Science and Technology Law Review

Volume 24 | Number 1 Article 2

2021

# Bertillonage in an Age of Surveillance: Fourth Amendment Regulation of Facial Recognition Technologies

David C. Gray
*University of Maryland School of Law*

# Bertillonage in an Age of Surveillance: Fourth Amendment Regulation of Facial Recognition Technologies

*David Gray**

## INTRODUCTION

In January 2020, when SARS-CoV-2 was just emerging as a global pandemic, Robert Julian-Borchak Williams received a call at his workplace from Detroit Police telling him to surrender himself for arrest.[1] A father of two young daughters, husband, and upstanding member of the venerable Detroit automotive community, Mr. Williams assumed it must be a prank of some kind, so he went about his day.[2] When he later returned to his suburban home, he found out it was no joke when armed officers surrounded him, handcuffed him, and arrested him in full view of his family and neighbors.[3] To add yet more insult, the arresting officers refused to tell Mr. Williams's wife where he was being taken, instead instructing her disdainfully to "Google it."[4]

After processing Mr. Williams, investigators took him to a room for interrogation.[5] There, they revealed that they had secured a warrant charging him with shoplifting $3,800 of watches from a store in 2018.[6] Their evidence? Two grainy still images taken from a security video of a man who was clearly not, the officers agreed, Mr. Williams.[7] Their response? "I guess the computer got it wrong."[8] Unfortunately, because he was arrested on a warrant, Mr. Williams was held for more than a day until he could post

---

* Jacob A. France, Professor of Law, University of Maryland, Francis King Carey School of Law. I would like to thank the editors of the Southern Methodist University Science and Technology Law Review and the Tsai Center for Law, Science, and Innovation for their invitation to give the keynote address at the Law Review's annual symposium. I could not have asked for more welcoming hosts. My thanks as well to Professor Meghan Ryan, the Altshuler Distinguished Teaching Professor at SMU Dedman School of Law, for moderating the session under challenging circumstances. SSG Michelle Leigh, USAF, provided in-depth research support for this project and was a patient tutor on the technology.

1. Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.
2. *Id.*
3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*
7. Hill, *supra* note 1.
8. *Id.*

bond.[9] Weeks later, at arraignment, prosecutors dismissed the charges altogether.[10] But what on earth did the officers mean when they blamed the whole affair on a computer error?

As it turned out, Mr. Williams was arrested largely on the basis of analysis performed by a facial recognition system operated by the Michigan State Police.[11] Analysts compared those two security camera images to a database of 49 million images, including driver's license photos.[12] Mr. Williams was targeted because the system identified him as a probable match using the picture from his license.[13] He was arrested when an employee of the store's security company identified Mr. Williams from a photo array despite her having no first-hand knowledge of the crime—she had just watched the security video.[14] Unfortunately, it does not appear that the human investigators made an independent assessment of the purported photo match, which investigators later agreed was obviously in error.[15] Neither did officers conduct any additional investigation or question Mr. Williams before applying for a warrant.[16]

Although Mr. Williams's case may be the first documented incident of false arrest based on facial recognition, Georgetown Law Professor and facial recognition expert Clare Garvie[17] commented that it is likely "not the first case to misidentify someone [or] to arrest them for a crime they didn't commit. This is just the first time we know about it."[18] That is because facial

9. *Id.*

10. *Id.*

11. *Id.*

12. *Id.*

13. Hill, *supra* note 1.

14. *Id.*

15. *Id.*

16. *Id.*

17. Professor Garvie is lead author with Alvaro Bedoya and Jonathan Frankle of the definitive study of law enforcement use of facial recognition technology. Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIVACY & TECH. (Oct. 18, 2016), www.perpetuallineup.org.

18. Hill, *supra* note 1. In May 2019, Professor Garvie documented one case that came close involving New York City Police investigators' using an image of actor Woody Harrelson to identify a shoplifting suspect. They first used a security camera photo, but when their facial recognition search failed to produce any matches, they noted a resemblance between the suspect and Mr. Harrelson, so used a picture of the actor retrieved from the web to run a second search. They were successful in identifying and arresting the wrong person. Though that incident is particularly problematic, Professor Garvie notes that law enforcement agencies frequently use composite sketches created in collaboration with witnesses as comparator images for facial recognition, which is a practice

recognition technology is increasingly in widespread use by law enforcement agencies[19]—at least half of us are in law enforcement face recognition networks[20]—despite documented evidence of false positives, particularly among members of minority groups.[21]

One of the most prominent providers of facial recognition technologies to law enforcement is Clearview AI.[22] Clearview scrapes the internet, social media, and even financial services sites—millions in total—to gather and aggregate images of faces.[23] It then offers users the opportunity to use the Clearview app to match comparator images provided by a user with images from that massive database.[24] Clearview has hundreds of law enforcement agencies among its clients and has exploded in popularity.[25] This is despite the fact that, unlike most technology companies in the facial recognition business, Clearview has not submitted its technology to the National Institute of Standards and Technology (NIST),[26] which has been conducting independent assessments of facial recognition technologies since 2000.[27] More disturbing

---

that is very likely to generate unreliable results. *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. L. CTR. ON PRIVACY & TECH. (May 19, 2019), www.flawedfacedata.com.

19. Jennifer Valentino-DeVries, *How 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.

20. Garvie et al., *supra* note 17.

21. *See* Travis LeBlanc, *INSIGHT: Facial Recognition is a Threat to People of Color*, BLOOMBERG L. (Aug. 18, 2020), https://news.bloomberglaw.com/tech-and-telecom-law/insight-facial-recognition-is-a-threat-to-people-of-color; PATRICK GROTHER, MEI NGAN, & KAYEE HANAOKA, NISTIR 8280, FACE RECOGNITION VENDOR TEST (FRVT), PART 3: DEMOGRAPHIC EFFECTS, NAT'L INST. OF STANDARDS & TECH. (2019), https://doi.org/10.6028/NIST.IR.8280 (documenting racial disparities in error rates produced by facial recognition technologies); Natasha Singer & Cade Metz, *Many Facial-Recognition Systems are Biased, Says U.S. Study*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html; 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.

22. Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

23. *Id.*

24. *Id.*

25. *Id.*

26. *Id.*

27. *Facial Recognition Technology (FRT): Testimony Before the House Committee on Homeland Security*, 116th Cong. (2020) (statement of Charles Romine, Di-

still, Clearview and its ilk are not subject to regulation, raising the specter of misuse, abuse, or just pervasive use that would dramatically alter our conceptions of privacy.[28] In the absence of restraint, law enforcement agencies are using facial recognition technologies with increasing frequency and often to solve relatively minor crimes like shoplifting.[29] Citing some of these concerns, many major technology companies have been very cautious in rolling out their facial recognition technologies.[30] Some have refused to make their tools available to law enforcement.[31] Others have abandoned the enterprise altogether.[32]

Law enforcement is not the only government agency seeking to leverage facial recognition technologies. Immigration and Customs Enforcement (ICE) uses facial recognition for investigative purposes.[33] ICE has also mined millions of driver's license photos in an effort to find undocumented aliens.[34]

---

rector, Information Technology Laboratory, Department of Commerce's National Institute of Standards and Technology), https://tinyurl.com/y2hte6aa.

28. Hill, *supra* note 22; Garvie et al., *supra* note 17 ("If deployed pervasively on surveillance video or police-worn body cameras, real-time face recognition will redefine the nature of public spaces."); Clearview is the target of a class action lawsuit in Illinois. *See ACLU Sues Clearview AI*, AM. C.L. UNION (May 28, 2020), https://www.aclu.org/press-releases/aclu-sues-clearview-ai; Davey Alba, *A.C.L.U. Accuses Clearview AI of Privacy 'Nightmare Scenario'*, N.Y. TIMES (May 28, 2020), https://www.nytimes.com/2020/05/28/technology/clearview-ai-privacy-lawsuit.html.

29. Alfred Ng, *Police are Using Facial Recognition for Minor Crimes Because They Can*, CNET (Oct. 24, 2020), https://www.cnet.com/news/police-are-using-facial-recognition-for-minor-crimes-because-they-can/#:~:text=police%20often%20frame%20facial%20recognition,used%20for%20low%2Dlevel%20offenses.

30. Karen Weise & Natasha Singer, *Amazon Pauses Police Use of Its Facial Recognition Software*, N.Y. TIMES (June 10, 2020), https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html.

31. *See, e.g.*, Clare Duffy, *Microsoft President Calls for Federal Regulation of Facial Recognition Technology*, CNN (June 18, 2020), https://www.cnn.com/2020/06/18/tech/brad-smith-microsoft-facial-recognition/index.html; Weise & Singer, *supra* note 30.

32. Ina Fried, *IBM Is Exiting the Face Recognition Business*, AXIOS (June 8, 2020), https://www.axios.com/ibm-is-exiting-the-face-recognition-business-62e79f09-34a2-4f1d-a541-caba112415c6.html.

33. PRIVACY IMPACT ASSESSMENT FOR THE ICE USE OF FACIAL RECOGNITION SERVICES, U.S. DEP'T HOMELAND SEC. (May 13, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf.

34. Drew Harwell & Erin Cox, *ICE Has Run Facial-Recognition Searches on Millions of Maryland Drivers*, WASH. POST (Feb. 26, 2020), www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers; Catie Edmondson, *ICE Used Facial Recognition to*

Customs and Border Protection uses facial recognition to confirm the identities of travelers exiting and reentering the country.[35] Airports are now making more expansive use of facial recognition to monitor domestic travel.[36] Although some uses are under review by the Privacy and Civil Liberties Oversight Board,[37] these deployments are not subject to legislative or judicial regulation.

Facial recognition technologies are even being deployed to combat the SARS-CoV-2 pandemic.[38] Clearview AI has proposed accessing feeds from security cameras to conduct contact tracing by tracking people who test positive, identifying persons who may have been exposed, and then tracing their movements to determine other potential exposures.[39] Hawaii is in the midst of deploying a surveillance system that uses thermal scanners and facial recognition to identify and track persons exhibiting symptoms of COVID-19.[40] The technology could also be used to enforce quarantine orders, alerting authorities when someone who should be at home is out in public. Some public school districts are considering similar systems, which would come with the bonus benefit of controlling access to school buildings and monitoring the comings and goings of students, faculty, and staff.[41] All of these various uses

*Mine State Driver's License Databases*, N.Y. TIMES (July 7, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html.

35. *Say Hello to the New Face of Speed, Security, and Safety: Introducing Biometric Facial Comparison*, U.S. CUST. & BORDER PROT., https://biometrics.cbp.gov/.

36. David Oliver, *Facial Recognition Scanners are Already at Some US Airports. Here's What to Know*, USA TODAY (Aug. 16, 2019), https://www.usatoday.com/story/travel/airline-news/2019/08/16/biometric-airport-screening-facial-recognition-everything-you-need-know/1998749001/.

37. *Projects*, U.S. PRIV. CIV. LIBERTIES OVERSIGHT BD., https://www.pclob.gov/Projects (last visited June 14, 2021).

38. *Controversial Tech Company Pitches Facial Recognition to Track COVID-19*, NBC NEWS (Apr. 27, 2020), https://www.nbcnews.com/now/video/controversial-tech-company-pitches-facial-recognition-to-track-covid-19-82638917537.

39. Jacob Ward & Chiara Sottile, *A Facial Recognition Company Wants to Help with Contact Tracing. A Senator has Questions.*, NBC NEWS (Apr. 30, 2020, 8:29 PM), https://www.nbcnews.com/tech/security/facial-recognition-company-wants-help-contact-tracing-senator-has-questions-n1197291.

40. Ryan Finnerty, *Thermal Screening Cameras in Place at Airports Statewide*, HAW. PUB. RADIO (Aug. 24, 2020), https://www.hawaiipublicradio.org/post/thermal-screening-cameras-place-airports-statewide.

41. Gregory Barber, *Schools Adopt Face Recognition in the Name of Fighting Covid*, WIRED (Nov. 3, 2020), https://www.wired.com/story/schools-adopt-face-recognition-name-fighting-covid/.

suggest an emerging reality of ubiquitous facial recognition,[42] what Professor Christopher Slobogin has dubbed "panvasive" surveillance.[43]

All of this is of course worrying from a privacy point of view. But there are also significant risks of abuse. As one example, China reportedly uses facial recognition technology to target its already beleaguered Uighurs.[44] Don't think facial recognition technology would be used to target political or religious groups here in the land of the free? There is already a long history of police and other government agencies using surveillance technologies to monitor political groups and identify participants in public protests.[45] In keeping with that tradition, the Department of Homeland Security (DHS) used unmanned aerial vehicles (drones) during the summer of 2020 to monitor protests and demonstrators in the wake of George Floyd's murder.[46] Although DHS denies that these drones were equipped with facial recognition technologies, there is nothing save technical limitations secondary to image quality and angle of surveillance to stop them from using facial recognition to identify participants.[47] Of course, ground-level images taken from body cameras, security cameras, and surveillance cameras suffer no such limits.[48]

Once contemplated only in science fiction, rapid advances in the technologies, plummeting costs, and endless demand have made it almost certain that we are now, or soon will be, subject to monitoring, surveillance, and

42. *Id.*

43. *See* Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721 (2014).

44. 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.

45. *See* Garvie et al., *supra* note 17 ("[H]ere is a real risk that police face recognition will be used to stifle free speech. There is also a history of FBI and police surveillance of civil rights protests."). One such case is *Handschu v. Special Services Division*, which involved the surveillance of political groups in New York. *See* Handschu v. Special Services Division *(Challenging NYPD Surveillance Practices Targeting Political Groups)*, N.Y. AM. C.L. UNION, https://www.nyclu.org/en/cases/handschu-v-special-services-division-challenging-nypd-surveillance-practices-targeting. *See also* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 116–17 (2013) (discussing *Handschu* as a model for consent decrees regulating surveillance technologies).

46. Zolan Kanno-Youngs, *U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance*, N.Y. TIMES (June 19, 2020), https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html.

47. *Id.* (reporting DHS's claims that images taken from the drones were taken from altitude and at a high angle, making the use of facial recognition technologies impossible).

48. *Id.*

tracking by facial recognition technologies on a routine basis. Although a few states and localities have taken steps to regulate the use of facial recognition technologies by law enforcement and other government agencies, most have not.[49] Congress has likewise failed to take any action to restrain these executive agencies.[50] Faced by that failure, we might hope that the courts, as a coequal branch, could impose some restraints on the deployment and use of facial recognition technologies. One place courts might look for a source of authority is the Fourth Amendment, which guarantees that the "right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated."[51] This article takes up that possibility.

This article argues that the Fourth Amendment limits the authority of government agents and their partners to deploy and use facial recognition technologies. Part I provides a very basic overview of facial recognition technology and situates it in a long tradition of biometric identification methods going back, at least, to the work of Alphonse Bertillon in the eighteenth century. As we shall see, facial recognition is a multi-step process.[52] Each step presents significant technical and practical challenges, which raise serious concerns about the ultimate reliability of the technology in many environments where government agents might hope to use it. Part II addresses the threshold question for any Fourth Amendment analysis: whether government actions constitute a "search" for purposes of the Fourth Amendment. Part II argues that the deployment and use of facial recognition technologies constitutes a "search" under both the text of the Fourth Amendment and prevailing Supreme Court doctrine. This does not mean that government agents cannot use facial recognition technologies. The Fourth Amendment instead commands that facial recognition "shall not" be used in ways that threaten the right of the people to be secure against unreasonable searches.[53] Part III describes how constitutional actors, inclusive of executive branch representatives, legislatures, and courts, might strike the right balance, allowing for the

49. *See* Singer & Metz, *supra* note 21 (reporting that "San Francisco, Oakland and Berkeley in California and the Massachusetts communities Somerville and Brookline [have] banned government use of [facial recognition] technology."). Some states have passed regulations on biometric data. *See, e.g.*, 740 ILL. COMP. STAT. ANN. 14 (West 2021); WASH. REV. CODE ANN. § 19.375.020 (West 2021); TEX. BUS. & COM. CODE ANN. § 503.001(a) (West 2021) (Biometric Identifiers). The American Civil Liberties Union recently sued Clearview AI under the Illinois Biometric Privacy Act. *ACLU Sues Clearview AI*, *supra* note 28.

50. *ACLU Sues Clearview AI*, *supra* note 28.

51. U.S. CONST. amend. IV.

52. Yaroslav Kuflinski, *How Facial Recognition Works*, IFLEXION (July 17, 2018), https://www.iflexion.com/blog/face-recognition-algorithms-work.

53. U.S. CONST. amend. IV.

reasonable use of facial recognition while guarding against its use to facilitate broad, indiscriminate, and intrusive searches.

