from the web, where content skews white, male, and western.").

369. Joy Buolamwini, *When AI Fails on Oprah, Serena Williams, and Michelle Obama, It's Time to Face the Truth*, MEDIUM (July 4, 2018), https://medium.com/@Joy.Buolamwini/when-ai-fails-on-oprah-serena-williams-and-michelle-obama-its-time-to-face-truth-bf7c2c8a4119 [https://perma.cc/AQC8-PQES] ("Error rates were as high as 35% for darker-skinned women . . . ."); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 1, 11 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf [https://perma.cc/Z2XX-GSB3] ("The most improvement is needed on darker females specifically.").

370. *Cf.* Cynthia M. Cook, John J. Howard, Yevgeniy B. Sirotin, Jerry L. Tipton & Arun R. Vemury, *Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*, INST. ELEC. & ELEC. ENG'RS TRANSACTIONS ON BIOMETRICS, BEHAV. & IDENTITY SCI. (Feb. 2019), https://ieeexplore.ieee.org/document/8636231 [https://perma.cc/5HB5-HAT2] ("Our analyses show that demographic factors influenced both the speed and accuracy of all eleven commercial biometric systems evaluated.").

371. MICHELE MERLER, NALINI RATHA, ROGERIO FERIS & JOHN R. SMITH, IBM RSCH., DIVERSITY IN FACES 4 (2019), https://arxiv.org/pdf/1901.10436.pdf [https://perma.cc/Z5BU-XXP9] ("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.").

372. *See* Garvie & Moy, *supra* note 58 (describing many unreliable methods for gathering photos for police facial recognition searches).

373. *Facial Recognition Technology: Its Impact on Our Civil Rights and Liberties: Before the H. Comm. on Oversight & Gov't Reform*, 116th Cong. 15 (2019) (statement of Joy Buolamwini, Founder, Algorithmic Justice League) ("[W]hen evaluating error rates for 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."); Ali Alkhatib et al., *On Recent Research Auditing Commercial Facial Analysis Technology*, MEDIUM (Mar. 26, 2019), https://medium.com/@bu64dcjrytwitb8/on-recent-research

gender lines, mistakes could also follow those patterns.[374] In some cases, it will mean that people with darker skin will be missed by the system, but in others, the matches will be less accurate.[375]

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.[376] 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.[377] 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.[378] In a computer design situation, the model's outcome can be directly impacted by the type of fairness deemed optimal.[379] 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

-auditing-commercial-facial-analysis-technology-19148bda1832 [https://perma.cc/W7SJ-38P2] ("[C]urrent gender classification methods use only a 'male' and 'female' binary—non-binary genders are not represented in these systems.").

374. *Cf.* Buolamwini & Gebru, *supra* note 369 (discussing current disparities among racial and gender groups in facial recognition AI systems).

375. *See* Garvie & Frankle, *supra* note 15 ("[E]ven if the features on which an algorithm focuses are race-neutral, a training set of images that contains disproportionate numbers of one race will bias the algorithm's accuracy rates in that direction.").

376. Ziyuan Zhong, *A Tutorial on Fairness in Machine Learning*, MEDIUM (Oct. 21, 2018), https://towardsdatascience.com/a-tutorial-on-fairness-in-machine-learning-3ff8ba1040cb [https://perma.cc/HL42-9ZEJ] ("[D]efinitions, however, are too abstract for the purpose of computation. As a result, there is no consensus on the mathematical formulations of fairness.").

377. *See, e.g.*, Andrew D. Selbst, danah boyd, Sorelle A. Friedler, Suresh Venkatasubramanian & Janet Vertesi, *Fairness and Abstraction in Sociotechnical Systems*, CONF. ON FAIRNESS, ACCOUNTABILITY & TRANSPARENCY 59 (2019), https://dl.acm.org/doi/pdf/10.1145/3287560.3287598 [https://perma.cc/V79B-WULJ]; Richard Berk, Hoda Heidari, Shahin Jabbari, Michael Kearns & Aaron Roth, *Fairness in Criminal Justice Risk Assessments: The State of the Art*, SOCIO. METHODS & RSCH. (forthcoming) (manuscript at 12–15), https://arxiv.org/pdf/1703.09207.pdf [https://perma.cc/W86U-9DP7].

378. *See* Selbst et al., *supra* note 377, at 59 ("[T]hese [fairness] concepts render technical interventions ineffective, inaccurate, and sometimes dangerously misguided when they enter the societal context that surrounds decision-making systems.").

379. *See id.*

a lack of accountability.[380] The artificial intelligence and machine learning community has long confronted issues of transparency, secrecy, accountability, inscrutability, interpretability, and explainability.[381] 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 enter 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

380. *See, e.g.*, Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 19, 20 (2017), https://www.nyulawreview.org/wp-content/uploads/2017/08/NYULawReviewOnline-92-Joh_0.pdf [https://perma.cc/AX4Z-TGGR] ("[A]ggressive assertions of secrecy about proprietary information may mean that the press, the courts, and the public have no access to the technology shaping substantive decisions about who should be subjected to police attention."); Brent Mittelstadt, Chris Russell & Sandra Wachter, *Explaining Explanations in AI*, CONF. ON FAIRNESS, ACCOUNTABILITY & TRANSPARENCY 279, 279 (2019) ("What distinguishes machine learning is its use of arbitrary black-box functions to make decisions. These black-box functions may be extremely complex and have an internal state composed of millions of interdependent values.").

381. Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085, 1090 (2018).

merely negligent errors.[382] The only time the Supreme Court appears to punish police error is if it is intentional, reckless, grossly negligent, systemic, or recurring—a high bar to clear.[383] This Section examines the extent of error allowed in Fourth Amendment doctrine to show how limited the Fourth Amendment would be as a guide to regulating error in facial recognition design.

a. Error and Reasonable Suspicion

The legal standard of "reasonable suspicion,"[384] 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.[385] 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."[386] In subsequent cases, the Court has acknowledged that reasonable suspicion can involve completely

382. *See, e.g.*, Herring v. United States, 555 U.S. 135, 144 (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."); *see also* 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.").

383. Davis v. United States, 564 U.S. 229, 238 (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 the 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' . . . ." (citations omitted)).

384. The rule comes from *Terry v. Ohio*, a case which involved Officer McFadden, an experienced police officer, watching the unusual behavior of John Terry and two associates outside a store in downtown Cleveland, Ohio. Terry v. Ohio, 392 U.S. 1, 5–6 (1968). McFadden believed the men were "casing" the store in preparation for a robbery, so he approached, stopped, and frisked them, and found an illegal handgun on John Terry. *Id.* In justifying 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. *Id.* at 33.

385. Heien v. North Carolina, 574 U.S. 54, 60–61 (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.* at 61 ("[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.").