## I. FACIAL RECOGNITION: THE NEW BERTILLONAGE

Modern facial recognition technologies owe much to Alphonse Bertillon, a nineteenth century civilian employee of the Parisian police.[54] In the 1880s, Bertillon developed a biometric method for identifying suspects and arrestees.[55] Eschewing vague and subjective physical descriptions, the Bertillon card system required officers to measure and record biomarkers such as the "circumferences of prisoners' heads, arms spans, left foot length, and length of left middle finger."[56] Bertillon "would later add sitting height, width of head between the cheek bones, the length of ears, left forearm, and left little finger, as well as standing height."[57] By taking and recording these measurements on cards that could be filed and later accessed, Bertillon hoped to help law enforcement and prosecutors to identify repeat offenders who might otherwise escape justice by changing their names or adopting aliases.[58] Referred to as "Bertillonage," the system operated on the presumption that concatenating a series of these biometric measurements could pick-out unique individuals.[59] Two people might have the same wrist and neck circumferences, but the odds that they would have the same measurements and ratios on all the Bertillon markers would be astronomical.[60]

Bertillonage arrived during an era when the social sciences were very interested in biometrics. Though already the target of significant skepticism in the academy, phrenology had a firm foothold in nineteenth century psychology and criminology.[61] Samuel Morton and Charles Caldwell were hard at work collecting and measuring skulls in an effort to provide scientific proof for the existence of race and empirical justifications for racist practices and social institutions.[62] Close on their heels, Paul Broca was establishing the

54. WILBUR R. MILLER, THE SOCIAL HISTORY OF CRIME AND PUNISHMENT IN AMERICA: AN ENCYCLOPEDIA 115–17, 453 (2012); Jim Fisher, *Alphonse Bertillon: The Father of Criminal Identification*, JIM FISHER: OFF. WEBSITE, https://jimfisher.edinboro.edu/forensics/bertillon1.html (last updated Jan. 7, 2008).

55. Fisher, *supra* note 54, at 1.

56. *Id.*

57. *Id.*

58. *Id.*

59. *Id.*

60. *Id.* (explaining Bertillon also worked to standardize mugshots, encouraging all precincts to take the same two photos—front-facing, and profile—under similar lighting conditions, further enhancing law enforcement's ability to identify repeat offenders).

61. STEPHEN JAY GOULD, THE MISMEASURE OF MAN 82–100 (1996).

62. *Id.*

field of craniometry, which purported to draw conclusions about intelligence and moral character by measuring the size, shape, angles, and ratios of heads and faces.[63] Although Bertillonage nominally aspired only to identify persons, the system rode this nineteenth century wave of ambitious empiricism to acclaim and acceptance.[64] Unfortunately, even these more modest ambitions for the careful measurement of bodies proved to be more than the method could bear.

Bertillonage proved to be less than effective, producing both false positives and false negatives.[65] Part of the problem was user error. Different departments used different biometric measurements.[66] For example, England's Bertillon system used head height, head width, length of middle finger, length of the left foot, and length of the forearm from elbow to middle finger, without apparent regard for whether these measurements were sufficiently unique to render reliable identifications, either individually or in the aggregate.[67] For example, that elbow-to-tip of the middle finger dimension is known as a "cubit," which has been used as a standard measure of length for thousands of years[68]—not the sort of biometric marker you would think capable of reliably identifying individual persons. Bertillon also seemed to have committed a bit of a sampling error, drawing conclusions about the power of his system based on measurements taken from relatively small groups.[69] Then there is the fact that most people are medium and have the same basic proportions in their bodies and facial structures[70]—facts familiar to any student of portraiture.

The Bertillon card system faded away in the early twentieth century, and ultimately was displaced by fingerprint analysis.[71] But that demise just

63. *Id.* at 114–39.

64. Fisher, *supra* note 54, at 1. There is some evidence that Bertillon himself was sympathetic to race science and eugenics. *See* Jacob Sherkow, Maryland (v. King) *Corrections Department: David Kaye on Bertillonage*, STAN. L. SCH. L. & BIOSCIENCES BLOG (June 11, 2013), https://law.stanford.edu/2013/06/11/lawandbiosciences-2013-06-11-maryland-v-king-corrections-department-david-kaye-on-bertillonage/.

65. *See* Fisher, *supra* note 54, at 2.

66. *See id.*

67. *Visible Proofs: Forensic Views of the Body: Galleries: Technologies: The Bertillon System*, U.S. NAT'L LIBR. MED., https://www.nlm.nih.gov/exhibition/visibleproofs/galleries/technologies/bertillon.html (last updated Dec. 3, 2014).

68. *Id.*

69. *See* Sherkow, *supra* note 64.

70. *Id.* (pointing out that Bertillonage suffers from endogeneity).

71. *See* LISA S. NELSON, AMERICA IDENTIFIED: BIOMETRIC TECHNOLOGY AND SOCIETY 31–34 (2011); Fisher, *supra* note 54, at 2. Of course, fingerprinting has its own challenges, some of which share a kinship with the Bertillon card system. For example, different law enforcement agencies apply different standards

confirmed the lasting influence of Bertillon's ideas about biometric identification. For example, the predominate approach to fingerprint analysis—the reigning gold standard of biometric identification—proceeds by analyzing specific biomarkers in a base sample, using that analysis to compare the base sample to another sample, evaluating that comparison to determine whether there is a match, and then verifying those results.[72] That basic process forms the analytic backbone of most forensic identification methods,[73] including facial recognition.

Modern facial recognition technology leverages digital imaging, data storage, and computer analysis to fulfill Bertillon's vision of a reliable biometric method for confirming identity.[74] These technologies generally serve one of two purposes: verification or identification.[75] As examples, facial recognition might be used to control access to secure facilities by verifying the identities of authorized personnel or to determine the identity of a person photographed at the scene of a crime. Regardless of the application, facial recognition entails five primary steps: (1) capturing an image; (2) facial localization or detection; (3) extracting features; (4) comparing features; and (5) making a determination or prediction.[76] Each of these steps comes with its own challenges. Different technologies adopt different strategies to ad-

when assessing whether two fingerprints have a sufficient number of similar "Galton points" to warrant determination of a "match" and the absence of clear evidence that matching any particular number of Galton points would guarantee accuracy. *See* United States v. Llera Plaza, 188 F. Supp. 2d 549, 555 (E.D. Pa. 2002); NAT'L ACAD. OF SCI., STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD 140–44 (2009). There is also a considerably amount of artistry to the "science" of fingerprinting, leading one critic to describe the process as little more than an exercise of "careful looking." United States v. Council, 777 F. Supp. 2d 1006, 1010 (E.D. Va. 2011) (quoting Dr. Jennifer Mnookin). *See also* Jennifer L. Mnookin, *The Validity of Latent Fingerprint Identification: Confessions of a Fingerprinting Moderate*, 7 L. PROB. & RISK 127, 132–34 (2008) (criticizing the certitude of fingerprinting as a science and fingerprint analysts as witnesses).

72. John R. Vanderkolk, *Examination Process*, *in* THE FINGERPRINT SOURCEBOOK 255 (2011), https://www.ojp.gov/pdffiles1/nij/225320.pdf (describing the ACE-V method).

73. *Id.*

74. P'SHIP ON AI, UNDERSTANDING FACIAL RECOGNITION SYSTEMS 2–8 (Feb. 19, 2020), https://www.partnershiponai.org/wp-content/uploads/2020/02/Understanding-Facial-Recognition-Paper_final.pdf (citing KRISTIE BALL ET AL., ROUTLEDGE HANDBOOK OF SURVEILLANCE STUDIES (2012)).

75. William Crumpler, *How Accurate are Facial Recognition Systems—and Why Does It Matter?*, CTR. FOR STRATEGIC INT'L STUD. (Apr. 14, 2020), https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter.

76. Garvie et al., *supra* note 17.

dress those challenges. Although an in-depth discussion of the technical details of these efforts is beyond the scope of this article, it is worth taking a few moments to provide a basic overview because it will inform our analysis in Part II and the prescriptive recommendations advanced in Part III.

Facial recognition starts with acquiring two images.[77] In most cases, one image is attached to a verified identity. A second, comparator image is taken for the purpose of, well, comparison. The major concern at the image capture phase is image quality.[78] Comparator images usually present the most significant challenges. That is because most facial recognition programs have a database of identified images that are taken under relatively controlled circumstances.[79] That will certainly be the case for verification systems because these programs gather and aggregate database images with the specific goal of facilitating facial recognition. But identification systems also do pretty well in terms of the quality of images in their databases because they choose sources, such as driver's license photos, passport pictures, and mugshots that are taken under controlled circumstances.[80] By contrast, comparator images are gathered from different sources, in diverse lighting conditions, from a variety of angles, and often in kinetic circumstances.[81] This means that comparator images are usually of much lower quality[82] and may result in errors.[83]

The second step of facial recognition entails detecting whether there is a face in a comparator image and isolating any faces that appear.[84] This is a simple task for carbon-based facial recognition systems, but can pose a sig-

77. *See id.* ("Face recognition is the automated process of comparing two images of faces to determine whether they represent the same individual.").

78. GROTHER ET AL., *supra* note 21, at 3.

79. *Id.* at 53–60.

80. Clearview AI is a notable exception to this rule because it rather indiscriminately scrapes publicly available images from the internet and social media to aggregate its image database. Clearview AI is also distinct in that images in its database are not necessarily identified. It instead operates by matching a comparator image to places where that same face has appeared. *See* Rebecca Heilweil, *The World's Scariest Facial Recognition Company, Explained*, VOX, https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement (last updated May 8, 2020) (explaining how Clearview AI works).

81. GROTHER ET AL., *supra* note 21, at 16–17.

82. Pei Li, Patrick J. Flynn, Loreto Prieto, & Domingo Mery, *Face Recognition in Low Quality Images: A Survey*, 1 ACM COMP. SURV. 1, 3–5 (Apr. 2019).

83. *Id.* at 6.

84. Ashu Kumar, Amandeep Kaur & Munish Kumar, *Face Detection Techniques: A Review*, 52 ARTIFICIAL INTEL. REV. 927, 928 (2018); *see also* Garvie et al., *supra* note 17 ("Before face recognition can identify someone, an algorithm must first find that person's face within the photo. This is called face detection.").

nificant challenge for silicon-based systems, particularly when comparator images are low-quality or visually complicated.[85] Most facial recognition systems use one or a combination of methods, trying to spot features that are unique to faces or performing a base comparison to database images, identifying things that look like faces by comparing things that might be faces to things that are known to be faces.[86] Image quality plays a role here as well, but so, too, do efforts to alter or obscure facial features—there is a cottage industry in facial recognition these days contending with ubiquitous mask-wearing as part of our collective effort to combat SARS-CoV-2.[87] Alternatively, programs may miss the fact that there is a face in the frame or misidentify dummies, masks, paintings, or photographs as faces. The emerging phenomenon of deep fakes and image morphing have added another layer of challenge here, raising the possibility of spoofing facial recognition technologies.[88]

The third step of facial recognition is feature extraction.[89] This is where a technology engages in its own version of Bertillonage, identifying and focusing on the features, landmarks, distances, and ratios that it will use to draw comparisons between faces.[90] This step ultimately creates a template that is used during the feature comparison phase.[91] For some systems, this process is not much different from Bertillon's approach—locate and measure the nose; measure angle from tip of nose to eyes; measure distance between

85. Kumar et al., *supra* note 84, at 928–30.

86. *Id.* at 931.

87. *See, e.g.*, Rebecca Heilweil, *Masks Can Fool Facial Recognition Systems, But the Algorithms are Learning Fast*, Vox (July 28, 2020), https://www.vox.com/recode/2020/7/28/21340674/face-masks-facial-recognition-surveillance-nist.

88. Pavel Korshunov & Sébastien Marcel, *Vulnerability of Face Recognition to Deep Morphing*, Cornell Univ. arXiv (Oct. 3, 2019), https://arxiv.org/pdf/1910.01933.pdf; Mei Ngan, Patrick Grother, Kayee Hanaoka & Jason Kuo, NISTIR 8292, DRAFT SUPPLEMENT: Face Recognition Vendor Test (FRVT) Part 4: MORPH—Performance of Automated Face Morph Detection, Nat'l Inst. of Standards & Tech., https://pages.nist.gov/frvt/reports/morph/frvt_morph_report.pdf (last updated Feb. 3, 2021). In 2019, researchers at the Idiap Research Institute in Switzerland found that high quality fakes, such as those created through the use of Generative Adversarial Networks, can fool facial recognition programs.

89. Yassin Kortli, Maher Jridi, Ayman Al Falou & Mohamed Atri, *Face Recognition Systems: A Survey*, 20 Sensors 342 (Jan. 2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7013584/.

90. Garvie et al., *supra* note 17 ("[T]he algorithm extracts features from the face—characteristics that can be numerically quantified, like eye position or skin texture.").

91. Kortli et al., *supra* note 89.

eyes; etc.[92] Most contemporary systems have moved past primitive biometrics and instead use artificial intelligence, machine learning, and neural networks to recognize faces[93] in ways as mysterious as we.[94] But these approaches require tremendous data storage capacity and computing power. Another emerging concern at the feature extraction stage is the impact that race, gender, and age have on the reliability of facial recognition technologies.[95] We will return to this in a moment.

It all comes together in the comparison stage. This is where facial recognition systems attempt to determine identities by comparing base images with a comparator image. If the purpose of the system is to verify an individual's identity, then the system will compare the extracted facial features to a stored facial template.[96] If the goal is to identify an individual, then the program will systematically compare extracted features from the comparator image with quantified descriptions of images on the database and run them through a database library of images or use artificial intelligence to arrive at an overall determination of identity.[97] Finally, facial recognition technologies assign a degree of certainty to comparisons.[98] Different systems operate with different probability thresholds before determining a positive match.

The primary concerns at these final stages of facial recognition are false negatives and false positives. For example, an access control system might erroneously deny an employee access to her workplace, or an immigration verification system might deny a citizen reentry into her country.[99] In most cases, these mistakes are likely to be sorted out fairly quickly and would have only temporary impact. Far more worrisome are false positives, which

92. *Id.*; *see also* Garvie et al., *supra* note 17 ("Many face recognition algorithms figure out which features matter most through training. During training, an algorithm is given pairs of face images of the same person. Over time, the algorithm learns to pay more attention to the features that were the most reliable signals that the two images contained the same person.").

93. Garvie et al., *supra* note 17 ("The mathematical machinery behind a face recognition algorithm can include millions of variables that are optimized in the process of training. This intricacy is what gives an algorithm the capacity to learn, but it also makes it very difficult for a human to examine an algorithm or generalize about its behavior.").

94. Not all of us of course. *See* Oliver Sacks, *Face-Blind*, NEW YORKER (Aug. 23, 2010), https://www.newyorker.com/magazine/2010/08/30/face-blind.

95. *See infra* notes 101–112 and accompanying text.

96. Garvie et al., *supra* note 17.

97. *Id.*

98. *Id.* ("Finally, the algorithm examines pairs of faces and issues a numerical score reflecting the similarity of their features. Face recognition is inherently probabilistic: It does not produce binary 'yes' or 'no' answers, but rather identifies more likely or less likely matches.").

99. *See* Hill, *supra* note 1.

may result in unauthorized persons gaining access to secure areas or to cross international borders. Worse still is the possibility of taking away someone's liberty due to a misidentification. The case of Robert Julian-Borchak Williams presents a stark example.[100] Human intervenors can provide some additional reassurance by independently verifying a purported match, but, as Mr. Williams's case shows, we tend to rely on technology rather than our own judgment in many circumstances. That kind of abdication is, of course, particularly tempting when a comparator image is low quality, in which case a human user might assume that the technology has superior capacities to discern the undiscernible. Here again, one cannot help but think that this kind of blind faith in oracular technology played a role in Mr. Williams's case. How else to explain investigating officers who trust a facial recognition match over their own, well-practiced, human capacities to tell people apart?

But there is another important dimension to the Williams case: race. Racial disparities are a pervasive feature of our criminal justice system from street engagements between citizens and law enforcement[101] all the way through to the death penalty.[102] Given that reality, it should come as no surprise that facial recognition technologies exhibit a racial bias.[103] This was confirmed by a 2019 NIST study.[104] For that study, investigators tested the ability of almost two hundred algorithms to perform basic verification and identification tasks.[105] The study showed consistently higher error rates when applied to non-white faces, generating as many as 100 times more false positives on both verification and identification when applied to African American, Native American, and Asian faces.[106] The systems were also less reliable when applied to women as compared to men, and older people as compared

100. *See supra* notes 1–18 and accompanying text.

101. *See, e.g.*, *Racial Disparities Remain, Despite Significant Decline in Stops*, AM. C.L. UNION (Mar. 14, 2019), https://www.aclu.org/press-releases/nyclu-releases-report-analyzing-nypd-stop-and-frisk-data; U.S. DEP'T OF JUST., INVESTIGATION OF THE BALTIMORE CITY POLICE DEPARTMENT 47–61 (2016).

102. *See, e.g.*, Phyllis Goldfarb, *Matters of Strata: Race, Gender, and Class Structures in Capital Cases*, 73 WASH. & LEE L. REV. 1395, 1395–96 (2016).

103. *See* LeBlanc, *supra* note 21. In fact, those background disparities may play a causal role in promoting racial disparities in facial recognition because "due to disproportionately high arrest rates, systems that rely on mug shot databases likely include a disproportionate number of African Americans." Garvie et al., *supra* note 17.

104. *See* GROTHER ET AL., *supra* note 21, at 3.

105. *Id.* at 25–27.

106. *See* Singer & Metz, *supra* note 21; LeBlanc, *supra* note 21.

to folks in middle-age.[107] These results confirmed prior studies, including one performed by researchers at the Massachusetts Institute of Technology.[108]

Given the history of Bertillonage and its association with eugenics and race science, we ought to be very cautious in deploying any modern digital equivalents that exhibit racial biases, putting people of color at higher risk of false arrest or worse. To their credit, developers seem to have embraced the social justice imperative at stake. Many top companies have hit pause on deploying their systems for law enforcement purposes so they can address racial disparities.[109] One promising approach seems to be adding diversity to the databases used to train the technology.[110] As proof of concept, it appears from the NIST study that technologies developed in China did not exhibit racial bias when applied to Asian faces.[111] Also promising is the fact that rates of racial bias in facial technologies have and continue to decline as the algorithms become more sophisticated.[112]

With this basic overview of facial recognition technologies and some of the practical challenges they face, let us turn to the question whether the Fourth Amendment has anything to say about whether and how these tools can be used. We start where all Fourth Amendment analysis must start, with the question whether using facial recognition constitutes a "search."

## II. SHOULD THE FOURTH AMENDMENT REGULATE FACIAL RECOGNITION?

The threshold question in any Fourth Amendment analysis is whether the actions of a government agent constitute a "search" or a "seizure." The U.S. Supreme Court has elaborated two primary tests for determining whether government activity constitutes a "search."[113] The first, which traces to the Court's 1928 decision in *Olmstead v. United States*, is whether a government agent intruded into a constitutionally protected area—a "person, house, paper, or effect"—for purposes of gathering information[114] in the ab-

107. *See* Singer & Metz, *supra* note 21.

108. *See id.*

109. *See supra* notes 31–32.

110. Will Knight, *AI is Biased. Here's How Scientists are Trying to Fix It*, *Wired* (Dec. 19, 2019), https://www.wired.com/story/ai-biased-how-scientists-trying-fix/.

111. *See* GROTHER ET AL., *supra* note 21, at 7.

112. Knight, *supra* note 110.

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

114. Olmstead v. United States, 277 U.S. 438, 465–66 (1928) (holding that there is no Fourth Amendment "search" "unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure."). *See also* Florida v. Jardines, 569 U.S. 1, 5 (2013)

sence of consent, whether expressed or implied.[115] Alternatively, government activities that intrude upon subjectively manifested expectations of privacy that society is prepared to recognize as reasonable may also constitute a search,[116] even if there is no physical intrusion involved.[117] Applying these two tests, the Court has held that there is no search or seizure involved when government agents make observations from a lawful vantagepoint.[118] Under this "public observation doctrine," the Court has held that officers' tracking a suspect's movements in public spaces does not constitute a "search" for purposes of the Fourth Amendment.[119] Courts have also held that the use of security cameras and closed-circuit surveillance systems deployed in public spaces does not implicate the Fourth Amendment, even if they are trained on constitutionally protected areas.[120]

("When 'the Government obtains information by physically intruding' on persons, houses, papers, or effects, 'a "search" within the original meaning of the Fourth Amendment' has 'undoubtedly occurred.' "); United States v. Jones, 565 U.S. 400, 404 (2012) ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

115. *Jardines*, 569 U.S. at 8 (" '[O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave.' As it is undisputed that the detectives had all four of their feet and all four of their companion's firmly planted on the constitutionally protected extension of Jardines' home, the only question is whether he had given his leave (even implicitly) for them to do so. . . . 'A license may be implied from the habits of the country . . . .' ") (quoting Entick v. Carrington, 95 Eng. Rep. 807, 817 (K.B. 1765)).

116. *Katz*, 389 U.S. at 353, 361 (Harlan, J., concurring) ("[T]he 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.' ").

117. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 40 (2001) (use of thermal detection device to gather information about activities in a home is a "search" for purposes of the Fourth Amendment even though use of the device does not entail a physical intrusion into the home).

118. United States v. Knotts, 460 U.S. 276, 281–82 (1983) (tracking a suspect on public roads using a radio beeper is not a "search"); *e.g.*, Florida v. Riley, 488 U.S. 445, 453, 455 (1989) (observing constitutionally protected areas of the home from public airspace is not a "search").

119. *Knotts*, 460 U.S. at 281–82.

120. United States v. Moore-Bush, 381 F. Supp. 3d 139, 145 (D. Mass 2019); State v. Anderson, No. 2018AP718-CR, 2019 WL 3294796, at *3 (Wis. Ct. App. July 23, 2019); United States v. Tuggle, No. 16-cr-20070-JES-JEH, 2018 WL 3631881, at *3 (D.C. Ill. July 31, 2018); *see also* Florida v. Riley, 488 U.S. 445, 449–50 (1989) (holding that looking into constitutionally-protected areas

Based on these precedents, there is good reason to believe that there would be no Fourth Amendment impediment to the deployment and use of facial recognition technology. So long as the technology is deployed in public spaces, its deployment would not entail any physical intrusion into constitutionally protected areas.[121] Neither does it seem to intrude upon reasonable expectations of privacy because the technology would do no more than observe what any member of the public might observe. The capacity to identify particular individuals does not appear to change matters. We are anonymous to many people we see in our daily travels through public places, but familiar to others. We are of course recognized most often in workplaces and frequent haunts,[122] but anonymity is never a guarantee in other spaces. We have all had the experience of being recognized by a friend, loved one, colleague, or long-forgotten classmate while out and about.[123] Given the possibility that a real person might recognize us as we walk down the street or drive through an intersection, facial recognition technology does not seem to pose any additional threats to reasonable expectations of privacy—at least as the Court has conventionally understood reasonable expectations of privacy.[124] But might there be grounds for abandoning or adapting the conventional view when it comes to facial recognition technologies?

The Court recently gave us some reason to doubt this conventional analysis as it would apply to facial recognition technologies.[125] In *Carpenter v. United States*, the Court held that law enforcement officers must obtain a

from public spaces does not constitute a search); California v. Ciraolo, 476 U.S. 207, 215 (1986).

121. *Cf.* United States v. Jones, 565 U.S. 400, 404 (2012) (holding that the installation of a tracking device on a private vehicle constituted a "search" for purposes of the Fourth Amendment because that installation entailed a physical intrusion into a constitutionally-protected area for purposes of gathering information).

122. *See* GARY PORTNOY, *Where Everybody Knows Your Name* (Cheers Theme) (1982) ("Sometimes you wanna go where everybody knows your name and they're always glad you came. You wanna be where you can see our troubles are all the same. You wanna be where everybody knows your name.").

123. *See* United States v. Maynard, 615 F.3d 544, 560 (D.C. Cir. 2010) ("It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work."); David Gray & Danielle K. Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J. L. & TECH. 381, 412 (2013) ("We are all familiar with such happenstances, and at one point or another have found ourselves driving the same roads with a fellow traveler for miles and hours, or perhaps even briefly following someone who looks vaguely familiar to determine whether they are, in fact, that person on whom we had a crush in the eighth grade.").

124. *Riley*, 488 U.S. at 449–50; *Anderson*, 2019 WL 3294796, at *3.

125. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

warrant before accessing cell site location data gathered and stored by cellphone service providers.[126] In that case, agents from the Federal Bureau of Investigation were investigating Timothy Carpenter on suspicion that he was involved in a series of armed robberies in Michigan and Ohio.[127] As part of their investigation, agents secured a court order issued under the Secured Communications Act[128] compelling Carpenter's cellular service providers to disclose several months' cell site location data (CSLI) associated with his accounts.[129] By analyzing this information, agents were able to establish that Carpenter—or, at least, Carpenter's phone—was close to several of the robberies.[130] Although the Court was not entirely clear in *Carpenter* about when the search occurred on these facts,[131] it was firm in the conclusion that there was a Fourth Amendment search and that a warrant requirement is the proper tool for guaranteeing the security of the people against unreasonable searches using cell site location data.[132]

The *Carpenter* Court recognized that its holding was in tension with its precedents decided under the public observation doctrine.[133] After all, the location data agents sought in *Carpenter* would only document his movements in public spaces in and around the locations of the armed robberies.[134] Since he did not have a reasonable expectation of privacy as to his presence in those public places, and there was no physical intrusion into a constitutionally protected area involved in the gathering of that information, it is hard to see why the Fourth Amendment would have anything to say. The answer,

126. *Id.* at 2221.

127. *Id.* at 2212.

128. 18 U.S.C. § 2703(d) (2019).

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

130. *Id.* at 2212–13.

131. *Compare id.* at 2217 ("The location information obtained from Carpenter's wireless carriers was the product of a search."), *with id.* at 2220 ("The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment.").

132. *Id.* at 2221.

133. *Id.* at 2215.

134. *Cf.* Kyllo v. United States, 533 U.S. 27, 34 (2001) (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)) ("[O]btaining by sense enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search."); United States v. Karo, 468 U.S. 705, 714 (1984) ("[T]he monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence.").

according to the Court, lies in the nature of CSLI as a technology and the fundamental role of the Fourth Amendment in our constitutional scheme.[135]

Before *Carpenter*, the signal Supreme Court case dealing with tracking technologies was *United States v. Knotts*.[136] There, the Court relied on the public observation doctrine to hold that the use of a radio beeper tracking device to monitor a suspect's movements on public streets did not constitute a "search" because a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[137] As the Court points out in *Carpenter*, the *Knotts* Court was "careful to distinguish between the rudimentary tracking facilitated by the [radio] beeper and more sweeping modes of surveillance . . . reserv[ing] the question whether 'different constitutional principles may be applicable' if 'twenty-four hour surveillance of any citizen of this country [were] possible.' "[138] In *Carpenter*, the Court makes explicit what was implied by that reservation in *Knotts*, holding that people have a reasonable expectation of privacy in the whole of their physical movements.[139] The radio beeper tracking technology used in *Knotts* did not threaten that expectation because it required active engagement by officers, which meant that "law enforcement might have pursued a suspect for a brief stretch, but doing so 'for any extended period of time was difficult and costly and therefore rarely undertaken.' "[140] CSLI is different.

135. *Carpenter*, 138 S. Ct. at 2223; *see* Gray & Citron, *supra* note 45, at 101–02 (arguing that the Court should shift its focus in Fourth Amendment on the potential for new technologies to facilitate programs of broad and indiscriminate surveillance); *see also id.* at 132–33 (arguing that the public observation doctrine should not extend to GPS-tracking and similar tracking technologies because they are capable of facilitating programs of broad and indiscriminate surveillance).

136. 460 U.S. 276, 285 (1983).

137. *Id.* at 281–82.

138. *Carpenter*, 138 S. Ct. at 2215 (quoting *Knotts*, 460 U.S. at 283–84).

139. *Id.* at 2219; *see also* David Gray, *The Fourth Amendment Categorical Imperative*, 116 MICH. L. REV. ONLINE 14, 34–35 (2017) ("Looking through CSLI records, using CSLI to look for an effect, and using CSLI to make inquiry or look for a person are all searches by any ordinary definition."); Gray & Citron, *supra* note 45, at 71–72 ("[T]he threshold Fourth Amendment question should be whether a technology has the capacity to facilitate broad and indiscriminate surveillance that intrudes upon reasonable expectations of quantitative privacy by raising the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of law enforcement officers or other government agents.").

140. *Carpenter*, 138 S. Ct. at 2217 (quoting United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring)); *see also* Gray & Citron, *supra* note 45, at 132 ("The beeper technology used in *Knotts* was simply incapable of broad and indiscriminate surveillance. It could only provide directional information, not a

Unlike the beeper technology used in *Knotts*, the *Carpenter* Court held that cell site tracking threatens reasonable expectations of privacy in the whole of our movements.[141] That is because it "provides an all-encompassing record of the holder's whereabouts."[142] It also "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.' "[143] Belying its power as a means of conducting surveillance, the Court noted that cell site location is "remarkably easy, cheap, and efficient,"[144] so CSLI is not only "detailed, [and] encyclopedic, [but also] effortlessly compiled."[145] This is particularly concerning, the Court noted, in light of the fact that cellular phones are ubiquitous (there are "396 million cell phone service

suspect's precise location. To be of any use at all, the beepers used in *Knotts* needed to be in close proximity to a dedicated radio receiver. Because no stable network of these receivers existed, officers had to follow the beepers, and hence the suspects, to track them. This beeper technology was thus little more than an adjunct to traditional human surveillance and therefore labored under the same practical limitations. That is why the *Knotts* Court ultimately held that the beeper technology used in that case 'raise[d] no constitutional issues which visual surveillance would not also raise.' ").

141. *Carpenter*, 138 S. Ct. at 2217–18; *see also* Gray, *supra* note 139, at 35 ("As the Fourth Amendment categorical imperative reveals, new and emerging tracking and surveillance technologies like CSLI are entirely different in terms of the threats they pose to the security of the people against unreasonable searches and seizures. That is because these technologies are powerful, scalable, and cheap."); Gray & Citron, *supra* note 45, at 132 ("GPS-enabled tracking technology used in *Jones* and other technologies that threaten quantitative privacy are materially different . . . GPS-enabled technology provides second-by-second location data . . . GPS is precise, highly scalable, and increasingly inexpensive . . . unlike the beeper technology . . . used in *Knotts* [that] came with inherent constraints that limited its ability to facilitate broad programs of indiscriminate surveillance. The GPS technology used in Jones suffers no such limitations.").

142. *Carpenter*, 138 S. Ct. at 2217; Gray & Citron, *supra* note 45, at 102 (("[F]actors that a court would need to consider are: (1) the inherent scope of a technology's surveillance capabilities, be they narrow or broad; (2) the technology's scale and scalability . . . .").

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

144. *Id.* at 2217–18; *see also* Gray, *supra* note 139, at 35 ("[N]ew and emerging tracking and surveillance technologies like CSLI are entirely different in terms of the threats they pose to the security of the people against unreasonable searches and seizures. That is because these technologies are powerful, scalable, and cheap."); Gray & Citron, *supra* note 45, at 102 (citing costs associated with deploying and using the technology); *id.* at 133 ("GPS is precise, highly scalable, and increasingly inexpensive.").

145. *Carpenter*, 138 S. Ct. at 2216; *see also* Gray & Citron, *supra* note 45, at 102 (pointing out that the scope of a surveillance technologies capabilities and

accounts in the United States—for a Nation of 326 million people")[146] and people "compulsively carry cell phones with them all the time" as if they were "'a feature of [their] anatomy.'"[147] "Accordingly, when 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."[148] And, "[c]ritically, 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."[149]

But why does all of this matter from a Fourth Amendment point of view? To answer that question, the *Carpenter* Court returned to history and first principles.[150] As the Court noted, "[t]he Founding generation crafted the Fourth Amendment as a 'response' to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity."[151] "In fact, as John Adams recalled, the patriot James Otis's 1761

"costs associated with deployment and use" are relevant when assessing its Fourth Amendment status).

146. *Carpenter*, 138 S. Ct. at 2211.

147. *Id.* at 2218.

148. *Id.*; *see also* Gray, *supra* note 139, at 36 ("[T]hese features of CSLI mean that it has the immediate capacity to facilitate broad and indiscriminate surveillance."); Gray & Citron, *supra* note 45, at 102 ("If a court finds that a challenged technology is capable of broad and indiscriminate surveillance by its nature, or is sufficiently inexpensive and scalable so as to present no practical barrier against its broad and indiscriminate use, then granting law enforcement unfettered access to that technology would violate reasonable expectations of quantitative privacy.").

149. *Carpenter*, 138 S. Ct. at 2218; *see also id.* ("[P]olice need not even know in advance whether they want to follow a particular individual, or when. Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance."); Gray, *supra* note 139, at 35 ("CSLI is an extremely powerful search tool that allows searches for persons and their effects anytime, even in the past."); Gray & Citron, *supra* note 45, at 144 (concluding that the Fourth Amendment should regulate access to technologies that enable the "monitoring of everyone all the time").

150. *Carpenter*, 138 S. Ct. at 2213–14.

151. *Id.* at 2213; *see also* Gray & Citron, *supra* note 45, at 70 ("Before America's founding, British agents routinely abused general warrants, including writs of assistance, to subject our forefathers to the eighteenth-century equivalent of a surveillance state. The Fourth Amendment responded to these abuses by limiting the right of law enforcement to effect physical searches and seizures and

speech condemning writs of assistance was 'the first act of opposition to the arbitrary claims of Great Britain' and helped spark the Revolution itself."[152] Based on this history, the Court concluded that "the [Fourth] Amendment seeks to secure 'the privacies of life' against 'arbitrary power'" and "'to place obstacles in the way of a too permeating police surveillance.'"[153] "In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection," the *Carpenter* Court concluded, "grant[ing] the state unrestricted access to a wireless carrier's database of physical location information" "risks Government encroachment of the sort the Framers, 'after consulting the lessons of history,' drafted the Fourth Amendment to prevent."[154]

Although the Court was careful in *Carpenter* to limit its holding to CSLI, it provides a framework for evaluating the Fourth Amendment status of other new and emerging surveillance technologies.[155] Specifically, *Car-*

---

the authority of politically driven legislatures and executives to license programs of broad and indiscriminate search.").

152. *Carpenter*, 138 S. Ct. at 2213; *see also* Gray & Citron, *supra* note 45, at 93–94 ("The Fourth Amendment drew on these historical experiences to describe limitations on 'the amount of power that [our society] permits its police to use without effective control by law.' During the colonial period, British officials and their representatives took advantage of writs of assistance and other general warrants, which immunized them from legal liability for their invasions, in order to search anyone they pleased, anywhere they pleased, without having to specify cause or reason. James Otis, who famously vacated his office as General when solicited to defend writs of assistance, described general warrants in a 1761 court argument as 'the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book.' Among those in the audience for Otis's speech was a young attorney named John Adams, who would later be a principal contributor to the text of the Fourth Amendment.").