386. *Terry*, 392 U.S. at 21.

innocent conduct,[387] can be based on less than perfectly reliable information, and should be evaluated under a "totality of circumstances" test.[388] 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.[389] In fact, courts have been emphatic in refusing to quantify the certainty of reasonable suspicion.[390] 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 20% to 30% level of "certainty,"[391] although one survey of judges had a broader range of 10% to 50%.[392] Reasonable suspicion is more than a hunch but less than probable cause, and no matter what "number" is chosen within this accepted range, the threshold to reach reasonable suspicion has a huge margin of error (again taking the average—somewhere between 70% to 80% of police suspicion can be mistaken and yet be constitutional).[393]

387. 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.").

388. Alabama v. White, 496 U.S. 325, 330 (1990) ("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.").

389. *See* Ric Simmons, *Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in Our Criminal Justice System*, 2016 MICH. ST. L. REV. 947, 964.

390. *Id.* ("[C]ourts have been unwilling to explicitly quantify the percentage chance for 'reasonable suspicion'. . . .").

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

392. 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 a reasonable suspicion, their estimates ranged from 50% at the high end to 10% at the low end."); *see also* Simmons, *supra* note 390, at 1005 ("[J]udges 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.").

393. Given the 20% to 30% chance of success cited by Slobogin, it can be surmised that 70% to 80% would then be unsuccessful products of reasonable suspicion. Slobogin, *supra* note 391.

For a facial recognition system, this uncertainty means that the error rate for a match could be significant (and yet constitutional).[394] Both false positives and false negatives may occur, and within the existing percentages many individuals could be incorrectly stopped based on erroneous matches.[395] 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 and 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.[396] The standard originates from the text of the Fourth Amendment, but despite this provenance, its meaning has never been established in any single definition.[397] The Supreme Court has articulated several formulations over the years, but has generally agreed that probable cause should be "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'"[398] or when "there is a fair probability that contraband or evidence of a crime will be found in a particular place."[399] The Court has

394. The human equivalent of this process would be an officer erroneously believing the person who just walked past him has an open warrant based on a misidentification of the person.

395. The variables that can be factored into the matching system (creating reasonable suspicion of a match) are wide open. *See* Garvie & Moy, *supra* note 58. The "totality of circumstances" does not exclude many factors, leaving design parameters open.

396. 5 AM. JUR. 2D *Arrest* § 9 (2020) ("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."). *See generally* Andrew Manuel Crespo, *Probable Cause Pluralism*, 129 YALE L.J. 1276, 1280 (2020) (discussing how pluralism in the meaning of probable cause creates no clear guidance in judicial interpretation of the standard).

397. Crespo, *supra* note 396, at 1279 ("[T]wo centuries after the Supreme Court first applied the phrase [probable cause], scholars continue to describe it as 'elusive,' 'hopelessly indeterminate,' and 'shrouded in mystery.'").

398. Gerstein v. Pugh, 420 U.S. 103, 111 (1975) (alteration in original) (citation omitted).

399. Illinois v. Gates, 462 U.S. 213, 238 (1983) ("The 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

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, reduced to a neat set of legal rules."[400] Because the standard is meant to be used in the real world, the Supreme Court has emphasized its "practical, common-sense" application[401] and specifically refused to offer any quantification.[402] Generally, the objective test is whether a "man of reasonable caution" or "reasonably prudent person" would judge that a crime had been committed.[403] Reasoned probability, not certainty, is the requirement, meaning that mistakes are baked into the standard.[404]

Scholars, judges, and law enforcement agents examining probable cause in practice have attempted to quantify this probability with some general consensus.[405] As Professor Ric Simmons has written, "Most commentators also agree that probable cause is something

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.").

400. *Id.* at 232; *see also* 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 (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.").

401. *Gates*, 462 U.S. at 244 ("[W]e think it suffices for the practical, common-sense judgment called for in making a probable-cause determination.").

402. 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.").

403. 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." (citation omitted)); 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.").

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

405. Simmons, *supra* note 389, at 987–88 ("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))); *id.* at 988 n.165 ("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."). *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).

close to but just less than 50%, while scattered evidence from prosecutors and law enforcement point to numbers between 40% and 51%."[406] The quantum of evidence is certainly greater than reasonable suspicion.[407] 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,[408] can base their decisions on inferences,[409] and their judgment can be mistaken.[410]

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 to arrest an individual matched by the computer system. In fact, four fairly recent Supreme

406. Simmons, *supra* note 389, at 1005; *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"); Henderson, *supra* note 391, at 38–39 ("Some think probable cause requires a preponderance of the evidence, whereas I think it a slightly less, albeit inarticulable, measure."); Slobogin, *supra* note 391 (reporting 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) (reporting 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) (reporting anecdotal account of FBI agent stating probable cause is 51%).

407. 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 . . . .").

408. 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.").

409. 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 officers where none exists."); Richardson, *supra* note 392, at 1155 ("[C]ourts consistently fail to determine whether the inferences drawn by the officer conducting the stop are actually *entitled* to any weight.").

410. Sherry F. Colb, *Probabilities in Probable Cause and Beyond: Statistical Versus Concrete Harms*, 73 LAW & CONTEMP. PROBS. 69, 69 (2010) ("'[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).").

Court cases have involved errors in arrest warrants.[411] 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[412] and raised the bar for qualified immunity for Fourth Amendment violations in the civil legal system.[413] 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 systemic or recurring problems.[414] 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.[415] As Chief Justice Roberts wrote in *Herring v. United States*:[416]

> 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.[417]

411. *See* Florence v. Bd. of Chosen Freeholders, 566 U.S. 318 (2012); Herring v. United States, 555 U.S. 135 (2009); Rothgery v. Gillespie Cnty., 554 U.S. 191 (2008); Arizona v. Evans, 514 U.S. 1 (1995).

412. *See, e.g.*, Jennifer E. Laurin, *Trawling for* Herring*: Lessons in Doctrinal Borrowing and Convergence*, 111 COLUM. L. REV. 670, 684 (2011) (noting when the Court first began to apply the exclusionary rule to police misconduct covered by the Fourth Amendment).

413. *Id.* at 671–77 (analyzing the evolution of the impact the Court's decisions have on the exclusionary rule and qualified immunity doctrines).

414. Andrew Guthrie Ferguson, *Constitutional Culpability: Questioning the New Exclusionary Rules*, 66 FLA. L. REV. 623, 639 (2014) (detailing cases regarding a "culpability-centered exclusionary rule").

415. Utah v. Strieff, 136 S. Ct. 2056 (2016); Davis v. United States, 564 U.S. 229 (2011); Herring v. United States, 555 U.S. 135 (2009).

416. *Herring*, 555 U.S. at 136.

417. *Id.* at 144.