153. *Carpenter*, 138 S. Ct. at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886); United States v. Di Re, 332 U.S. 581, 595 (1948)); *see also* Gray & Citron, *supra* note 45, at 95 ("Although the negative rights afforded by the Fourth Amendment have specific historical antecedents, the text itself evinces a broader historical purpose to protect against indiscriminate and invasive governmental practices that are characteristic of a surveillance state.").

154. *Carpenter*, 138 S. Ct. at 2223; *see also* Gray & Citron, *supra* note 45, at 103 ("The Fourth Amendment guards against the government's unfettered use of techniques and technologies that raise the specter of a surveillance state. For our forebears, those fears arose in reaction to the broad and indiscriminate use of physically invasive searches and seizures. Today, the risk of a surveillance state arises with law enforcement's unfettered access to advanced surveillance technologies, including aerial drones, GPS-enabled tracking devices, and data aggregation and mining projects like DAS, fusion centers, and NSA's telephonic and data surveillance programs.").

155. *Carpenter*, 138 S. Ct. at 2217–18, 2223.

*penter* instructs us to focus on the technology at issue, to ask about the extent to which the information it gathers might reveal intimate details about our lives,[156] including our associations and activities,[157] the "retrospective quality of the data,"[158] whether the data can be "store[d] and efficiently mine[d] for information years into the future,"[159] whether the technology can be scaled-up easily, facilitating "dragnet-type law enforcement practices" such as "twenty-four hour surveillance of any citizen of this country,"[160] whether the technology "by design, proceeds surreptitiously,"[161] and whether the deployment and use of the technology "evades the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility."[162] The Court's analysis of those factors leads to its holding that unregulated access to CSLI[163] threatens our reasonable expectations of privacy in the "whole of our physical movements."[164]

156. *Id.* at 2217; *see also* Gray & Citron, *supra* note 45, at 101–25 (elaborating this "technology-centered" approach).

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

158. *Id.*

159. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); *see also Carpenter*, 138 S. Ct. at 2218 ("[T]he 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 . . . .").

160. United States v. Knotts, 460 U.S. 276, 283–84 (1983); *see also Carpenter*, 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring)) ("'[S]ociety's expectation . . . 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' . . . Allowing government access to cell-site records contravenes that expectation."); *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (contending that technologies that are "cheap in comparison to conventional surveillance techniques" may raise Fourth Amendment concerns); Gray & Citron, *supra* note 45, at 75, 90 (explaining the Fourth Amendment significance of technology costs and scalability).

161. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring); *see also Carpenter*, 138 S. Ct. at 2217 (quoting with approval Justice Sotomayor's assertion in *Jones* about society's expectation on law enforcement secret monitoring).

162. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (citation omitted); *see also Carpenter*, 138 S. Ct. at 2217 (quoting with approval Justice Sotomayor's assertion in *Jones* about society's expectation on law enforcement secret monitoring).

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

164. *Id.* at 2219.

So, what does *Carpenter* teach us about the Fourth Amendment status of facial recognition technologies? The answer depends somewhat on the way the technology would be deployed and used. Discrete uses, such as verifying identity at immigration checkpoints or running an image captured at a crime scene through a database to identify a specific criminal suspect caught on a surveillance camera, might not implicate the Fourth Amendment under either a conventional analysis or the approach modeled in *Carpenter*.

On a conventional analysis, these discrete uses of facial recognition technology entail gathering information disclosed to the public, the use of information that is voluntarily shared with third parties,[165] or both. For example, facial recognition used at immigration entry points involves cameras making observations in public places and comparing those observations to images voluntarily shared with the Department of State when securing a passport or visa.[166] Facial recognition technology used to identify a criminal suspect whose image was caught on a security camera would involve recorded observations of conduct in a public place—or, at the very least, a place where the criminal suspect does not have a reasonable expectation of privacy—and would compare those images against a database of images voluntarily shared with public agencies, such as a department of motor vehicles.[167] In either case, the use of facial recognition technology would not entail physical intrusions into constitutionally protected areas or violations of reasonable expectations of privacy.[168]

The result appears to be the same under the analytic framework adopted in *Carpenter*. Both of these examples involve discrete uses of facial recognition technology.[169] They, therefore, do not threaten to disclose the whole of someone's physical movements.[170] Neither would they facilitate the kinds of

165. *See* Florida v. Riley, 488 U.S. 445, 449–50 (1989) (observing constitutionally protected areas of the home from public airspace is not a "search"); California v. Ciraolo, 476 U.S. 207, 215 (1986); *Knotts*, 460 U.S. at 281–82 (tracking a suspect on public roads using a radio beeper is not a "search").

166. *Say Hello to the New Face of Speed, Security, and Safety: Introducing Biometric Facial Comparison*, *supra* note 35.

167. PRIVACY IMPACT ASSESSMENT FOR THE ICE USE OF FACIAL RECOGNITION SERVICES, *supra* note 33.

168. *Compare Riley*, 488 U.S. at 449–50 (observing constitutionally protected areas of the home from public airspace is not a "search"), *with* Kyllo v. United States, 533 U.S. 27, 34 (2001) (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)) ("[O]btaining by sense enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search.").

169. *See Carpenter*, 138 S. Ct. at 2215 (quoting *Knotts*, 460 U.S. at 284–85 (emphasizing that the limited use of a beeper by the government during an "automotive journey" was discrete).

170. *Cf. id.* at 2219.

broad and indiscriminate surveillance that implicates Fourth Amendment protections against grants of "arbitrary power" and "too permeating police surveillance."[171] Of course, there is no reason to think that facial recognition technology would be deployed and used so parsimoniously.

Contemporary conversations about surveillance technologies often are informed by science fiction. For example, George Orwell's *1984* is a familiar trope in debates about surveillance.[172] These references are useful not only for making visceral and immediate some threats to privacy and liberty that may otherwise seem abstract and remote, but also because they can provide us with a window into potential futures—challenging us to decide what world we want for ourselves. When it comes to facial recognition technology, one possible future is depicted in the 2002 film *Minority Report*.[173] Based on a short story by Philip K. Dick, the movie follows protagonist John Anderton, who is an officer in a unit charged with arresting individuals based on predictions of future crimes rendered by a group of prognosticators called "Precogs."[174] Anderton goes on the lam after he becomes a target of his own unit when the Precogs predict that he will commit a murder.[175] In one vivid scene, his efforts to escape are thwarted by a dense network of cameras capable of identifying passersby using retinal scans.[176] Some of these cameras are deployed for public safety and crime control purposes, but many are attached to advertisement signs and linked to consumer databases.[177] This allows advertisers to target their offers to Anderton or anyone else who happens to be walking by—kind of like Google ads in the real world.[178] In one scene, a holographic greeter asks Anderton how a recent tank-top purchase is working out.[179]

*Minority Report* presents us with a dystopian vision of a world in which a dense net of biometric identification technology makes it impossible for anyone to move anonymously through public spaces.[180] Because the cameras are networked, the technology also provides a detailed accounting of individ-

171. *Id.* at 2214.

172. *See, e.g.*, Margaret Hu, *Orwell's 1984 and a Fourth Amendment Cybersurveillance Nonintrusion Test*, 92 WASH. L. REV. 1819, 1865 (2017).

173. Clarisse Loughrey, *Minority Report: 6 Predictions That Came True, 15 Years On*, INDEPENDENT (June 25, 2017), https://www.independent.co.uk/arts-entertainment/films/features/minority-report-15th-anniversary-predictive-policing-gesture-based-computing-facial-and-optical-recognition-a7807666.html.

174. *Id.*

175. *Id.*

176. *Id.*

177. *Id.*

178. *Id.*

179. Loughrey, *supra* note 173.

180. *Id.*

uals' movements through public spaces.[181] Facial recognition technology has the same potential to facilitate close monitoring of everyone's movements through public spaces.[182] Linked networks of surveillance cameras increasingly is the norm.[183] Most police agencies have their own surveillance networks[184] but also have access to cameras and networks operated by private institutions[185] and even private persons.[186] Although a combination of technical challenges, including variations in image quality, bandwidth, computer power, and image databases, make it a challenge to run all of these feeds through facial recognition filters, that day is not far off.[187] In fact, Clearview AI has proposed using this kind of program to conduct contact tracing and enforce quarantine orders.[188] At any rate, the Court has made clear that we must fashion Fourth Amendment rules that are not limited by present technologies, but "take account of more sophisticated systems that are already in use or in development."[189] With that guidance in mind, we should ask serious questions about whether facial recognition technology would violate our reasonable expectations of privacy if it were deployed widely, accessed images from a wide range of sources deployed across a broad diversity of public spaces, and constantly identified individuals on an automatic basis.[190] In short, we must ask whether the Fourth Amendment can protect us against what was once science fiction, but is now, or soon will be, everyday fact.

There can be little doubt that broadly deployed facial recognition technology would violate our reasonable expectations of privacy in the whole of

181. *Id.*

182. *Id.*

183. *See* Gray & Citron, *supra* note 45, at 65–66 (describing New York's Domain Awareness System).

184. *Id.*

185. *Id.*

186. *See* Drew Harwell, *Doorbell-Camera Firm Ring has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019, 4:53 PM), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/ (describing how police access footage from home surveillance systems).

187. *See* Garvie et al., *supra* note 17 ("Contract documents and agency statements show that at least five major police departments—including agencies in Chicago, Dallas, and Los Angeles—either claimed to run real-time face recognition off of street cameras, bought technology that can do so, or expressed a written interest in buying it. Nearly all major face recognition companies offer real-time software.").

188. *See supra* note 39 and accompanying text.

189. Carpenter v. United States, 138 S. Ct. 2206, 2218–19 (2018) (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)).

190. *Id.* at 2218–19.

our public movements. As the technology improves, it will be relatively cheap and easy to scale-up the deployment and use of facial recognition. By design and in practice, it does and will operate surreptitiously, evading the normal checks on the abusive use of police powers, including limited resources and public scrutiny. Much like CSLI, these networks would document intimate details about our lives, including where we go, with whom we associate, and a wide range of our activities.[191] In fact, this threat would be more acute in the case of facial recognition technology than it is with CSLI. That is because we can choose not to own or not to carry a cellular phone.[192] Not so our faces. In addition, and again in parallel with CSLI, information gathered by widespread facial recognition technologies would be easy to store and mine in the future, allowing those with access not only to follow us in real time, but to trace our movements back in time.[193] As a consequence, granting government agents unfettered discretion to deploy and use facial recognition technology would be akin to granting general warrants and writs of assistance, raising the specter of a surveillance state by licensing "too permeating police surveillance," marking an "encroachment of the sort the Framers, after consulting the lessons of history, drafted the Fourth Amendment to prevent."[194]

Facial recognition technology appears to check all the boxes the Court ticked off in *Carpenter* on its way to holding that affording law enforcement unfettered access to cell site location information violates reasonable expectations of privacy.[195] But there is a simpler path: we could just take seriously the text and history of the Fourth Amendment. Specifically, we could determine whether the deployment and use of facial recognition technology would constitute a "search" under the original public meaning of the text and then ask whether granting government agents unfettered discretion to deploy and use this technology would threaten the right to be secure against unreasonable searches guaranteed to the people by the Fourth Amendment.[196]

The use of facial recognition technology either as part of a broader system of networked surveillance technologies or to facilitate discrete investigative goals would constitute a "search" by any reasonable definition, whether eighteenth century or modern. "Search" had much the same meaning in 1792 as it does today, including efforts "[t]o examine; to explore; to look through"

191. *Id.*

192. *Id.* at 2218 ("Only the few without cell phones could escape this tireless and absolute surveillance.").

193. *Id.*

194. *Id.* at 2223 (internal quotation marks and citation omitted).

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

196. DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE 251 (2017).

and "[t]o make inquiry" or "[t]o seek; to try to find."[197] On this definition, efforts to look for or try to find a person, whether in their home, their office, or even on public streets, would constitute a "search."[198] Founding-era sources, including justice of the peace manuals, reflect this commonsense conclusion.[199] So, too, contemporary semantic instincts—there is nothing odd or unfamiliar at all about phrases like "I'm searching for my spouse in the Target" or "I'm searching for Waldo in this picture." On this straightforward definition, looking for persons using a surveillance network equipped with facial recognition technology or using facial recognition technology to identify someone by examining photographs and looking through image databases would both qualify as "searches" under the plain language of the Fourth Amendment—no need to perform doctrinal backflips to avoid doctrinal pitfalls.[200]

197. *Search*, *in* SAMUEL JOHNSON, A DICTIONARY OF THE ENGLISH LANGUAGE (10th ed. 1792). Justice Scalia has identified Johnson as an "authoritative" source for the meaning of words in the Constitution. *See* ANTONIN SCALIA & BRYAN A. GARNER, READING LAW: THE INTERPRETATION OF LEGAL TEXTS 419 (2012); *see also* District of Columbia v. Heller, 554 U.S. 570, 581 (2008) (citing and relying on JOHNSON, *supra*. *See also* GRAY, *supra* note 196, at 251; Gray, *supra* note 139, at 34–35.

198. GRAY, *supra* note 196, at 158–60.

199. *See, e.g.*, THE CONDUCTOR GENERALIS: OR, THE OFFICE, DUTY AND AUTHORITY OF JUSTICES OF THE PEACE, HIGH-SHERIFFS, UNDER-SHERIFFS, CORONERS, CONSTABLES, GAOLERS, JURY-MEN, AND OVERSEERS OF THE POOR 187–88 (1792) (providing that "upon hue and cry levied against any person, or where any hue and cry comes to a constable, whether the person be certain or uncertain, the constable may search suspected places within his vill[age] for the apprehending of the felons"); WILLIAM SHEPPARD, THE OFFICES OF CONSTABLES, CHURCH WARDENS, OVERSEERS OF THE POOR, SUPRAVISORS OF THE HIGH-WAYES, TREASURERS OF THE COUNTY-STOCK; AND SOME LESSER COUNTREY OFFICERS PLAINLY AND LIVELY SET FORTH ch. 8, § 2 ("An Action of Trespass was brought by a man for an Assault and Battery of his Servant, whereby he did lose his service three dayes, and the Defendant pleaded that A was robbed at midnight of Goods to the value of two pounds, whereupon the said A came to the Constable, and prayed him to search for the suspicious persons, and to apprehend and arrest them; and accordingly he did search, and found the same servant walking suspiciously in the street in the night . . . ."); *id.* ("And this Officer receiving a Hue and Cry after a Fellon, must, with all speed, make diligent pursuit, with Horse and Foot, after the offendors from Town to Town the way it is sent, and make diligent search in his own Town . . . ."). *See also* WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 322 (2009) (discussing early eighteenth-century cases of searches for "Rogues, Vagabonds, sturdy Beggars, and disorderly Persons apprehended by virtue of search Warrants in Night Houses and other disorderly Houses or such as infest the Streets in the Night-time").

200. The whole notion that a search is not a search traces to *Katz*, after all. GRAY, *supra* note 196, at 159–60.

This more straightforward approach would still leave open the question whether granting law enforcement officers unfettered discretion to deploy and use facial recognition technologies threatens the security of the people against unreasonable searches.[201] On this question, the Court's rehabilitation of founding-era concerns about grants of arbitrary power tracing to eighteenth century experiences with general warrants and writs of assistance is helpful and instructive.[202] To see why, let us again consider the text, which guarantees that "the right of the people to be secure against unreasonable searches and seizures shall not be violated." Eighteenth century readers would have understood "unreasonable" similarly to how we understand it today:[203] as "[n]ot agreeable to reason,"[204] "[e]xorbitant; claiming or insisting on more than is fit," or "[g]reater than is fit; immoderate."[205] As the Court recognized in *Carpenter*, the phrase "unreasonable searches and seizures" would have been read as a reference to general warrants and writs of assistance, which granted government agents broad, unfettered authority to search anywhere they liked for good reasons, for bad reasons, or for no reasons at all without fear of legal consequence.[206] By contrast, a search conducted pursuant to a lawful warrant issued by a judicial officer based on probable cause that described with particularity the place to be searched and the items to be seized was generally considered "reasonable" precisely because that process guaranteed that searches would be conducted for good and sufficient reasons

201. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (recognizing that the fundamental question is whether "to grant the state unrestricted access to a wireless carrier's database of physical location in formation."); United States v. Jones, 565 U.S. 400, 416–17 (2012) (noting that courts must "consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power [and to] prevent 'a too permeating police surveillance.' ") (Sotomayor, J., concurring) (internal citation and quotation marks omitted). *See also* GRAY, *supra* note 196, at 157–58 (pointing out that "to be secure" in the Fourth Amendment refers to general warrants, writs of assistance, and their grants of unfettered discretion to search).

202. *See Carpenter*, 138 S. Ct. at 2214.

203. For example, Merriam-Webster defines "unreasonable" as "not governed by or acting according to reason," "not conformable to reason," or "exceeding the bounds of reason or moderation." *Unreasonable*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/unreasonable [https://perma.cc/4XXV-54EE].

204. JOHNSON, *supra* note 197. Johnson defined "reason" as "[t]he power by which man deduces one proposition from another, or proceeds from premises to consequences," "[r]ight; justice," or "[m]oderation." *Id.*

205. *Id.*

206. GRAY, *supra* note 196, at 160–65; Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 776–81 (1994).

and pursuant to a limited license that constrained the discretion of those conducting a search.[207]

This leads us to the question of security. In 1792, as now, "to be secure" would have been understood as a condition "free from fear" or "danger."[208] Thus, the Fourth Amendment guarantees that "the people," collectively,[209] have the absolute right to live free from fear that they will be subjected to

207. *See* GRAY, *supra* note 196, at 160–65; Laura K. Donohue, *Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1270–71 (2016); Amar, *supra* note 206, at 776–81. This reading is reinforced later in the text where we are told that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. After all, what is the requirement to show "probable cause" but a demand for good and sufficient reasons? Why require an "Oath or affirmation" if not to submit those reasons to formal, independent evaluation? And why require particularity if not to limit the discretion of government agents when conducting searches and seizures?

208. JOHNSON, *supra* note 197; *see also* GRAY, *supra* note 196, at 157–58; Luke M. Milligan, *The Forgotten Right to be Secure*, 65 HASTINGS L.J. 713, 740, 749–50 (2014). Merriam-Webster defines "secure" as "free from danger." *Secure*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/secure [https://perma.cc/57ML-9X74].

209. According to the text, the Fourth Amendment protects "the people," not "persons." U.S. CONST. amend. IV. That choice indicates a founding-era recognition that Fourth Amendment rights have an important collective dimension. *See* GRAY, *supra* note 196, at 144–56; David Gray, *Fourth Amendment Rights as Remedies: The Warrant Requirement*, 96 B.U. L. REV. 425, 444–56 (2016); David Gray, *Dangerous Dicta*, 72 WASH. & LEE L. REV. 1181, 1184–203 (2015); Richard H. McAdams, *Tying Privacy in Knotts: Beeper Monitoring and Collective Fourth Amendment Rights*, 71 VA. L. REV. 297, 318 (1985). That conclusion is evidenced by the fact that this choice of words marked a departure from parallel protections against unreasonable search and seizure in contemporary state constitutions. For example, both the Massachusetts and New Hampshire constitutions guaranteed the right of "every subject" to be secure against unreasonable searches and seizures. N.H. CONST. pt. 1, art. XIX (amended 1792); MASS. CONST. pt. 1, art. XIV. Eighteenth century readers could not have missed the significance of this choice, particularly in light of the important role of John Adams and the Massachusetts Declaration of Rights on the Fourth Amendment. *See* GRAY, *supra* note 196, at 147–56 (discussing significance of "the people" as compared to "every subject"); CUDDIHY, *supra* note 199, at 729 (identifying the Pennsylvania Constitution as the origin of the phrase "the right of the people" in the Fourth Amendment). Readers at the time would have read this as a reference to the same "people" acting in the Preamble to form a more perfect union and whose rights are protected by the First, Second, Ninth, and Tenth Amendments—namely "the People of the United States." United States v. Verdugo-Urquidez, 494 U.S. 259, 265–66 (1990) (contrasting "the people" with "the words 'person' and 'accused' used in the Fifth and Sixth Amendments regulating procedures in criminal cases.").

arbitrary search and seizure at the despotic whim of an executive agent.[210] This, of course, is precisely the threat posed by general warrants and writs of assistance.[211]

General warrants and writs of assistance were not particular as to the person to be arrested or the property to be seized.[212] They instead provided general authority for executive agents or their designees to search anywhere they liked. Worse still, executive agents could issue general warrants on their own authority, circumventing judicial review.[213] In fact, the warrants under scrutiny in *Entick v. Carrington*, one of the famed general warrants cases, which has been described by the Supreme Court "as a monument of English freedom, undoubtedly familiar to every American statesman at the time the Constitution was adopted, and considered to be the true and ultimate expression of constitutional law with regard to search and seizure,"[214] were issued under the authority of Secretary of State, George Montagu-Dunk, the Second Earl of Halifax. As a result, general warrants provided government agents with virtually unlimited authority to search wherever they pleased without need of justifying their conduct by good and sufficient reasons.[215] In fact,

210. U.S. CONST. amend. IV.

211. *See* Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018); Riley v. California, 134 S. Ct. 2473, 2494 (2014) (discussing how the Fourth Amendment "was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.").

212. *Carpenter*, 138 S. Ct. at 2213; *Riley*, 134 S. Ct. at 2494.

213. *See* Amar, *supra* note 206, at 772–73.

214. United States v. Jones, 565 U.S. 400, 405 (2012) (quoting Brower v. Cnty. of Inyo, 489 U.S. 593, 596 (1989); Boyd v. United States, 116 U.S. 616, 626 (1886)).

215. *See* Huckle v. Money, 95 Eng. Rep. 768 (C.P. 1763) (general warrants license searches "without any information or charge"); *see also* James Otis, *In Opposition to Writs of Assistance*, *in* THE WORLD'S FAMOUS ORATIONS 27–37 (William Jennings Bryan ed., 1906) (discussing how general warrants justify searches and seizures on nothing more than "[b]are suspicion without oath" allowing "[e]very one with this writ may be a tyrant . . . accountable to no person for his doings. Every man may reign secure in his petty tyranny . . . ."); *Ex parte* Burford, 7 U.S. (3 Cranch) 448, 453 (1806) (a warrant issued for "want of stating some good cause certain, supported by oath" is unconstitutional) (emphasis omitted). Under eighteenth century common law, those targeted for searches or seizures could compel those who conducted the search or seizure to justify himself by providing good and sufficient reasons for his actions in a court. Entick v. Carrington (1765) 95 Eng. Rep. 807, 817 (K.B.). Warrants, including general warrants, provided immunity against suits in trespass, effectively excusing bearers the duty of justifying their conduct after the fact. Amar, *supra* note 206, at 774–78. General warrants and writs of assistance also did not provide for procedural review such as requiring agents to keep an

general warrants licensed searches conducted for bad reasons[216] or no reasons at all while also providing broad immunity from civil actions.[217]

So, a search conducted under the authority of a general warrant provides the paradigm case of an unreasonable search.[218] By contrast, a search conducted under the authority of a specific warrant issued by a detached and neutral magistrate based "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"[219] provides the paradigm example of a reasonable search.[220] That is because general warrants are, well, general! By definition, they do not specify the places to be searched or the items to be seized.[221] They therefore leave the decision to search to the unfettered discretion of executive agents unmediated by any process of reason-giving or judicial review.[222] That is the very definition of "arbitrary power." As with any grant of

inventory of papers or property they seized. Wilkes v. Wood (1763) 8 Eng. Rep. 489, 498–99 (C.P.).

216. *See* Otis, *supra* note 215, at 32 (noting that "[e]very man prompted by revenge, ill humor, or wantonness, to inspect the inside of his neighbor's house, may get a writ of assistance"). Another founding-era commentator similarly warned that "if magistrates had a power of arresting men . . . merely upon their own suspicions, or pretended suspicions, they might cause any person, how innocent soever, to be thrown into prison whenever they thought fit." FRANCIS MASERES, THE CANADIAN FREEHOLDER: IN THREE DIALOGUES BETWEEN AN ENGLISHMAN AND A FRENCHMAN, SETTLED IN CANADA 246 (1779).

217. Amar, *supra* note 206, at 774–78.

218. *See, e.g.*, Money v. Leach (1765) 97 Eng. Rep. 1075, 1088 (K.B.) ("[A]n uncertain warrant [is] void: and there is no case or book to the contrary."); *Huckle*, 95 Eng. Rep. at 769 (concluding the same); *Wilkes*, 98 Eng. Rep. at 498–99 (concluding the same).

219. U.S. CONST. amend. IV.

220. GRAY, *supra* note 196, at 170.

221. *See Huckle*, 95 Eng. Rep. at 768; *Wilkes*, 98 Eng. Rep. at 498–99.

222. *Wilkes*, 98 Eng. Rep. at 498–99 (general warrants provide "a discretionary power given to messengers to search wherever their suspicions may chance to fall"); Entick v. Carrington (1765) 95 Eng. Rep. 807, 817 (K.B.) (general warrants leave "to the discretion of these defendants" the decision to search); *Money*, 97 Eng. Rep. at 1088 ("It is not fit, that the receiving or judging of the information should be left to the discretion of the officer."); *see also* Opinion of Attorney General De Grey upon Writs of Assistance, 7 Geo. 3, c. 46 (Eng.) ("[I]t will be unconstitutional to lodge such Writ in the Hands of the Officer, as it will give him a discretionary Power to act under it in such Manner as he shall think necessary."); 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 291–92 (Joseph Chitty ed., 1826) ("[I]t is the duty of the magistrate, and ought not to be left to the officer, to judge of the ground of suspicion."). Justice Jackson would later reprise these themes in *Johnson v. United States*, 333 U.S. 10 (1948), where he famously pointed out that

unchecked power, general warrants open the door to abuse,[223] leaving "the people" to live in a state of insecurity against the threat of unreasonable searches.[224] The general warrants cases provide a good example of how such broad grants of unfettered power are "inimical to a democratic society."[225] After all, the executive agents in those cases used their power to search and seize as tools to target and suppress political dissent.[226] On this side of the Atlantic, James Otis levied similar criticisms of general warrants in *Paxton's Case*.[227] In a speech later lauded as "the first scene of the first act of opposition to the arbitrary claims of Great Britain,"[228] Otis warned against granting

> The point of the Fourth Amendment which often is not grasped by zealous officers is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate, instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. [Footnote 3] Any assumption that evidence sufficient to support a magistrate's disinterested determination to issue a search warrant will justify the officers in making a search without a warrant would reduce the Amendment to a nullity, and leave the people's homes secure only in the discretion of police officers.
>
> *Id.*

223. Otis, *supra* note 215, at 30–32 ("Every one with this writ may be a tyrant," and "may reign secure in [their] petty tyranny, and spread terror and desolation around [them], until the trump of the archangel shall excite different emotions in [their] soul[s] . . . and whether they break through malice or revenge, no man, no court can inquire."); *see also id.* ("Every man prompted by revenge, ill humor, or wantonness, to inspect the inside of his neighbor's house, may get a writ of assistance. Others will ask it from self-defense; one arbitrary exertion will provoke another, until society be involved in tumult and in blood.").

224. *See* Donohue, *supra* note 207, at 1270, 1319 (discussing how general warrants granted arbitrary powers that were "unreasonable" to the Framers, being "against the reason of the common law," and had oppressive impact on the people as a whole); Milligan, *supra* note 208, at 738–50 (discussing how the Fourth Amendment conferred on the people a right to be "free from fear" of unreasonable searches). In *Wilkes v. Wood*, the court condemned this kind of general power to search as "totally subversive of the liberty of the subject." *Wilkes*, 98 Eng. Rep. at 498. James Otis famously denounced writs of assistance as "the worst instrument of arbitrary power," placing "the liberty of every man in the hands of every petty officer." Otis, *supra* note 215, at 28–29.

225. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

226. *See* CUDDIHY, *supra* note 199, at 122–23; Donohue, *supra* note 207, at 1208–10; Milligan, *supra* note 208, at 749.

227. GRAY, *supra* note 196, at 70; CUDDIHY, *supra* note 199, at 377–95.

228. Riley v. California, 134 S. Ct. 2473, 2494 (2014) (quoting Letter from John Adams to William Tudor (Mar. 29, 1817), *in* 10 JOHN ADAMS, THE WORKS OF JOHN ADAMS 244, 248 (Charles Francis Adams ed., 1856)).

executive agents broad discretionary powers to search and seize[229] in the absence of judicial review.[230]

The mere existence of general warrants and writs of assistance threatened the security of our eighteenth century forebears, forcing everyone[231] to live in fear that they might at any moment be the victim of arbitrary executive power.[232] As the court in one of the general warrants cases put the point, granting "discretionary power . . . to messengers to search wherever their suspicions may chance to fall . . . certainly may affect the person and property of every man in this kingdom."[233] In another of these cases, the court warned that general warrants "would destroy all the comforts of society."[234] In a third, the court criticized executive agents for "exercising arbitrary power, violating *Magna Charta*, and attempting to destroy the liberty of

229. *See* Otis, *supra* note 215, at 30 (condemning general warrants for granting a license to "imprison, or murder anyone within the realm" whom government agents might choose as a target); *see also* Mark Graber, *Seeing, Seizing, and Searching Like a State: Constitutional Developments from the Seventeenth Century to the End of the Nineteenth Century*, *in* CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 395, 406 (David Gray & Stephen Henderson eds., 2017) ("Americans believed that government by administrators was arbitrary government inconsistent with the constitutional principles of rule by law. General warrants and excise searches were intimate parts of this conspiracy against republican government that Americans eventually concluded justified separation from Great Britain.").

230. Otis, *supra* note 215, at 29 (general warrants put "the liberty of every man in the hands of every petty officer," by allowing officers to "enter our houses when they please," exercising unchecked "arbitrary power"); *see also* THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776) (condemning King George III for "erect[ing] a multitude of New Offices, and sen[ding] hither swarms of Officers to harass our people and eat out their substance.").

231. *See, e.g.*, 1 THE DEBATES OF THE SEVERAL STATE CONVENTIONS ON THE ADOPTION OF THE FEDERAL CONSTITUTION 387 (2d ed. Jonathan Elliot ed., 1937) (1836) (quoting Luther Martin as warning against general warrants' allowing government officials to "examine into your private concerns").

232. *See* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 366 (1974) ("[T]he primary abuse thought to characterize the general warrants and the writs of assistance was their indiscriminate quality, the license that they gave to search Everyman without particularized cause, the fact that they were—as *Wilkes* proclaimed Lord Halifax's warrant for the authors and publishers of No. 45 of the North Briton—'a ridiculous warrant against the whole English nation.'" (quoting 2 THOMAS ERSKINE MAY, THE CONSTITUTIONAL HISTORY OF ENGLAND SINCE THE ACCESSION OF GEORGE THIRD 247 (1864)).

233. Wilkes v. Wood (1763) 8 Eng. Rep. 489, 498 (C.P.).

234. Entick v. Carrington (1765) 95 Eng. Rep. 807, 817 (K.B.).

the kingdom, by insisting upon the legality of this general warrant . . . ."[235] In a similar vein, James Otis condemned general warrants as "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book."[236] He was not alone in this view among our founders. Elbridge Gerry railed against general warrants as "a detestable instrument of arbitrary power" that licensed "capricious house searches by insolent officers of the new central government."[237] The Sons of Liberty, headed by Samuel Adams, complained that general warrants allowed "our bed chambers . . . to be searched by brutal tools of power . . . ."[238] Patrick Henry condemned general warrants as licenses to search "in the most arbitrary manner, without any evidence or reason" leaving "the most sacred" to be "ransacked by the strong hand of power."[239] Those concerns lasted through the nineteenth[240] and twentieth[241] centuries, providing a clear and consistent historical reference for the *Carpenter* Court's criticism of technologies capable of facilitating programs of broad and indiscriminate surveillance.

There can be no doubt that facial recognition technologies pose real dangers to these core Fourth Amendment values. Clearview's recent proposals to use facial recognition to facilitate contact tracing and quarantine en-

235. Huckle v. Money (1763) 95 Eng. Rep. 768, 769 (C.P.).

236. Otis, *supra* note 215, at 28.

237. Elbridge Gerry, *Observations on the New Constitution, and on the Federal and State Conventions* (Boston, n. pub. 1788), *reprinted in* PAMPHLETS ON THE CONSTITUTION OF THE UNITED STATES 1, 13 (Paul Leicester Ford ed.,1888); CUDDIHY, *supra* note 199, at 677.

238. *A Son of Liberty*, N.Y. J. (Nov. 8, 1787), *reprinted in* 13 THE DOCUMENTARY HISTORY OF THE RATIFICATION OF THE CONSTITUTION 481, 481 (John P. Kaminski & Gaspare J. Saladino eds., 1981).

239. 3 THE DEBATES OF THE SEVERAL STATE CONVENTIONS ON THE ADOPTION OF THE FEDERAL CONSTITUTION, *supra* note 231, at 588.

240. *See, e.g.*, Boyd v. United States, 116 U.S. 616, 630 (1886) ("The struggles against arbitrary power in which [the Founders] had been engaged for more than twenty years, would have been too deeply engraved in their memories to have allowed them to approve of such insidious disguises of the old grievance which they had so deeply abhorred."); Grummon v. Raymond, 1 Conn. 40, 43 (Conn. 1814) (allowing general warrants would leave "every citizen of the United States within the jurisdiction . . . liable to be arrested and carried before the justice for trial.").

241. *See, e.g.*, United States v. Di Re, 332 U.S. 581, 595 (1948) ("But the forefathers, after consulting the lessons of history, designed our Constitution to place obstacles in the way of a too permeating police surveillance, which they seemed to think was a greater danger to a free people than the escape of some criminals from punishment.").

forcement during the SARS-CoV-2 pandemic provides a prime example.[242] What could be more threatening to the liberty or more threatening of arbitrary government power than a technology capable of identifying us wherever we are, or were, and tracking us wherever we go, or have been?