In practical effect, this means that the negligent error of a police officer or police employee will not result in suppression.[418]

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.[419] Only intentional or reckless or systemic instances of error will warrant an exclusionary rule remedy.[420] While rights and remedies are certainly different, this forgiving of error allows a greater freedom for mistakes. If merely negligent, an error in a facial recognition match will have no consequence for police investigation.[421]

418. The Court held that "the error was the result of isolated negligence attenuated from the arrest." *Id.* at 137. Four relatively recent Supreme Court cases involved arrests based on police errors. *See* Florence v. Bd. of Chosen Freeholders, 566 U.S. 318 (2012); *Herring*, 555 U.S. 135; Rothgery v. Gillespie Cnty., 554 U.S. 191 (2008); Arizona v. Evans, 514 U.S. 1 (1995). The Court also 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. Baker v. McCollan, 443 U.S. 137, 144–46 (1979). *See generally* Andrew D. Selbst, *Negligence and AI's Human Users*, 100 B.U. L. REV. (forthcoming 2020) (noting that the use of artificial intelligence by police is not regulated by tort law, and discussing the need to adapt oversight of emerging technologies to ensure negligence law works as intended).

419. Interestingly *Herring* itself was a case about data error, specifically, how a mistake in a computer database did not justify suppression because there was no evidence of systemic or recurring problems. *Herring*, 555 U.S. at 135–36. Herring was arrested because a database search erroneously stated that he had an open felony arrest warrant. *Id.* at 137. However, the database was not updated, and by the time the investigating agent learned of the mistake, drugs and a gun were recovered on Herring's person. *Id.* at 138. In refusing to exclude the evidence, the Court suggested that merely negligent data errors would not be the subject of constitutional remedy. *Id.* at 146. 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 (2016) ("[R]esearch has long documented significant quality problems with criminal justice databases . . . ."); *id.* at 543 ("[T]he prevailing zeitgeist of governments [includes] . . . a blasé acceptance of data error and its negative consequences for individuals."); *see also Herring*, 555 U.S. at 155–56 (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 *Evans*, 514 U.S. at 23 (Stevens, J., dissenting))).

420. *See, e.g.*, Andrew Guthrie Ferguson, *The Exclusionary Rule in the Age of Blue Data*, 72 VAND. L. REV. 561, 591–94 (2019) (describing why even systemic instances of error do not always warrant Fourth Amendment suppression).

421. Similarly, civil remedies ordinarily effectuated by lawsuits against police officers have also been limited by an expanded qualified immunity doctrine. *See, e.g.*, Arthur H. Garrison, *Criminal Culpability, Civil Liability, and Police Created Danger: Why and How the Fourth Amendment Provides Very Limited Protection from Police Use of*

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.[422] Yet, intentional or unintentional racial bias does not factor into the Fourth Amendment calculus (although it may raise equal protection or due process concerns).[423] 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.[424] In hundreds of investigations, lawsuits, media stories, and

Deadly Force, 28 GEO. MASON U. C.R.L.J. 241, 246–61 (2018) (describing the Supreme Court's civil immunity jurisprudence). 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. *Id.* Moreover, the layers of legal rules scaffolding the qualified immunity doctrine and § 1983 doctrine make individual civil rights cases rare to bring and even rarer to win. *See, e.g.*, Andrew Chung, Lawrence Hurley, Jackie Botts, Andrea Januta & Guillermo Gomez, *For Cops Who Kill, Special Supreme Court Protection*, REUTERS: REUTERS INVESTIGATES (May 8, 2020, 12:00 PM), https://www.reuters.com/investigates/special-report/usa-police-immunity-scotus [https://perma.cc/8D8Q-7D6P] (scrutinizing the impact of Supreme Court decisions on police immunity for excessive use of force suits). Most false stop or arrests cases do not get litigated. *Id.*

422. *See, e.g.*, Paul Butler, *The System Is Working the Way It Is Supposed To: The Limits of Criminal Justice Reform*, 104 GEO. L.J. 1419, 1458–66 (2016) (analyzing multiple long term studies on the impact of racial bias on policing practices); Meares, *supra* note 108, at 162 (characterizing stop-and-frisk as a policing program); Richardson, *supra* note 240, at 1170 (discussing the impact of implicit bias on shoot/don't shoot decisions); L. Song Richardson, *Arrest Efficiency and the Fourth Amendment*, 95 MINN. L. REV. 2035, 2061–63 (2011) (discussing the impact of implicit racial bias on the development of police hunches).

423. Whren v. United States, 517 U.S. 806, 813 (1996) ("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.").

424. *See* Monica C. Bell, *Police Reform and the Dismantling of Legal Estrangement*, 126 YALE L.J. 2054, 2071 (2017) ("A large body of historical research has documented the entanglement of police in the long-running national project of racial control."); M. Adams & Max Rameau, *Black Community Control over Police*, 2016 WIS. L. REV. 515, 527 ("The specific system of power used to enforce the economic and social relationship between low-income Black communities in the United States and the larger White community in general, and corporate interests in particular, is the domestic colony. In the context of the domestic colony, the police are responsible for maintaining the coercive exploitative and oppressive relationship by serving as an occupying force in low-income Black communities."). *See generally* VITALE, *supra* note 349 (making the case for police reform to stop systemic racial bias); PAUL BUTLER, CHOKEHOLD: POLICING

personal anecdotes the reality of racial bias in policing has been made plain.[425] Especially in urban areas with higher crime rates, the problems of explicit and implicit bias and structural racism persist.[426]

Despite this reality, the Supreme Court has refused to allow the Fourth Amendment to be a vehicle to address racial bias in individual cases.[427] In *Whren*,[428] 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."[429] This understanding that racial bias is largely irrelevant to policing decisions has essentially foreclosed Fourth Amendment claims based on racial

BLACK MEN 59–61 (2017) (describing the power the Supreme Court gave officers to legally stop vehicles and the use by police in racial profiling practice).

425. *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) (stating stop-and-frisk is a continuation of racial subordination that began with slavery); R. Richard Banks, *Beyond Profiling: Race, Policing, and the Drug War*, 56 STAN. L. REV. 571 (2003) (making the argument to abandon efforts to eliminate racial profiling and instead focus on the consequences); BEYOND THE RODNEY KING STORY: AN INVESTIGATION OF POLICE CONDUCT IN MINORITY COMMUNITIES 24, 52–53 (Charles J. Ogletree et al. eds., 1995) (describing how abuse of stop-and-frisk is perpetuated by the reluctance of minority communities to report police abuse); *see also* C.R. DIV., U.S. DEP'T OF JUST., INVESTIGATION OF THE FERGUSON POLICE DEPARTMENT 2–3 (2015) [hereinafter DOJ FERGUSON REPORT], https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_report.pdf [https://perma.cc/W7NS-9CSB] (discussing how police practices that promote "productivity" over community relations lead to a negative relationship between police and minority neighborhoods in Ferguson, Missouri); C.R. DIV., U.S. DEP'T OF JUST., INVESTIGATION OF THE BALTIMORE CITY POLICE DEPARTMENT 24 (2016) [hereinafter DOJ BALTIMORE REPORT], https://www.justice.gov/crt/file/883296/download [https://perma.cc/U4CT-49ZN] (describing how "zero tolerance" enforcement strategies lead to systemic and widespread stop, search, and arrests that violate the Fourth Amendment).

426. Cedric Merlin Powell, *The Structural Dimensions of Race: Lock Ups, Systemic Chokeholds, and Binary Disruptions*, 57 U. LOUISVILLE L. REV. 7, 8 (2018) (stating that disproportionately high rates of incarceration for African Americans and Latinos makes the criminal justice system a leading source of racial inequality); Scott Holmes, *Resisting Arrest and Racism—the Crime of "Disrespect,"* 85 UMKC L. REV. 625, 637–38 (2017) (discussing structural racism in the context of implicit and explicit racial bias and how it is presented within policing).

427. 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) (stating that *Whren* legitimized racial profiling by denying that a police officer's intentions when making a stop have any bearing on Fourth Amendment analysis).

428. Whren v. United States, 517 U.S. 806 (1996).

429. *Id.* at 813.

discrimination.[430] 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.[431] In the pattern matching context, this would mean that a system programmed 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.[432] "[H]igh crime areas,"[433] "drug courier

430. 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)).

431. Simmons, *supra* note 389, at 971 ("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, 887 (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.").

432. Simmons, *supra* note 389, at 976–77; *see also* 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) (describing the impact of New York City's zero tolerance policing strategy).

433. Illinois v. Wardlow, 528 U.S. 119, 124 (2000); Simmons, *supra* note 389, at 976 ("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.").

profile[s],"[434] incongruity,[435] and immigration-related stops[436] all rely on proxies for individuals who have historically been targeted by police.[437] 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).[438]

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,[439] or the system could be programmed for tattoo recognition as a proxy for gang involvement (and thus criminality).[440] 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

434. 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." (first citing United States v. Mendenhall, 446 U.S. 544 (1980); and then citing Florida v. Royer, 460 U.S. 491 (1983))).

435. 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.'").

436. *Brignoni-Ponce*, 422 U.S. at 880.

437. *See generally* David Rudovsky, *Law Enforcement by Stereotypes and Serendipity: Racial Profiling and Stops and Searches Without Cause*, 3 U. PA. J. CONST. L. 296, 307 (2001) (describing arguments used to defend racially disparate police practices).

438. Richardson, *supra* note 422, at 2080 ("Some courts currently allow officers to rely on race and proxies for race (such as consideration of high-crime neighborhoods) to justify *Terry* seizures."); Rudovsky, *supra* note 437, at 304.

439. 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.").

440. *See generally* Aaron Mackey, Dave Maass & Soraya Okuda, *5 Ways Law Enforcement Will Use Tattoo Recognition Technology*, ELEC. FRONTIER FOUND. (June 2, 2016), https://www.eff.org/deeplinks/2016/05/5-ways-law-enforcement-will-use-tattoo-recognition-technology [https://perma.cc/4SQH-RGQB] (discussing tattoo recognition technology tested by the FBI and National Institute of Standards and Technology and relating it to similar technologies already used or being contracted for use by various police departments).

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,[441] and especially darker skinned women.[442]

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 remains an aspirational goal for police. Police are supposed to enforce the law the same regardless of race, class, age, gender, or neighborhood.[443] 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.[444] As a matter of procedural

441. *See* Garvie & Frankle, *supra* note 15.

442. Steve Lohr, *Facial Recognition Is Accurate, If You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html [https://perma.cc/47EG-Q6XH].

443. *Cf.* Tracey L. Meares & Tom R. Tyler, *Justice Sotomayor and the Jurisprudence of Procedural Justice*, 123 YALE L.J.F. 525, 539 (2014) ("[Experience of fairness is determined by] considering both the fairness of decisionmaking and the fairness of treatment."); Stephen D. Mastrofski, Jeffrey B. Snipes & Anne E. Supina, *Compliance on Demand: The Public's Response to Specific Police Requests*, 33 J. RSCH. CRIM. & DELINQ. 269, 277 (1996) (studying compliance in police interactions and finding procedural fairness increases compliance with police).

444. *See* Andrew Kahn & Chris Kirk, *What It's Like to Be Black in the Criminal Justice System*, SLATE (Aug. 9, 2015, 12:11 PM), https://slate.com/news_and_politics/crime/2015/08/racial-disparities-in-the-criminal-justice-system-eight-charts-illustrating-how-its-stacked-against-blacks.html [https://perma.cc/Z49Q-PHMM] (using charts to demonstrate how blacks are discriminated against at nearly every level of the criminal justice system); Brad Heath, *Racial Gap in U.S. Arrest Rates: 'Staggering Disparity,'* USA TODAY (Nov. 19, 2014, 2:24 PM), https://www.usatoday.com/story/news/nation/2014/11/18/ferguson-black-arrest-rates/19043207 [https://perma.cc/H4RQ-Z5L7] (discussing various factors that result in blacks being arrested at the highest rates of all racial groups). *See generally* Tate Ryan-Mosely & Jennifer Strong, *The Activist Dismantling Racist Police Algorithms*, MIT TECH. REV. (June 5, 2020), https://www.technologyreview.com/2020/06/05/1002709/the-activist-dismantling-racist-police-algorithms [https://perma.cc/3TQQ-DD92] (describing a grassroots effort in L.A. to dismantle police artificial intelligence programs that perpetuate racism).

fairness,[445] procedural justice,[446] or just common experience, police treat different people differently.[447] And sadly, from a Fourth Amendment perspective, "fairness" defined as equal treatment of people, groups, and places has never been constitutionally required.[448]

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.[449] 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,[450] use of force, and surveillance all undermine a claim of a fair (i.e., uniform and equal) application of the Fourth Amendment. Some

445. 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) ("*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)." (citing Justice Tankebe, *Viewing Things Differently: The Dimensions of Public Perceptions of Police Legitimacy*, 51 CRIMINOLOGY 103 (2013))).

446. Tyler & Fagan, *supra* note 345, at 264–65; *see also* Tracey Meares, *The Legitimacy of Police Among Young African-American Men*, 92 MARQ. L. REV. 651, 657–66 (2009) (describing police practices that can promote legitimacy and procedural justice).

447. 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) (commenting that order-maintenance and subsequently attendant *Terry* stop policing priorities impact police legitimacy); Devon W. Carbado, *(E)racing the Fourth Amendment*, 100 MICH. L. REV. 946, 952 (2002) (describing how microaggressions generated by policing activity that targets black people has negative social effects).

448. *Cf.* Christopher Slobogin, *The Poverty Exception to the Fourth Amendment*, 55 FLA. L. REV. 391, 401 (2003) (finding unfairness in the Supreme Court's Fourth Amendment decisions that adversely affect less affluent and privileged groups).

449. *Id.* ("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.").

450. 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.").

communities bear the brunt of police tactics with no relief provided by the Fourth Amendment.[451] 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.[452]

For purposes of building a facial recognition matching system, the same tension between ideals and application arises. The ideal of fairness, meaning applying the same decision-making rules to similar problems, is present.[453] AI systems are good at procedural fairness rules.[454] 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).[455] 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.[456] 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.[457]

Beyond unequal treatment, the Fourth Amendment also has little to say about unequal or disparate effects of policing. Policing resources historically are not equally distributed across society.[458] Police respond to crime patterns, strategic assessments, and political pressure, and those influences do not result in an equal distribution of

451. 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.").