Notably, the result of this analysis is the same even if law enforcement only wants to use facial recognition for a discrete investigation. Although that particular use may not, of itself, threaten the security of the people, neither would a single search conducted under the authority of a general warrant. The point made by founding-era courts and commentators was that the very existence of general warrants threatened the security of the people. If agents could conduct searches or seizures at their arbitrary whim, then that left everyone to live in a state of fear that they would be subjected to an unreasonable search or seizure. Any instance of search or seizure sanctioned by a general warrant, though particular, stood for that general threat.[243] So too would granting government agents unfettered access to facial recognition technology. As we shall see in Part III, discrete uses may well be reasonable, but only if they are subject to Fourth Amendment regulation rather than the whims of executive agents.

## III. REGULATING FACIAL RECOGNITION TECHNOLOGIES

So, what does this mean for facial recognition technologies? The Fourth Amendment prohibits grants of broad and unfettered discretion to search and seize akin to those made by general warrants and writs of assistance because they threaten the right of each of us and all of us, "the people," to be secure against unreasonable searches and seizures.[244] To allow government agents unfettered access to facial recognition technologies would constitute precisely this kind of threat, leaving at risk the "liberty of every man"[245] and the security of "society"[246] against "too permeating police surveillance"[247] because it would facilitate the kind of broad and indiscriminate surveillance that was the *bête noir* of the Fourth Amendment in 1792 and the *Carpenter* Court in 2018. True, broad, networked visual surveillance systems enabled with facial recognition technology are not a present reality. But, as the *Carpenter* Court noted, courts must "take account of more sophisticated systems that are already in use or in development" when applying the Fourth Amend-

242. *See supra* note 39 and accompanying text.

243. Gray, *supra* note 139, at 35 (explaining this concept using Immanuel Kant's categorical imperative).

244. Milligan, *supra* note 208, at 738–50; Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 552 (1999).

245. Otis, *supra* note 215, at 29.

246. Entick v. Carrington, (1765) 95 Eng. Rep. 807, 817 (K.B.).

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

ment[248]—and we have already seen applications of facial recognition technology that make clear that what was once science fiction is a looming reality.[249] Moreover, if the goal of imposing Fourth Amendment restraints on new and emerging technologies is to protect the security of the people against unreasonable searches and seizures, then it makes sense to set limits early in the evolutionary cycle of a technology to make sure those guarantees are never compromised and to guard against the dangers of technological determinism, which marks a degradation of privacy as a result of the deployment and use of surveillance technologies, making it hard to scale-back technologies once they are in widespread use.[250] In short, it behooves us to act now rather than waiting until it is practically too late. That is true no matter how limited the proposed use of facial recognition technology. The point is that the decision whether, how, and in what circumstances facial recognition technology can be used cannot be left to the unfettered discretion of executive agents any more than the choice whether, how, and in what circumstances to physically search a home.[251]

But what action should we take? The Supreme Court's primary tool for regulating search activities, including the deployment and use of surveillance technologies, has been to require that officers obtain a warrant issued by a detached and neutral magistrate based on probable cause.[252] The constitutional pedigree of this "warrant requirement" is suspect.[253] Some scholars have argued that the warrant requirement is baked into the common law

248. *Id.* at 2218 (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)).

249. *See supra* notes 1–51 and accompanying text.

250. *Cf. Kyllo*, 533 U.S. at 34 (holding that "obtaining by sense enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use.") (citation omitted).

251. Gray, *supra* note 139, at 31–34; *see also* Johnson v. United States, 333 U.S. 10, 13–14 (1948) ("The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often-competitive enterprise of ferreting out crime.").

252. *See, e.g.*, *Carpenter*, 138 S. Ct. 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."); *Kyllo*, 533 U.S. at 40 ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.").

253. California v. Acevedo, 500 U.S. 565, 581–84 (Scalia, J., concurring).

fabric of the Fourth Amendment.[254] Others contend that the Fourth Amendment is genetically skeptical of warrants because they provide immunity against civil actions.[255] As a practical matter, the warrant requirement is so riddled with exceptions that it operates more as a safe harbor, providing a presumption of reasonableness when officers secure a warrant in advance of a search while creating a presumption of unreasonableness when they do not.

Taking into account the best textual, historical, and doctrinal evidence, the most sensible way to understand the warrant requirement is as a judicial remedy created by the Court under authority granted to it by the reasonableness clause.[256] It is certainly a sensible prescription both in the abstract and in light of the text. After all, the goal of the Fourth Amendment is to guarantee our collective security against arbitrary exercises of executive power.[257] The warrant clause targets one potential source of insecurity—general warrants—but also describes a process for limiting the discretionary powers of executive agents by requiring them to provide good and sufficient reasons to a neutral judicial officer for limited grants of power to conduct searches of

254. *See, e.g.*, Donohue, *supra* note 207, at 1276–80.

255. Amar, *supra* note 206, 770–81 (arguing that the Fourth Amendment sought to regulate warranted searches because warrants provided immunity against the traditional common law protections afforded by juries in trespass actions); *see also* AKHIL REED AMAR, THE LAW OF THE LAND: A GRAND TOUR OF OUR CONSTITUTIONAL REPUBLIC 212 (2015) (arguing that reading "an implicit warrant requirement for all searches and seizures runs counter to text, Founding-era history, and common sense. Textually, as we have seen, the amendment contains no third clause explicitly stating that 'warrantless searches and seizures are inherently unreasonable,' or explicitly barring all 'warrantless searches and seizures.'"); Akhil Reed Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, 30 SUFFOLK U.L. REV. 53, 55 (1996) ("[T]he [Fourth] Amendment does not require a warrant for each and every search or seizure. It simply requires that each and every search or seizure be reasonable.").

256. GRAY, *supra* note 196, at 202–17; Gray, *Fourth Amendment Rights as Remedies: The Warrant Requirement*, *supra* note 209, at 464–81; *see also Acevedo*, 500 U.S. 565, 581–84 (Scalia, J., concurring) ("Although the Fourth Amendment does not explicitly impose the requirement of a warrant, it is of course textually possible to consider that implicit within the requirement of reasonableness."); *cf. Carpenter*, 138 S. Ct. at 2221 ("Although the ultimate measure of the constitutionality of a governmental search is 'reasonableness,' our cases establish that warrantless searches are typically unreasonable where 'a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing.' Thus, '[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.'") (internal citations omitted).

257. Gray, *Fourth Amendment Rights as Remedies: The Warrant Requirement*, *supra* note 209, at 476–79.

particular places for specific things.[258] Although perhaps cumbersome for police officers, the Supreme Court has held that requiring them to run this procedural gauntlet strikes a reasonable balance between the competing interests of citizens and law enforcement that are at stake in many cases where officers want to search persons, houses, papers, or effects.[259]

But does a warrant requirement always strike the right balance? Is it always what reasonableness demands? According to the Court, the answer is a resounding "no." In a wide variety of circumstances, the Court has held that requiring that government agents obtain a warrant before engaging in a search or seizure would unreasonably compromise the governmental interests at stake. So, government agents do not need warrants to make arrests in public,[260] to conduct stops or frisks,[261] to carry out searches incident to arrest,[262] to search cars,[263] to search in the face of exigent circumstances,[264] or to conduct searches in service of regulatory regimes.[265] In all of these circumstances, the Court has sanctioned alternative means for limiting the discretionary powers of government agents.[266] In the criminal law context, these alternatives usually require officers to justify their actions to a judicial officer after the fact.[267] In the regulatory context, legislatures and executive agencies have considerable latitude to design mechanisms that serve as constitutionally adequate substitutes for the warrant requirement.[268] As the foregoing discussion has shown, "constitutional adequacy" should be understood

258. Johnson v. United States, 333 U.S. 10, 13–14 (1948); *see also* GRAY, *supra* note 196, at 212.

259. *Johnson*, 333 U.S. at 14 ("Crime, even in the privacy of one's own quarters, is, of course, of grave concern to society, and the law allows such crime to be reached on proper showing. The right of officers to thrust themselves into a home is also a grave concern, not only to the individual but to a society which chooses to dwell in reasonable security and freedom from surveillance. When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or government enforcement agent. . . . No reason is offered for not obtaining a search warrant except the inconvenience to the officers and some slight delay necessary to prepare papers and present the evidence to a magistrate. These are never very convincing reasons . . .").

260. Gerstein v. Pugh, 420 U.S. 103, 113–14 (1975).

261. Terry v. Ohio, 392 U.S. 1, 21–22 (1968).

262. Chimel v. California, 395 U.S. 752, 762–63 (1969).

263. California v. Carney, 471 U.S. 386, 391–93 (1985).

264. Mincey v. Arizona, 437 U.S. 385, 394 (1978).

265. New York v. Burger, 482 U.S. 691, 700–02 (1987).

266. *Id.* at 703.

267. *See, e.g.*, Gerstein v. Pugh, 420 U.S. 103, 114 (1975).

268. *Burger*, 482 U.S. at 702–03.

as procedural restraints on the discretion of executive agents sufficient to guarantee the right of the people to be secure against arbitrary uses of state power and broad, indiscriminate surveillance.[269]

Work done in the special needs context on alternatives to the warrant requirement has much to teach us as we confront the Fourth Amendment imperative to set constitutional limits on the deployment and use of facial recognition technology.[270] That is because the government interests at stake in these kinds of surveillance technologies are somewhat different than those at stake in the usual law enforcement context.[271] In the mine run of criminal cases, searches and seizures serve discrete investigative interests. Officers suspect a particular individual of wrongdoing and want to search his home for evidence of those specific crimes. Requiring officers to secure a warrant in these circumstance does not unreasonably compromise the governmental interests at stake. Instead, it simply means that officers must gather sufficient evidence by other means to demonstrate to a reasonable degree of certainty that evidence will be found in the place to be searched at the time of the

269. *Cf.* Carpenter v. United States, 138 S. Ct. 2206, 2235 (2018) (Kennedy, J., dissenting) ("Having concluded, however, that the Government searched Carpenter when it obtained cell-site records from his cell phone service providers, the proper resolution of this case should have been to remand for the Court of Appeals to determine in the first instance whether the search was reasonable. Most courts of appeals, believing themselves bound by *Miller* and *Smith*, have not grappled with this question. And the Court's reflexive imposition of the warrant requirement obscures important and difficult issues, such as the scope of Congress' power to authorize the Government to collect new forms of information using processes that deviate from traditional warrant procedures, and how the Fourth Amendment's reasonableness requirement should apply when the Government uses compulsory process instead of engaging in an actual, physical search."); *id.* at 2261 (Alito, J., dissenting) ("All of this is unnecessary. In the Stored Communications Act, Congress addressed the specific problem at issue in this case. The Act restricts the misuse of cell-site records by cell service providers, something that the Fourth Amendment cannot do. The Act also goes beyond current Fourth Amendment case law in restricting access by law enforcement. It permits law enforcement officers to acquire cell-site records only if they meet a heightened standard and obtain a court order. If the American people now think that the Act is inadequate or needs updating, they can turn to their elected representatives to adopt more protective provisions. Because the collection and storage of cell-site records affects nearly every American, it is unlikely that the question whether the current law requires strengthening will escape Congress's notice.").

270. *See* Natalie Ram & David Gray, *Mass Surveillance in the Age of COVID-19*, 7 J.L. & BIOSCIENCE 1, 9–10 (2020) (suggesting a special needs framework for regulating public health tracking technologies).

271. GRAY, *supra* note 196, at 266–67; Gray & Citron, *supra* note 45, at 116 (explaining the distinction between technologies used in discrete investigative circumstances and technologies that must be deployed in advance).

search and then submit that evidence to a neutral decisionmaker.[272] On the other side of the scales, the privacy and security interests at stake belong most immediately to a specific person. A warrant process is well-designed to vindicate those personal interests. Perhaps more importantly, that law enforcement officers are subject to the warrant requirement allows "the people" to live a relative state of security against threats of arbitrary search and seizure.[273]

In contrast with individual searches, the warrant process seems ill-suited to the interests at stake in the deployment and use of surveillance technologies capable of facilitating "too permeating police surveillance."[274] That is because these technologies need to be up and running in advance of when they might be needed for a particular law enforcement purpose. For example, imagine that law enforcement officers have an image of a murder suspect and want to use facial recognition to identify her.[275] That investigative strategy could only bear fruit if a facial recognition system was already in place with access to a robust database of identity-matched faces. Similarly, imagine that investigators have the image of a terrorist suspect, know he is operating somewhere in a metropolitan area, and want to use facial recognition technology to determine where he is and where he has been in recent days. They could only vindicate these completely legitimate law enforcement interests if a system of networked surveillance cameras with facial recognition capabilities and substantial image storage capacities was already in place and operating in the background to gather, aggregate, and store comparator images.

In either of these scenarios, the legitimate government interests served by facial recognition could not be served if officers had to get a warrant before creating and deploying the technology. The only way for facial recognition technologies to serve these legitimate government interests is to develop and deploy them before they are needed in a particular case. This is an endeavor that simply could not meet the particularity and probable cause requirements of a warrant process. And then there are more quotidian applications, such as biometric access to secured areas, and non-criminal uses, such as identity verification at immigration entry points. Though perhaps reasonable, these kinds of programs are just not amenable to a warrant requirement.

---

272. Johnson v. United States, 333 U.S. 10, 13–14 (1948).

273. *Id.*

274. *Carpenter*, 138 S. Ct. at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

275. Garvie et al., *supra* note 17 ("[t]he police are looking for an individual or a small number of individuals. They upload images of those individuals to a 'hot list.' A face recognition program extracts faces from live video feeds of one or more security cameras and continuously compares them, in real-time, to the faces of the people on the hot list. Every person that walks by those security cameras is subjected to this process. When it finds a match, the system may send an alert to a nearby police officer.").

So, if it is unreasonable from a Fourth Amendment point of view to require law enforcement to obtain a warrant before deploying and using facial recognition technologies, then what is the alternative? This is where we can take some guidance from the special needs context. Specifically, we should think more expansively about systems and processes with the goal of serving legitimate law enforcement interests while preserving the security of the people against unreasonable searches. There are also many applications of facial recognition technology that would fall squarely within the compass of special needs, such as Hawaii's proposal to use facial recognition as part of its efforts to combat the SARS-CoV-2 pandemic,[276] the use of facial recognition at immigration checkpoints,[277] and the use of facial recognition as a component of airport security.[278] But even in the context of normal criminal law enforcement, the special needs model has much to teach us about how to set reasonable limits on the deployment and use of facial recognition technologies.

Elsewhere, I have identified a framework that we can use to guide this analysis.[279] In that work, I argue that technologists and policymakers should think about the lifecycle of searches conducted using contemporary surveillance technologies and think about ways to interpose restraints on the development, deployment, and use of those technologies with the goal of striking a reasonable balance between the various government, privacy, and liberty interests at stake. Applying that approach to facial recognition technologies suggests focusing on five stages:

(1) Pre-Deployment Design and Review;
(2) Gathering and Aggregating Images and Data;
(3) Storage of Images and Data;
(4) Access to and Analysis of Images and Data;
(5) Use of the Results of that Analysis

The coming pages explore what is at stake at each of these opportunities and identify some measures we might consider when designing, deploying, and using facial recognition technologies.[280]

276. *See supra* note 40 and accompanying text.

277. *See supra* note 33–37 and accompanying text.

278. *See supra* note 35–37 and accompanying text.

279. GRAY, *supra* note 196, at 267–74; Ram & Gray, *supra* note 270, at 10–16.

280. Clare Garvie, Alvaro Bedoya, and Jonathan Frankle have proposed very thoughtful model legislation governing facial recognition. *See* Garvie et al., *supra* note 17 (model legislation can be found at https://www.perpetuallineup.org/sites/default/files/2016-10/Model%20Face%20Recognition%20Legislation.pdf). They have also drafted parallel administrative rules. *Id.* (model policy can be found at https://www.perpetuallineup.org/appendix/model-police-use-policy).

### A. Pre-Deployment Design and Review

Before deploying a facial recognition technology, proponents must identify the goals of the program and explain why it is likely to achieve these goals. Likewise, proponents must identify potential consequences for Fourth Amendment and other constitutional interests, including privacy, the potential for mass surveillance, grants of discretionary power, and equality.[281] Parsimony is a critical criterion at this stage.[282] Program designers should clearly and objectively weigh the likely benefits of a program against its potential impact with an eye toward minimizing harm. This requirement is directly in line with the Court's elaboration of "reasonableness" in the Fourth Amendment context, which requires striking a balance among the competing interests at stake in both general rules[283] and specific instances of search and seizure.[284] This basic requirement for reason-giving and balancing of interests also mirrors the warrant clause's oath and probable cause requirements, which imagines government agents' offering justifications for searches and seizures, including likelihood of success, timing, manner, and extent to a neutral arbiter.[285] If pre-deployment review of a facial recognition program shows that it is ineffective, not well-matched to its goals, unreasonably compromises citizens' privacy and security interests, is excessively broad or intrusive, or produces too many negative externalities, then it would be unreasonable to go forward. Proponents would then need to go back to the drawing board.

Pre-deployment review should also include an analysis of how the deployment and use of a technology would exacerbate background conditions of social injustice.[286] These are particularly salient questions when it comes to facial recognition technologies.[287] As Travis LeBlanc, former Chief of Enforcement at the Federal Communications Commission and current member of the Privacy and Civil Liberty Oversight Board, has pointed out, facial recognition technologies are notoriously error-prone when asked to identify

281. *See* LeBlanc, *supra* note 21.