452. *See generally* DAVID COLE, NO EQUAL JUSTICE: RACE AND CLASS IN THE AMERICAN CRIMINAL JUSTICE SYSTEM (2010).

453. *See supra* Part II.C.

454. Machines, after all, follow the process designed by the computer engineers.

455. *See* Ryan-Mosely, *supra* note 444.

456. *See supra* Part II.

457. *See supra* Part II.C.4.

458. 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).

police resources across a community.[459] Some neighborhoods are over-policed and some under-policed, and in both police have been criticized as being unfair.[460] Distributive fairness has never been realized or really a priority.[461] The Fourth Amendment neither mandates equal policing resources nor freedom from policing attention.[462]

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

Police decision-making is decidedly not transparent.[463] 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

459. *See generally* Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109 (2017) (manipulating police response factors to improve predictive policing).

460. *See* John Cassidy, *The Statistical Debate Behind the Stop-and-Frisk Verdict*, NEW YORKER (Aug. 13, 2013), https://www.newyorker.com/news/john-cassidy/the-statistical-debate-behind-the-stop-and-frisk-verdict [https://perma.cc/FT7P-QZTZ] (analyzing the S.D.N.Y. court's interpretation of statistical data for New York City's stop-and-frisk program, finding it unconstitutional for indirectly racially profiling minorities).

461. Reynolds et al., *supra* note 445, at 120 ("*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)." (citing Justice Tankebe, *Viewing Things Differently: The Dimensions of Public Perceptions of Police Legitimacy*, 51 CRIMINOLOGY 103 (2013))).

462. *Cf.* Stoughton, *supra* note 458 and accompanying text (demonstrating the differences in police resources and attention across diverse groups).

463. *See* 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.").

mind prevent an accurate understanding.[464] Police officers, like everyone else, see a distorted world without noticing the distortions.[465] While there are some *ex post* mechanisms for recording the observations of officers (e.g., police reports, testimony, recordings of body camera footage), these types of formal memorialization are limited in scope and value.[466]

As mentioned, the Supreme Court has stated that subjective reasoning of police officers is largely irrelevant for Fourth Amendment purposes.[467] 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.[468] The goal, instead, is to look for objective justifications for a stop, not actual reasons.[469] 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[470] or a reasonable mistake of law,[471] as long as there are some objective justifications for their actions.[472]

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.[473] More than occasionally, police have been affirmatively

464. *See* Megan Quattlebaum, *Let's Get Real: Behavioral Realism, Implicit Bias, and the Reasonable Police Officer*, 14 STAN. J.C.R. & C.L. 1, 10 (2018).

465. *See id.* at 10–13.

466. *But see* Sharad Goel, Maya Perelman, Ravi Shroff & David Alan Sklansky, *Combatting Police Discrimination in the Age of Big Data*, 20 NEW CRIM. L. REV. 181, 182 (2017) (using recorded data to understand police patterns).

467. *See* 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 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.").

468. *See King*, 563 U.S. at 464 (reasoning that "[l]egal tests based on reasonableness are generally objective," and allow for fairer law enforcement than do subjective examinations).

469. *See id.*

470. *See* Illinois v. Rodriguez, 497 U.S. 177, 185–86 (1990).

471. *See* Heien v. North Carolina, 574 U.S. 54, 62 (2014).

472. *See* 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.").

473. *See* 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

secretive.[474] At both operational and institutional levels, local governments have avoided various transparency initiatives and have occasionally fought them.[475] 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.[476] The result has been that the reasons for police decisions, training standards, and protocols remain under-examined, if not completely opaque.[477] 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.[478] 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

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.").

474. *See* 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.").

475. *See* Harmon, *supra* note 473, at 1133 ("[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.").

476. *See* 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."); 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."); *NYPD Predictive Policing Document*, BRENNAN CTR. FOR JUST. (July 12, 2019), https://www.brennancenter.org/analysis/nypd-predictive-policing-documents [https://perma.cc/5WUH-QTR9].

477. *See* Harmon, *supra* note 475 and accompanying text.

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

be challenged. All that has mattered to the Court has been that there was an objective justification; the actual reason does not matter. 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 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.[479] 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

479. Renan, *supra* note 108, at 1041–42 ("While our Fourth Amendment framework is transactional, then, surveillance is increasingly *programmatic*."); Slobogin, *supra* note 108, at 97; Meares, *supra* note 108, at 162.

front lines of quick discretionary decisions. Police, as ordinary people, get things wrong.[480] As the Court recognized in *Heien v. North Carolina*, "[t]o 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.'"[481] The Supreme Court has forgiven mistakes of fact[482] and mistakes of law.[483] Within this "human" forgiveness, the Supreme Court emphasizes the quickness required for immediate decisions, the complexity of human behavior and observations, and the one-off nature of decision-making.[484] In addition, the Court forgives error because Fourth Amendment law can be technical and hard to interpret.[485]

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.[486] Dragnet sweeps, roadblocks, and other types of broad-based suspicionless searches for law enforcement

480. *See* 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.").

481. Heien v. North Carolina, 574 U.S. 54, 60–61 (2014) (quoting *Brinegar*, 338 U.S. at 176).

482. *See Heien*, 574 U.S. at 61 ("We have recognized that searches and seizures based on mistakes of fact can be reasonable." (citing Illinois v. Rodriguez, 497 U.S. 177, 183–86 (1990))); Hill v. California, 401 U.S. 797, 802–05 (1971).

483. *See Heien*, 574 U.S. at 61 ("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.").

484. *See* Kentucky v. King, 563 U.S. 452, 466 (2011) ("[T]he 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." (quoting Graham v. Connor, 490 U.S. 386, 396–97 (1989))); Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388, 418 (1971) ("Inadvertent errors of judgment that do not work any grave injustice will inevitably occur under the pressure of police work.").

485. *See* 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' is no more tenable for police today than it is for the lay public.").

486. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 33 (2000).

purposes are not favored.[487] The reason in part is because police administrators have the ability to craft constitutionally respectful rules before implementing the plans.[488] Absent special needs or special circumstances, the Supreme Court has been reluctant to allow systems of general suspicionless searches for ordinary law enforcement purposes.[489] The more planned the practice is, the less deferential the Court appears.[490] In the case of a designed system of facial recognition technology, any deference would seem to drop away to a fully programmatic (i.e., computer-programmed) 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.[491] Fourth Amendment rights are decided in one-off settings where systemic or structural error is not presented.[492] 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 violations have been found in cities like

487. *See id.* at 37 (illustrating how searches are considered unreasonable without individualized suspicion).

488. *See* Logan, *supra* note 485, at 101 (explaining how police enjoy the power and opportunities to enact more laws to seize and prosecute).

489. *See* FRIEDMAN, *supra* 224, at 143–84 (explaining the difference between cause based and suspicionless searches).