282. GRAY, *supra* note 196, at 267–68.

283. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 20–25 (1968) (weighing the competing interests of law enforcement and citizens at stake to hold that stops and frisks based on reasonable suspicion are constitutional).

284. *See, e.g.*, Wilson v. Arkansas, 514 U.S. 927, 934–36 (1995) (holding that the Fourth Amendment "knock and announce" requirement may give way in circumstances where knocking and announcing would compromise law enforcement safety or the security of evidence).

285. GRAY, *supra* note 196, at 171.

286. LeBlanc, *supra* note 21 (arguing that surveillance technologies should be designed with equality in mind and programs utilizing those technologies should be subject to an equality impact assessment).

287. *Id.*

non-White faces, leading to wrongful arrests and detentions that disproportionately affect persons of color.[288] In a trenchant analysis, Mr. LeBlanc argues that technologists should take social justice goals into account when creating facial recognition tools—a process he calls "equality by design"—and that facial recognition technologies should be subject to "Equality Impact Assessments,"[289] a process akin to the environmental impact assessments often required by the Environmental Protection Agency. It would be unreasonable, he concludes, to deploy and use a facial recognition tool that exhibits racial bias in its pattern of false positives.[290]

Pre-deployment review of facial recognition programs should be transparent and public or, at the very least, publicly accountable.[291] Ideally, pre-deployment review would be open, affording all interested parties the opportunity to be heard. The end goal would be to generate some degree of consensus among stakeholders either through the normal operations of civil society and the political process[292] or through consent decrees entered into to resolve or avoid litigation.[293]

Designers should also incorporate regular, rigorous, transparent audits and reviews in their plans for a program. No matter how careful and robust

288. *Id.*; *see also* GROTHER ET AL., *supra* note 21, at 2–3 (documenting racial disparities in error rates produced by facial recognition technologies); Larry Hardesty, *Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems*, MIT NEWS (Feb. 11, 2018), https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212 (same).

289. LeBlanc, *supra* note 21.

290. *Id.* Although the Court has opined that racial disparities in enforcement practices are not cognizable under the Fourth Amendment. *See* Whren v. United States, 517 U.S. 806, 813 (1996).

291. GRAY, *supra* note 196, at 268; Garvie et al., *supra* note 17 ("All face recognition use should be subject to public reporting and internal audits.").

292. *See* Carpenter v. United States, 138 S. Ct. 2206, 2261 (2018) (Alito, J., dissenting) ("Legislation is much preferable to the development of an entirely new body of Fourth Amendment caselaw for many reasons, including the enormous complexity of the subject, the need to respond to rapidly changing technology, and the Fourth Amendment's limited scope. The Fourth Amendment restricts the conduct of the Federal Government and the States; it does not apply to private actors. But today, some of the greatest threats to individual privacy may come from powerful private companies that collect and sometimes misuse vast quantities of data about the lives of ordinary Americans. If today's decision encourages the public to think that this Court can protect them from this looming threat to their privacy, the decision will mislead as well as disrupt. And if holding a provision of the Stored Communications Act to be unconstitutional dissuades Congress from further legislation in this field, the goal of protecting privacy will be greatly disserved.").

293. Gray & Citron, *supra* note 45, at 116–23 (explaining the role of negotiated agreements and consent decrees in regulating surveillance technologies).

pre-deployment planning processes might be, it is impossible to understand fully both the potentials and dangers of these programs before they are deployed. In order to maintain the balance of interests that the Fourth Amendment demands, government agencies, their private contractors, legislators, courts, and civil society must learn from that experience with an eye toward evaluating efficacy, measuring encroachment upon Fourth Amendment interests, and guarding against mission creep. It would certainly be unreasonable to persist with a program that is not effective.[294] Reviews may also reveal that some programs are more intrusive than anticipated while others prove to be more innocuous than first anticipated, requiring or allowing adjustments to the program. But, above all else, programs must be protected from efforts to leverage them for other purposes. Mission creep is always a danger with surveillance technologies[295]—a reflection of the genetic propensities of executive agencies to expand their claims to power.[296] Regular, rigorous review, audits, and accountability to neutral third parties provide the best means for guarding against mission creep.

294. Although the probable cause requirement of the warrant clause makes clear the constitutional relevance of pre-search assessments of the likelihood of success, courts have been reluctant to measure the grounds of those assessments against past performance. Shima Baradaran Baughman has highlighted this oddity in the Court's jurisprudence. *See* Shima Baradaran, *Rebalancing the Fourth Amendment*, 102 GEO. L.J. 1 (2013). As Professor Baradaran Baughman shows, that reluctance is particularly evident in the stop and frisk context, where courts routinely accept platitudes like "furtive movements" as grounds for reasonable suspicion despite shockingly low success rates. *Id.* The Supreme Court, or at least Justice Kagan, seems to be coming around to Professor Baradaran Baughman's point, though. In *Florida v. Harris*, Justice Kagan, writing for the Court, held that drug detection dogs' past performances are relevant when assessing whether their alerts are grounds for reasonable suspicion or probable cause. Florida v. Harris, 568 U.S. 237, 245–50 (2013). Concurring in *Kansas v. Glover*, Justice Kagan made the same point with respect to human police officers, noting that "defendants may question testifying officers about such information. Indeed, an officer may have his own hit rate, which if low enough could itself negate reasonable suspicion." Kansas v. Glover, 140 S. Ct. 1183 (2019).

295. SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT TOGETHER WITH ADDITIONAL, SUPPLEMENTAL, AND SEPARATE VIEWS, 289–90 (Apr. 26, 1976).

296. *Id.* at 289 ("In time of crisis, the Government will exercise its power to conduct domestic intelligence activities to the fullest extent. The distinction between legal dissent and criminal conduct is easily forgotten."); *see also* Gray, *supra* note 139, at 169 (quoting MASERES, *supra* note 216, at 243–44 (noting that governments and their agents are "fond of doctrines of reason of state, and state necessity, and the impossibility of providing for great emergencies and extraordinary cases, without a discretionary power in the crown to proceed sometimes by uncommon methods not agreeable to the known forms of law.")); Gray & Citron, *supra* note 45, at 92, 96–97.

So, what might this requirement for rigorous pre-deployment review look like in practice? Consider, as an example, a technology akin to Clearview AI that purports to allow government agents to establish the identity of a person in an image. It sounds cool, but policymakers would need to ask serious questions about efficacy. Is the technology actually capable of doing what it promises? Does it provide material benefits over carbon-based facial recognition systems? What is the error rate, both in terms of false positives and false negatives? Is the error rate higher when the technology is applied to some races, genders, or ages? How will the program protect against adverse consequences from mistakes? It would be unreasonable to license the deployment of a technology that would seldom be helpful or would produce unreliable results.[297] In fact, several high-profile technology companies and municipalities have suspended or terminated facial recognition programs when confronted with evidence of racial disparities in false positives.[298]

### B. Gathering and Aggregating Images and Data

Facial recognition requires at least two images: one that is identified and a second that is compared to the first.[299] Functionally, this means that a facial recognition program needs a database of identified facial images that it can use to make comparisons and sources of comparator images that require identification. Each of these steps gives rise to practical, technical, privacy, and liberty concerns.

297. This basic rule of reason is pervasive in the law. For example, reliability is a central question when it comes to evaluating witness testimony or the admissibility of scientific evidence. *See* FED. R. EVID. 607, 701, 702.

298. *See, e.g.*, Ally Jarmanning, *Boston Bans Use of Facial Recognition Technology. It's the 2nd-Largest City to Do So*, WBUR, https://www.wbur.org/news/2020/06/23/boston-facial-recognition-ban (June 24, 2020); Dina Bass, *Microsoft Won't Sell Face Recognition Software to Police*, BLOOMBERG L. (June 12, 2020), https://news.bloomberglaw.com/tech-and-telecom-law/microsoft-wont-sell-police-face-recognition-software-for-now; Weise & Singer, *supra* note 30; Shirin Ghaffary, *San Francisco's Facial Recognition Technology Ban, Explained*, VOX (May 14, 2019), https://www.vox.com/recode/2019/5/14/18623897/san-francisco-facial-recognition-ban-explained; Hannah Denham, *IBM's Decision to Abandon Facial Recognition Technology Fueled by Years of Debate*, WASH. POST (June 11, 2020), https://www.washingtonpost.com/technology/2020/06/11/ibm-facial-recognition/.

299. Clearview AI appears to use a slightly different model, compiling massive databases of images, comparing images in that database, and drawing connections between probable matches, but does not necessarily establish the identity of a particular face. *See How Clearview AI Works*, CLEARVIEW.AI, https://clearview.ai/ (last visited June 14, 2021). It instead preserves source data on images in its database so a user can, for example, go to the webpage whence the image came. *See id.*

To build its database, a facial recognition program would need to either gather and aggregate images directly or access existing image caches. Both approaches entail practical challenges. Where will the program get the images? How will it attach identities to those images? How will it verify the accuracy of those identifications? There are technical considerations as well, which affect both database images and comparator images. Facial recognition technologies require images that are of sufficiently high quality and must either be in a digital format or converted to a digital format. Clarity, lighting, and angle also affect the ability of facial recognition tools to make reliable matches. Databases comprised of low-quality images taken from a variety of angles and taken under different conditions are less likely to produce consistent, reliable results.

There are also questions of robustness. Does the technology have access to a sufficiently large database of confirmed identities? This is a particularly important question for identification programs—as opposed to verification programs. Identification programs cannot succeed unless they contain an image of the person presented for comparison. Robustness must, of course, be balanced against privacy interests. A universal image database would certainly be sufficiently robust but would also raise the specter of broad and indiscriminate surveillance while threatening the privacy of, well, everyone! On the other hand, an image database comprised of booking photographs taken of arrestees would pose fewer privacy and liberty concerns,[300] but might well be sufficiently robust to serve most law enforcement interests in identifying suspects of crime—the usual suspects, and all.

Notice, consent, and scale also play important roles here. The Court has long held that if a person is on notice that they are subject to surveillance, then their expectations of privacy may be diminished or exhausted.[301] Similarly, those who voluntarily share information do not have a Fourth Amendment complaint if government agents access that information through lawful means.[302] Neither can they complain if they consent to a search.[303] While the

300. *Cf.* Maryland v. King, 569 U.S. 435, 438 (2013) (finding that arrestees and indictees have reduced expectations of privacy that licenses warrantless search procedures related to normal custodial procedures); Florence v. Bd. of Chosen Freeholders, 566 U.S. 318, 322–23 (2012) (holding that prisoners have diminished expectations of privacy, allowing jails to conduct strip searches).

301. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 449–50 (1989) (observing constitutionally protected areas from public airspace is not a "search" for purposes of the Fourth Amendment); Dow Chem. Co. v. United States, 476 U.S. 227, 250–51 (1986) (same); California v. Ciraolo, 476 U.S. 207, 215 (1986) (same); United States v. Knotts, 460 U.S. 276, 281–82 (1983) (using a radio beeper tracking device to monitor movements in public is not a "search" for purposes of the Fourth Amendment).

302. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 741–42 (1979) (holding law enforcement's accessing telephonic records does not violate a user's reasonable expectations of privacy); Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 23 (1974)

Court has declined to extend these doctrines in the case of means and methods of surveillance that are capable of facilitating broad and indiscriminate surveillance,[304] it generally does not impose Fourth Amendment constraints on more limited means.[305]

Together, these considerations counsel in favor of programs that are limited in scope and seek consent from, or at least provide notice to, those whose images are gathered and aggregated, or at least provide notice that their images are being gathered. Programs that derogate from this ideal raise more serious Fourth Amendment concerns and therefore require compelling justification and stricter constraints when it comes to analysis and access. Additionally, programs that use means that are themselves subject to Fourth Amendment restraint would need to incorporate additional constitutional protections. To see how all of this might work, let us consider a few examples.

---

(holding law enforcement's accessing banking records through a bank does not violate customers' reasonable expectations of privacy); Hoffa v. United States, 385 U.S. 293, 302 (1966) (holding no Fourth Amendment violation when an undercover agent reports what suspect said in his presence).

303. United States v. Drayton, 536 U.S. 194, 207 (2002) ("In a society based on law, the concept of agreement and consent should be given a weight and dignity of its own. Police officers act in full accord with the law when they ask citizens for consent. It reinforces the rule of law for the citizen to advise the police of his or her wishes and for the police to act in reliance on that understanding. When this exchange takes place, it dispels inferences of coercion.").

304. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) ("We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."). *See also* 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. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.").

305. *Knotts*, 460 U.S. at 283–84 (declining to subject radio beeper tracking devices to Fourth Amendment regulation in part because they cannot facilitate "dragnet-type" law enforcement practices). *See also* Gray & Citron, *supra* note 45, at 131–33 (explaining how a "technology-centered approach" to the Fourth Amendment distinguishes between technologies capable of facilitating programs of broad and indiscriminate search, which should be subject to Fourth Amendment regulation, and those that are not, which should not).

One application for facial recognition technologies might be to limit access to facilities such as workplaces and residential buildings. This would require an image database comprised of authorized employees or residents, which could be collected directly and with the notice and consent of those whose images are in the database. As a result, the privacy concerns raised by this kind of program would be relatively slight and the risks of broad and indiscriminate surveillance small—so long as the program stays in its lane. It would be both unnecessary and ineffective for this kind of program to aggregate or draw from a larger, more general database of images. It would likewise be unreasonable for images gathered by this kind of limited verification program to share its data with other programs—at least on a routine basis (one can certainly imagine circumstances where law enforcement officers might want access to a system like this to help solve a specific crime). As we shall see in a moment, limits on access akin to a warrant requirement would probably strike the right constitutional balance.

This is not to suggest that these limited use programs do not entail any privacy, liberty, or surveillance concerns. At the very least, they construct a record of people's comings and goings. In a world where these kinds of systems are broadly deployed, there is the potential to engage in the kind of location tracking that raised Fourth Amendment concerns for the *Carpenter* Court.[306] So, organizations considering facial recognition as a verification tool would need to consider carefully whether facial recognition is necessary in light of the security and access concerns at stake. It might well be reasonable to use facial recognition at a secure research facility but unreasonable to use it at an elementary school or public library.

By contrast, some facial recognition applications would need very large image databases and would probably need to access databases and image caches created for other purposes. Here we might imagine a system, such as Clearview AI, with aspirations of being able to identify anyone, and therefore everyone. A system with these kinds of ambitions would need wide access to a variety of image sources ranging from drivers' licenses to social media. Almost by definition, those whose images would be gathered and aggregated for this kind of program would be neither notified nor given the opportunity to consent.[307] These programs therefore raise serious privacy concerns. They also represent an immediate threat of broad and indiscriminate surveillance. What could be more threatening of a surveillance dystopia than an all-inclusive database of everyone's face! Whether these programs could meet Fourth Amendment demands would therefore turn on the benefits they realistically promise for law enforcement and the ability to guarantee security against unreasonable searches by setting strict limits on analysis and access, which, as we shall see, is the approach the Court took in *Carpenter*.

306. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

307. This is the basis of the class action lawsuit against Clearview AI in Illinois. *See supra* note 28.

Between these two extremes there is a wide range of potential applications that would vary in terms of scale, the sizes of their databases, sources of images, and levels of notice and consent. For example, cross-referencing systems, such as those used to verify the identity of visa and passport holders entering the country, would need a database that included all visa and passport holders, but those images would be gathered directly, on notice, and with at least implied consent. These databases would also be fairly modest in scale, only gathering comparator images from persons presenting themselves at immigration entry points.

We can also imagine more targeted identification systems focusing on terrorists or dangerous criminals. These kinds of programs would only require relatively small databases of images associated with known terrorists or designated criminal suspects. Such images might come from a variety of sources ranging from surveillance footage taken at the scene of a crime to mugshots to driver's license photos,[308] some of which would be gathered on notice and consent, and others not. But, given the limited scope and targeted need, these kinds of programs would raise many fewer privacy and surveillance concerns than programs like Clearview AI—at least with respect to the aggregation of databases. Gathering comparator images might present thornier concerns if, for example, law enforcement agents wanted to screen constantly images of everyone traversing public spaces in a search for criminal suspects. So, these programs would need to run the same Fourth Amendment gauntlets as any other program by clearly articulating the reasonable benefits they hope to achieve while balancing the privacy interests at stake, threats to liberty, and risks of broad and indiscriminate surveillance.

Separate from the process of gathering and aggregating images for a database, facial recognition technologies must also gather comparator images. Here, again, the Fourth Amendment issues at stake depend on the purpose and scale of the program. Returning to our examples, an access control system would only need to, and should only, acquire images of persons seeking access to the secured facility. It would be unnecessary and unreasonable for the system to gather images of passersby or from cameras at a remote location. But, assuming proper restraint, all those whose images would be taken for comparison purposes by this kind of limited facial recognition program would have consented to having their image taken by virtue of their presenting themselves for verification, again limiting the scope of Fourth Amendment concerns for these limited systems.

By contrast, more ambitious programs raise serious concerns when gathering and aggregating comparator images. This is entirely due to their scale and aspirations. At their apotheosis, these programs aim at what Christopher Slobogin has described as "panvasive" surveillance.[309] They aspire to

308. *See* Garvie et al., *supra* note 17 (finding that more than half of states allow facial recognition programs to access driver's license databases).