490. *See* Ferguson v. City of Charleston, 532 U.S. 67, 81 (2001) ("In looking to the programmatic purpose, we consider all the available evidence in order to determine the relevant primary purpose.").

491. *See* Logan & Ferguson, *supra* note 419, at 579 (explaining that suits against individual officers remain the main avenue for victims of wrongful search or seizure).

492. *But see* Ferguson, *supra* note 420, at 591 (discussing the promise of litigating systemic or recurring error through the use of new data-driven technologies).

Chicago,[493] Baltimore,[494] Philadelphia,[495] New York City,[496] and most famously Ferguson, Missouri.[497] The Department of Justice Civil Rights Division has opened sixty-nine investigations and entered into forty reform agreements.[498] Since 2012, the DOJ Civil Rights Division has "opened 11 new pattern-or-practice investigations and negotiated 19 new reform agreements."[499]

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.[500] Similarly, in *Utah*

493. C.R. DIV., U.S. DEP'T OF JUST. & U.S. ATT'Y'S OFF. N. DIST. OF ILL., INVESTIGATION OF THE CHICAGO POLICE DEPARTMENT 23 (2017), https://www.justice.gov/opa/file/925846/download [https://perma.cc/U8W6-6C9G].

494. DOJ BALTIMORE REPORT, *supra* note 425.

495. *See* Plaintiffs' First Report to Court and Master on Stop and Frisk Practices at 7, Bailey v. City of Philadelphia, No. 10-5952 (E.D. Pa. 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]; *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.").

496. *See* 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.* 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) (finding that nine independent police stops illustrated misconduct); Davis v. City of New York, 902 F. Supp. 2d 405, 412–30 (S.D.N.Y. 2012) (illustrating seven instances of NYPD 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) (illustrating how the settlement of the *Daniels* case "mandated procedures for NYPD officers to record the rationale for stops" due to deficiency in the program).

497. *See* DOJ FERGUSON REPORT, *supra* note 425.

498. C.R. DIV., U.S. DEP'T OF JUST., THE CIVIL RIGHTS DIVISION'S PATTERN AND PRACTICE POLICE REFORM WORK: 1994–PRESENT 3 (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.").

499. *Id.* at 1.

500. Herring v. United States, 555 U.S. 135, 146 (2009) ("In a case where systemic errors were demonstrated, it might be reckless for officers to rely on an unreliable warrant system.").

v. Strieff, both the majority and dissent recognized that proof of systemic violations would have impacted the analysis.[501]

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.[502] One would hope that intentionally choosing an 80% error rate in a facial recognition system (following reasonable suspicion rules) qualifies as recklessly promoting error. And, because *Herring* talks 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.[503] 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.

501. Strieff v. Utah, 136 S. Ct. 2056, 2063 (2016) ("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.").

502. *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.").

503. *See* DOJ FERGUSON REPORT, *supra* note 425, at 3–4; DOJ BALTIMORE REPORT, *supra* note 269; 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."); Fagan & Geller, *supra* note 496, at 69 (providing empirical data to demonstrate violations of the Fourth and Fourteenth Amendments).

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, 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 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.[504] 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.[505] 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 legal 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 programmed 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 it 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

504. Whren v. United States, 517 U.S. 806, 813 (1996).

505. *See* United States v. Sokolow, 490 U.S. 1, 7 (1990).

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 address issues of bias, fairness, transparency, and error.

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;[506] (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 following discussion attempts to interweave the technologies and legal analysis discussed in Parts I and 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

506. *See* Alfred Ng, *Lawmakers Propose Indefinite Nationwide Ban on Police Use of Facial Recognition*, CNET (June 25, 2020), https://www.cnet.com/news/lawmakers-propose-indefinite-nationwide-ban-on-police-use-of-facial-recognition [https://perma.cc/TUE3-JE93].

and identify individuals without individualized suspicion and to discover personal information about their location, interests, or activities should simply be banned by law.[507]

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[508] 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, and tracking, 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.[509] In fact, underlying the Supreme Court's recent Fourth Amendment reasoning about privacy in public is a realization that surveillance chills First Amendment protected activity.[510] Free expression, association, petitioning for redress, and political dissent all will be negatively impacted by face surveillance systems.[511] Police have already shown a willingness to use surveillance technologies to monitor dissenting voices,[512] and face surveillance will only strengthen that power. In

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

508. *See supra* Part III.C.3.

509. *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) (discussing Fourth Amendment searches in which the police accesses recordings in public that they would otherwise not be able to see or hear). Public surveillance in violation of the Fourth Amendment can have a chilling effect on the First Amendment.

510. *See* Alex Abdo, *Why Rely on the Fourth Amendment To Do the Work of the First?*, 127 YALE L.J.F. 444, 445 (2017).

511. *See* Kelly & Lerman, *supra* note 69; Boyd, *supra* note 69.

512. *See* George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, INTERCEPT (July 24, 2015, 1:50 PM), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson [https://perma.cc/LTZ2-V3LR]; Darwin BondGraham, *Counter-Terrorism Officials Helped Track Black Lives Matter Protestors*, E. BAY EXPRESS (Apr. 15, 2015), https://www.eastbayexpress.com/oakland/counter-terrorism-officials

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.[513] By eroding what Woodrow Hartzog and Evan Selinger term the "practical obscurity" of public activity,[514] face surveillance raises significant First and Fourth Amendment concerns and provides ample reason to ban its use.[515] In sum, generalized face surveillance should be banned under federal law, with the only exceptions being for emergency or non-law enforcement uses. Some cities have already enacted local bans.[516]

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 may not be constitutionally required under today's doctrine, 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

-helped-track-black-lives-matter-protesters/Content?oid=4247605 [https://perma.cc/4AGG-HKVP].

513. *See* Woodrow Hartzog & Evan Selinger, *Why You Can No Longer Get Lost in the Crowd*, N.Y. TIMES (Apr. 17, 2019), https://www.nytimes.com/2019/04/17/opinion/data-privacy.html [https://perma.cc/9QQ2-9N4J].

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

515. *See* 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).

516. *See, e.g.*, Caroline Haskins, *Oakland Becomes Third U.S. City To Ban Facial Recognition*, VICE (July 17, 2019, 6:41 AM), https://www.vice.com/en_us/article/zmpaex/oakland-becomes-third-us-city-to-banfacial-recognition-xz [https://perma.cc/N3X3-S9F7]; Jon Schuppe, *San Francisco's Facial Recognition Ban Is Just the Beginning of a National Battle over the Technology*, NBC NEWS, https://www.nbcnews.com/news/us-news/san-francisco-s-facial-recognition-ban-just-beginning-national-battle-n1007186 [https://perma.cc/M7XY-XLU2] (May 22, 2019, 2:09 PM); Rachel Metz, *California Lawmakers Ban Facial-Recognition Software from Police Body Cams*, CNN BUS. (Sept. 13, 2019, 8:04 AM), https://www.cnn.com/2019/09/12/tech/california-body-cam-facial-recognition-ban/index.html [https://perma.cc/NHF8-PHGQ].

that the quantitatively and qualitatively different capabilities of digital matching require caution and greater court oversight.[517]

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 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.[518] 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.[519] 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.[520]

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 qualitatively different capabilities of AI-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[521] and the capacity to search these millions of innocent faces is simply too powerful without regulation.[522]

517. *See* Petrescu, *supra* note 19.

518. *See supra* Part I.B.

519. U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-267, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY (2016), https://www.gao.gov/assets/680/677098.pdf [https://perma.cc/E9XK-8S93].

520. *See supra* Part I.B.

521. Kaveh Waddell, *Half of American Adults Are in Police Facial-Recognition Databases*, ATLANTIC (Oct. 19, 2016), https://www.theatlantic.com/technology/archive/2016/10/half-of-american-adults-are-in-police-facial-recognition-databases/504560 [https://perma.cc/8U5T-QVWJ].

522. Evan Selinger & Woodrow Hartzog, *Amazon Needs To Stop Providing Facial Recognition Tech for the Government*, MEDIUM (June 21, 2018), https://medium.com/s/story/amazon-needs-to-stop-providing-facial-recognition-tech-for-the-government-795741a016a6 [https://perma.cc/BYX2-5Y7N].

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.[523] The result would be that every photograph in police possession or every photo taken through police-worn body cameras could be uploaded to see if a face identification match occurs (with all the images permanently stored for future searches).[524] 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. Interposing a judge in the process will also provide an additional check to minimize human error or a rush to target an individual.[525]

Second, the requirement of a 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.[526] 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 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.[527]

As an added benefit, the warrant process will generate a written record allowing for a measure of transparency, accountability, and avoidance of abuse.[528] Probable cause warrants are not simply about justifying an intrusion into personal privacy but also about documenting the use after the fact.[529] Written records will reveal the scale,

523. *See supra* Part II.C.3.

524. *See supra* Part II.C.3.a.

525. *See* Williams, *supra* note 82.

526. *See supra* Part I.B.2.

527. Such a process has been proposed for other new digital technologies. *See* Natalie Ram, Christi J. Guerrini & Amy L. McGuire, *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).

528. *See, e.g.*, *Wiretap Report 2017*, U.S. CTS. (Dec. 31, 2017), https://www.uscourts.gov/statistics-reports/wiretap-report-2017 [https://perma.cc/2TJ4-G5HN].

529. *See, e.g.*, *id.*

scope, and efficacy of the programs and also allow regular auditing and accountability.[530] 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.[531] 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.[532]

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.[533] The technological process and surveillance power is the same, but the purpose is to find a particular person at a location, not generalized 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.[534] Systems of surveillance will exist and be difficult to deconstruct or limit.[535] 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 use the face surveillance capabilities of the video camera systems.[536] Trusting police to use a judicial

530. *See, e.g.*, *id.*

531. *E.g.*, Drew Harwell, *Police Have Used Celebrity Look-Alikes, Distorted Images To Boost Facial-Recognition Results, Research Finds*, WASH. POST (May 16, 2019), https://www.washingtonpost.com/technology/2019/05/16/police-have-used-celebrity-lookalikes-distorted-images-boost-facial-recognition-results-research-finds [https://perma.cc/JUQ9-LNDF].

532. *See* Ben Conarck, *Florida Courts Could Decide How Police Use Facial Recognition Tech*, FLA. TIMES-UNION (Mar. 12, 2018), https://www.govtech.com/public-safety/Florida-Courts-Could-Decide-How-Police-Use-Facial-Recognition-Tech.html [https://perma.cc/G7UN-R3EW]; Mak, *supra* note 252.

533. *See supra* Part I.B.

534. *See supra* Part II.

535. *See supra* Part II.B.7.

536. *See, e.g.*, Petty, *supra* note 349; Devich-Cyril, *supra* note 5; Evan Selinger & Woodrow Hartzog, *What Happens When Employers Can Read Your Facial Expressions?*, N.Y. TIMES (Oct. 17, 2019), https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html [https://perma.cc/ZHE7-GB9X]; Luke Stark, *Facial Recognition Is the Plutonium of AI*, XRDS: CROSSROADS, Apr. 2019, at 50, 52–55, https://xrds.acm.org/article.cfm?aid=3313129 [https://perma.cc/65PQ-CFX6]; Evan Greer, *Don't*

process or trusting that the legislative limits will not change is not a risk advocates 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 should 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 (e.g., mugshots, 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). Having thought about the issue carefully, were I given the choice, I would vote to ban face tracking because of a lack of structural checks to prevent misuse against marginalized communities and dissenting voices. The history of policing shows little reason to have faith that the systems of surveillance would not be abused.[537]

If, however, legislatures wished to allow carefully regulated police face tracking capabilities, legislation could authorize use of face tracking for limited crimes and only with a heightened legal process. One option would be to allow face tracking only on a probable cause-plus standard for the most serious violent crimes, 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.[538] 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.[539] As will be discussed below, while a significant risk to liberty, this proposal fills the gaps of Fourth Amendment protection, offers significantly more protection than the constitutional floor, and responds to the different ways digital surveillance technologies will expand in scope and scale over time.

Regulate Facial Recognition. Ban It., BUZZFEED NEWS (July 18, 2019), https://www.buzzfeednews.com/article/evangreer/dont-regulate-facialrecognition-ban-it [https://perma.cc/WEQ7-J7WS]; Woodrow Hartzog & Evan Selinger, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 [https://perma.cc/Q992-YHKE].

537. *See* Vitale, *supra* note 347.

538. GRAY, *supra* note 527.

539. *Id.*

The analogy here to the Wiretap Act is admittedly imperfect but offers a working model for legislation.[540] 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 in addition to a few other requirements.[541]

The Wiretap Act is built around several limitations. First, it is limited to specific enumerated crimes, most of which are serious felonies.[542] 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.[543] Notably, this process has been used without significant complaint for decades by investigators and the courts in the context of communications evidence.[544]

In the facial recognition context, a parallel process should be relatively easy to implement because all that would be required is a showing of probable cause that a serious felony violent crime had been committed, a declaration that the face tracking search was

540. 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* Donohue, *supra* note 527; Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3; Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1280 (2004).

541. 18 U.S.C. § 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;
>
> (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. § 2518(4).

542. *Id.* § 2518.

543. *Id.*

544. *See Wiretap Reports*, U.S. CTS. (2020), https://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports [https://perma.cc/8VAG-ANJE] (reporting information provided by federal and state officials on applications for wiretaps).

necessary because there were no other ways to obtain an identification, a statement about how other images of innocent people would be minimized (e.g., 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). The limitation for only serious crimes would bar the use of facial recognition to investigate property-based or quality of life crimes and non-violent incidents.

For some forms of targeted face tracking (e.g., stored footage scans, third-party images scans with metadata), this type of probable cause-plus standard is not only an important check on police power 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). To be clear, the dangers of face tracking outweigh the advantages and, especially at this early stage of development, the technology filled with error, marred by bias, and embedded in structural problems of police power should be banned along with face surveillance.

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.[545]

As this Article largely focuses on domestic law enforcement use of facial recognition, the regulation of face verification is slightly misaligned, but the technology exposes related dangers. 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,[546] one could imagine that face verification could be used to confirm identity. In addition, as the dissenting

545. *See* Joshi & Gupta, *supra* note 19, at 58 (describing uses such as "electoral registration, banking, electronic commerce, identifying newborn babies, establishing national IDs, passports, driving licenses, employee IDs and so on").

546. Hiibel v. Sixth Jud. Dist. Ct. of Nev., 542 U.S. 177, 182 (2004).

Justices acknowledged in *Utah v. Strieff*, police have been known to use warrant checks as a pretext to stop individuals.[547] With face verification, this warrant-check justification could lead to the use or abuse of facial recognition technology in pedestrian stops or car stops. Similarly, narcotics interdiction stops on busses and trains have become a routine practice.[548] 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.[549]

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 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,[550] the Fourth Amendment has little purchase,[551] and individuals are already presenting themselves with government issued identification to prove

547. Utah v. Strieff, 136 S. Ct. 2056, 2068 (2016) (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 id.* at 2073 (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.").

548. United States v. Drayton, 536 U.S. 194, 197 (2002).

549. Maryland v. King, 569 U.S. 435, 449 (2013).

550. United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985) ("Consistently, therefore, with Congress's 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.").

551. Rosenzweig, *supra* note 321, at 1119 ("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.").

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.[552] After the match, the digital image is destroyed.[553] While entry and exit records are maintained, the face image taken is not.[554] 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, Fairness, and Transparency

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 and forbid use if the technology does not pass the test.[555] For example, as a precondition to utilizing any form of 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 be conducted by independent researchers.[556] Similarly, after adoption, auditing measures to continue to test the technology could be required.[557] 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 and ensure that the technology is improving in accuracy and precision and not harming particular communities.[558]

552. *See supra* notes 42–43.

553. *See supra* notes 42–43.

554. *See supra* notes 42–43.

555. *See* Learned-Miller et al., *supra* note 355 (promoting an FDA-like regulation structure to minimize harmful errors).

556. *See, e.g.*, Ali Alkhatib et al., *supra* note 373; Inioluwa Deborah Raji & Joy Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*, *in* PROCEEDINGS OF THE 2019 AAAI/ACM CONFERENCE ON AI, ETHICS, AND SOCIETY 429 (2019).

557. *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 519 (discussing the need for auditing); *see also* U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-579T, DOJ AND FBI HAVE TAKEN SOME ACTIONS IN RESPONSE TO GAO RECOMMENDATIONS TO ENSURE PRIVACY AND ACCURACY, BUT ADDITIONAL WORK REMAINS (2019) (statement of Gretta L. Goodwin, Director of Homeland Security & Justice for the U.S. Government Accountability Office before the House Committee on Oversight and Reform), https://www.gao.gov/assets/700/699489.pdf [https://perma.cc/SLT5-8A72].

558. *See* Raji & Buolamwini, *supra* note 556.

To address concerns about bias, certification and auditing could include testing to track how facial recognition is used on people of different races, ethnicities, genders, ages, or other demographic characteristics. Of particular importance, the training data and on-going data being fed into the system should be revealed. 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 and include individuals from all races, genders, and orientations in the creation of the technologies.[559] Systems that cannot show through audits that the technology avoids bias should not be adopted. Systems that have not incorporated and consulted with impacted communities should not be authorized.

In addition, legislation could require public reporting about how facial recognition technologies are deployed. Surveillance tools automatically raise discrimination concerns, so if past is prologue, the use of the technology will impact poor communities and communities of color more than other groups.[560] The history of policing in America supports an acute awareness that technology has been weaponized as a mechanism of social control.[561] 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.[562] 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 and unregulated systems of police surveillance power.

Fairness is a hard concept to legislate because the initial fairness choices will all be baked into the design.[563] 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

559. *See generally supra* Part I.A.

560. *See* Bedoya, *supra* note 349; Roberts & Vagle, *supra* note 349.

561. *See* Vitale, *supra* note 347; PAUL BUTLER, CHOKEHOLD: POLICING BLACK MEN 59–61 (2017); Roger A. Fairfax, Jr., *The Grand Jury and Police Violence Against Black Men*, *in* POLICING THE BLACK MAN: ARREST, PROSECUTION, AND IMPRISONMENT 209, 209–33 (Angela J. Davis ed., 2017).

562. Garvie & Moy, *supra* note 58.

563. *See supra* Part I.A.

can all be included as a mechanism to check abuses. The costs for failing to comply with legislative requirements must be significant enough to encourage adoption of best practices in terms of privacy, civil liberties, and civil rights.

Most importantly in terms of fairness, legislatures should ensure that due process protections are protected for criminal defendants.[564] 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, impeach a witness, undermine the government's investigation of the case, or 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.[565] This preplea and pretrial disclosure would include all search queries used, near matches not used in the photo array, documentation of the process, underlying validation and testing results, and information about any alterations or changes made to the photographs.

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 issued.[566] A public report of how facial recognition was used, in what types of cases, by whom, and the results can be required by statute.[567] In combination with the auditing provision that recertifies and protects against error and bias, these types of reporting requirements can generate a measure of public trust.

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

564. *See* Jack Karp, *Facial Recognition Software Sparks Transparency Battle*, LAW360 (Nov. 3, 2019), https://www.law360.com/articles/1215786/facial-recognition-software-sparks-transparency-battle [https://perma.cc/7DVC-GSXK]; Jason Tashea, *As Facial Recognition Software Becomes More Ubiquitous, Some Governments Slam on the Brakes*, A.B.A. J. (Sept. 24, 2019), https://www.abajournal.com/web/article/facial-recog-bans [https://perma.cc/A7PQ-GM29]; Mak, *supra* note 252.

565. Mak, *supra* note 252; Lynch v. State, 260 So. 3d 1166, 1168 (Fla. Dist. Ct. App. 2018).

566. The Wiretap Act audits are all publicly available on a government website. *See Wiretap Reports*, *supra* note 544.

567. *Id.*

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.[568] Even when not directed by police officers, omnipresent digital surveillance undermines human privacy and threatens personal liberty.[569]

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.[570] The ability to carve out a private life independent of government watchers is fundamental to modern American life.[571] 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.[572]

Because of these dangers, facial recognition must be regulated by legislative action.[573] 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.

568. *See supra* Part II.

569. *See id.*

570. 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.").

571. *See* Hartzog & Selinger, *supra* note 334.

572. *See supra* Part III.

573. Barry Friedman & Andrew Guthrie Ferguson, Opinion, *Here's a Way Forward on Facial Recognition*, N.Y. TIMES (Oct. 31, 2019), https://www.nytimes.com/2019/10/31/opinion/facial-recognition-regulation.html [https://perma.cc/GEL9-YLGH] (proposing a legislative solution).