309. *See* Slobogin, *supra* note 43, at 1723.

identify everyone, everywhere, at any time. Granting these kinds of programs unlimited authority to gather and aggregate comparator images on an ongoing basis from hundreds or thousands of cameras would violate the reasonable expectations of privacy we all have in the totality of our public movements.[310] It would also trigger concerns about broad, indiscriminate surveillance and unfettered executive discretion that animated the Fourth Amendment when it was ratified. Given these concerns, there are serious questions about the Fourth Amendment viability of these kinds of facial recognition programs. The Fourth Amendment may just prohibit the deployment and use of technologies capable of identifying and tracking everyone, everywhere, all the time.[311] At the very least, the scale of these programs, as described by their ravenous need for both database and comparator images, signals the need for very strict access and use controls.[312]

Fourth Amendment concerns raised by other facial recognition programs will scale according to when comparator images are gathered, how, and how many. It might be reasonable for immigration control programs to gather comparator images at border kiosks and reentry desks in order to confirm the identities of travelers seeking entry into the country. These folks are on notice that their images are being taken, and the application would be sufficiently limited to avoid fears of broad and indiscriminate surveillance. Less reasonable would be requests to gather comparator images from shopping malls and street cameras to identify persons who might be in the country illegally. This would ensnare tens of thousands of persons who are not on notice that their images are being taken for facial comparison. It also smacks of the kind of "too permeating police surveillance" that has animated the Fourth Amendment since 1792.[313] Likewise, programs targeted at identifying known terrorist and criminal suspects that seek broad access to surveillance cameras and networks in order to monitor public places would trigger serious privacy concerns while also raising the specter of a surveillance state.[314] As with panvasive surveillance programs, these uses of facial recognition technology may just be unreasonable under the Fourth Amendment, but, at the very least, would require strict access and use controls sufficient to guarantee the right of the people to be secure from unreasonable searches.[315]

310. *Carpenter*, 138 S. Ct. at 2217 ("individuals have a reasonable expectation of privacy in the whole of their physical movements").

311. *See, e.g.*, Beautiful Struggle v. Balt. Police Dep't, 979 F.3d 219, 248 (4th Cir. 2020) (Gregory, J., dissenting) (concluding that plaintiffs were entitled to a preliminary injunction halting an aerial surveillance program).

312. *Id.* at 230–32 (holding that an aerial surveillance program was constitutional in part because it featured extensive internal regulations and access controls).

313. *Carpenter*, 138 S. Ct. at 2214.

314. *See id.*

315. *See* Slobogin, *supra* note 43, at 1761.

### C. Storage of Images and Data

Aggregated images do not simply flow through facial recognition technologies. They must be stored. The primary questions program designers must address when it comes to storage are what, how much, and how long. Our present capacity to store information is basically unlimited. Government agencies have access to facilities capable of storing yottabytes of data.[316] There are, therefore, no practical limits on the capacity of facial recognition programs to aggregate and store billions of images.[317] This kind of storage capacity would provide facial recognition programs with long memories, allowing government agents to return to both databases and comparator images again and again into perpetuity.

There is no doubt that this storage capacity and the ability to conduct future queries about the past raises serious Fourth Amendment concerns. The *Carpenter* Court highlighted some of these pointing out that "the retrospective quality of [cell site location] data" allows government agents to "travel back in time to retrace a person's whereabouts."[318] This potential would be at its apogee in the case of programs that aspire to panvasive surveillance capacities because "this newfound tracking capacity runs against everyone,"[319] but even more modest programs would raise concerns. For example, an access control program that uses facial recognition technology could monitor a subject's comings and goings in secured premises going back years, providing a record of location data that might be very revealing of the intimate details of their lives—think, here, about a system that monitored the movements of college students in dormitories. And then there is the very real risk that stored images and data might be mined for purposes other than those justifying their initial gathering and aggregation. Large caches of stored data seem to invite mission creep.

The primary tools for mitigating the Fourth Amendment harms of facial recognition technologies at the storage phase is to set clear limits on what is stored and for how long.[320] Systems inevitably will gather and aggregate surplus images. That information should not be stored. Regular audits are likely to be required to make sure that programs do not stock-up on images they do

316. *See* JAMES BAMFORD, THE SHADOW FACTORY 177–96 (2008) (documenting government efforts to build data storage facilities capable of storing yottabytes of data); James Bamford, *The NSA Is Building the Country's Biggest Spy Center*, WIRED (Mar. 15, 2012, 7:34 PM), https://www.wired.com/2012/03/ff-nsadatacenter/.

317. Bamford, *supra* note 316.

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

319. *Id.*

320. *See id.* at 2220.

not need or should not have.[321] Programs must also have strict rules on data destruction. If an employee leaves a company that uses facial recognition to control access to corporate facilities, then their image should be deleted from the database. In a similar vein, comparator images should be deleted immediately after the time horizon for the program's goals have passed. Once a person's identity has been confirmed at the front door of a building or an immigration checkpoint, there is no reason to store it.

Of course, the most challenging programs from a Fourth Amendment point of view will be those that aspire to panvasive capacities. By design, these programs will seek to store as many database images as they can while gathering, aggregating, and storing as many comparator images from as many sources as is possible for as long as is possible.[322] These aspirations to omnipotence are squarely opposed to Fourth Amendment guarantees against broad, indiscriminate surveillance and grants of unfettered discretion to search.[323] To have any hope of achieving constitutionally required reasonableness, these programs must curb their aspirations by culling images. This is particularly true of comparator images. Regularly deleting comparator images, such as feeds from surveillance cameras, would go a long way toward meeting the Fourth Amendment concerns cited by the Court in *Carpenter*.[324]

Another potentially important tool for regulating facial recognition technologies at the storage stage is siloing. This can be accomplished either by constructing discrete silos into which aggregated images and information are segregated or by simply leaving information in the custody and control of those who gathered it in the first place. This is one of the strategies adopted by Congress in its efforts to set limits on the National Security Agency's (NSA) telephony metadata program.[325] Under the terms of the 2015 USA Freedom Act, caller metadata is no longer turned over to the NSA in bulk.[326] That data remains instead with the telephone companies. To gain access to this data, the NSA must now formulate targeted search queries.[327] Similar measures designed to make sure that database images and comparator images are properly segregated will go a long way toward guarding against mission creep while also reinforcing rules on access.

321. Notably, facial recognition programs in place now are seldom subject to audit or review. *See* Garvie et al., *supra* note 17 (finding that the vast majority of facial recognition systems "are not audited for misuse").

322. *See* Slobogin, *supra* note 43, at 1746.

323. *See id.* at 1722.

324. *See Carpenter*, 138 S. Ct. at 2213.

325. Cody M. Poplin, *NSA Ends Bulk Collection of Telephony Metadata under Section 215*, L. FARE (Nov. 30, 2015, 3:47 PM), https://www.lawfareblog.com/nsa-ends-bulk-collection-telephony-metadata-under-section-215.

326. *Id.*

327. *Id.*

In addition to established limits on the storage of database and comparator images, facial recognition programs should be subject to regular audits and recursive review to determine whether more images and data are being stored than is necessary to achieve the stated goals of the program. These ongoing reviews are sure to reveal waste, surplusage, and opportunities to tailor information storage practices in light of actual experience. That is as it should be. Programs that keep and store more images and information than is reasonably necessary to achieve their stated goals compromise Fourth Amendment interests in privacy and security from surveillance while also offering temptations for mission creep.[328]

### D. Access to and Analysis of Images and Data

Databases of identified facial images are the lifeblood of facial recognition technologies. Once aggregated, these databases present a tempting target for facial recognition programs, particularly those with broad or ill-defined ambitions. Consider image databases aggregated by departments of motor vehicles. These are frequent targets for facial recognition programs.[329] Fourth Amendment concerns with broad and indiscriminate surveillance as well as grants of unfettered state power become more significant as programs gain access to more and larger facial databases. At the same time, reliance on notice and consent as grounds to justify the gathering, aggregation, and storage of images in these databases dissipate as access broadens. If I consent to have my picture taken and the image stored by my employer in order to gain access to secured areas of my workplace, then that consent cannot justify sharing that image with a national crime control database used to identify suspects and witnesses.

In order to guarantee security against unreasonable searches, access to image databases must be controlled in accordance with their original purposes and the terms governing their gathering and aggregation practices.[330] By limiting access along these lines, facial recognition programs can dramatically reduce threats of unreasonable searches and panvasive surveillance. Constitutional actors, inclusive of executive agencies, legislatures, and courts, should be very cautious about expanding access to image databases and should never do so without providing clear notice and real opportunities for individuals to opt-out.

More may be necessary to provide similar protections for databases or image resources held by private actors. For example, Clearview AI reportedly scrapes social media websites to build its image databases.[331] Although there is a case to be made that Clearview AI is a state actor for purposes of

328. *See Carpenter*, 138 S. Ct. at 2218.

329. *See supra* note 34, and accompanying text.

330. *Cf.* Garvie et al., *supra* note 17 (calling for strict limits to image databases, such as driver's license photos).

331. *See supra* note 22 and accompanying text.

the Fourth Amendment by virtue of the fact that its primary contracts are with law enforcement and other government agencies,[332] courts are reluctant to impose Fourth Amendment restraints on private corporations and persons.[333] Legislatures therefore ought to act by passing privacy protections that give individuals control over the use of their images and identities. The European Union's General Data Protection Regulation protects biometric information.[334] So do some state privacy laws.[335] Unfortunately, Congress has

332. Gray & Citron, *supra* note 45, at 133–37 (arguing that corporations that regularly provide consumer information to law enforcement are "state agents" for purposes of the Fourth Amendment); Ram & Gray, *supra* note 270, at 6 (explaining how the Supreme Court's decision in Carpenter, 138 S. Ct. at 2217, widens the scope of Fourth Amendment protections when government agents seek location information from private companies).

333. *See* Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 614 (1989) ("The Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative."); *see also* Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971) (distinguishing between private agents who act at the direction of law enforcement and those who do not); Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (holding that a burglar acting on his own initiative is not a state agent for purposes of the Fourth Amendment).

334. *See* General Data Protection Regulation, art. 9 (Eur.) ("Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.").

335. Illinois was the first state to identify concerns involving the use of biometric technology. In 2008, Illinois passed its Biometric Information Privacy Act (BIPA), which places limitations on how private entities can collect, store, and use biometric data. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008). Texas and Washington have since enacted similar laws. Henry Kusjanovic, *BIPA: An Example That More States Should Follow*, LOWEY DANNENBERG (Oct. 30, 2020), https://www.lowey.com/blog/bipa-an-example-that-more-states-should-follow/. The BIPA requires private corporations in possession of biometric information or identifiers to establish a publicly accessible retention policy. *See* 740 ILL. COMP. STAT. ANN. 14/5 (West 2008). Additionally, the BIPA provides guidelines of what requires written approval and written notice and provides guidelines for how a private entity could profit from the use of someone's biometric information. *See id.* In January 2020, Facebook settled a class-action suit alleging violations of the BIPA. *See* Natasha Singer & Mike Isaac, *Facebook to Pay $550 Million to Settle Facial Recognition Suit*, N.Y. TIMES (Jan. 29, 2020), https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html. Later that year, the American Civil Liberties Union sued Clearview for violation of the BIPA. *ACLU Sues Clearview AI*, *supra* note 28.

Few states have taken steps to address mounting concerns surrounding facial recognition. A few of the most notable states are Oregon, New Hampshire, and California who each have laws banning facial recognition technology on

yet to take any action to constrain access to images by facial recognition programs.[336] That is a failure to perform on its constitutional duty to guarantee the security of the people against unreasonable searches.[337]

Separate from the question of access to image databases is the question of access to facial recognition programs and their analytic results. The Fourth Amendment is genetically concerned with grants of broad, unfettered discretion to executive agents.[338] The Court is very cautious about granting executive agents that kind of broad authority, which presages broad and indiscriminate surveillance.[339] The primary tool for limiting discretion to

police body cameras. *See* Benjamin Hodges & Kelly Mennemeier, *The Varying Laws Governing Facial Recognition Technology*, IP WATCHDOG (Jan. 28, 2020), https://www.ipwatchdog.com/2020/01/28/varying-laws-governing-facial-recognition-technology/id=118240/. On March 31, 2020, Washington State approved most of the SB 6280, which attempts to regulate the state and local government agencies use of facial recognition services by July 2021. *See* Eugenia Lostri, *Washington's New Facial Recognition Law*, CTR. FOR STRATEGIC & INT'L STUDIES (Apr. 3, 2020), https://www.csis.org/blogs/technology-policy-blog/washingtons-new-facial-recognition-law.

336. There is not yet a federal law regulating facial recognition. In June 2020, legislators introduced the Facial Recognition and Biometric Technology Moratorium Act of 2020, in the Senate—S. 4084, 116th Cong. (2020)—and the House—H.R. 7356, 116th Cong. (2020)—which would ban federal agencies from acquiring, possessing, accessing, or using any form of biometric surveillance on U.S. soil. The legislation would also make federal funding for state and local law enforcement dependent on the establishment of similar bans. In August 2020, Senators Jeffrey Merkley and Bernie Sanders introduced the National Biometric Information Privacy Act of 2020. S. 4400, 116th Cong. (2020). Their bill would require that companies receive consent before collecting biometric information and establish clear retention and destruction schedules. *See id.*

337. *See* United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring) (lamenting the fact that "Congress and most States have not enacted statues regulating the use of GPS tracking technology for law enforcement purposes").

338. *See supra* notes 201–230 and accompanying text; *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) ("The net result is that GPS monitoring—by 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.'") (internal citation omitted).

339. *See* Carpenter v. United States, 138 S. Ct. 2206, 2213–14 (2018) ("The 'basic purpose of this Amendment,' our cases have recognized, 'is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.' . . . the Amendment seeks to secure 'the privacies of life' against 'arbitrary power.'") (internal citations omitted); *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) ("I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amend-

conduct physical searches is the warrant requirement, which lodges with "neutral and detached magistrate[s]" rather than "zealous officers . . . engaged in the often competitive enterprise of ferreting out crime" the task of determining whether a search is reasonable.[340] But the Court has demonstrated considerable flexibility, allowing for a range of remedial measures designed to limit the authority and discretion of government agents to conduct searches and seizures.[341] For example, police officers have authority in the first instance to determine whether there is probable cause to justify an arrest,[342] but must justify those decision to detached and neutral magistrates after the fact.[343] The Court has also sanctioned a range of different regulatory structures for searches conducted in service of regulatory and administrative goals under the "special needs" doctrine.[344] These precedents show that the form of constitutional restraint on executive agents should be linked to the nature and purpose of a search program and the means and methods deployed.[345]

The ultimate goal of limiting access to databases and analysis is to protect individual privacy while also guarding against overbroad searches, unlimited searches, and mission creep. The dangers of overbreadth are obvious. Using facial recognition programs to conduct general surveillance or to search for connections and patterns unrelated to or only tangentially related to the legitimate governmental interests cited to justify a program is, by definition, unreasonable.[346] So, too, is granting unlimited discretion for agents to access and run searches. It would certainly be unreasonable, for example, if officers could use a facial recognition program to conduct personal searches, such as identifying a person whom they suspect of having an affair with a spouse. Likewise, it would be unreasonable to use facial recognition technology to target political, religious, or racial groups.[347] Finally, there is the danger that a facial recognition program justified for one purpose may be used for entirely different purposes that were not contemplated when the program was designed, rendering its regulatory control structures incapable of securing constitutional rights. This kind of mission not only threatens to expand

ment's goal to curb arbitrary exercises of police power to and prevent 'a too permeating police surveillance.'") (internal citations omitted).

340. Johnson v. United States, 333 U.S. 10, 13–14 (1948).

341. *See* New York v. Burger, 482 U.S. 691, 702–03 (1987); Gerstein v. Pugh, 420 U.S. 103, 113–14 (1975).

342. *Gerstein*, 420 U.S. at 113–14.

343. *Id.*

344. *See, e.g.*, Burger, 482 U.S. at 702–03.

345. *See id.*; *Gerstein*, 420 U.S. at 113–14.

346. *See* Garvie et al., *supra* note 17.

347. *Id.* ("Use of face recognition to track people on the basis of their political or religious beliefs or their race or ethnicity should be banned.").

the scope of a facial recognition program, but also increases the dangers of false negatives and false positives.

Taking these considerations into account leads to the conclusion that access to some facial recognition programs should be governed by a warrant requirement. The most likely candidates are programs that pose the most significant dangers for broad and indiscriminate surveillance. On first blush, it may seem that a warrant requirement would spell the death knell for these kinds of facial recognition programs. To serve their purposes, these kinds of programs must be up and running well before they are needed, gathering, aggregating, and storing images and refining the algorithms used to conduct comparisons on a grand scale. But that charge misunderstands the remedy. The point would be to use warrants to limit access, not to bar deployment. So, the program might be deployed and active, but officers who want to run a search would need prior approval from a detached and neutral magistrate. This is precisely the approach adopted by the Court in *Carpenter*.[348] There, the Court used a warrant requirement to limit government access to cell site location data, which is continually gathered, aggregated, and stored by cellular service providers.[349] In the Court's view, that struck the right balance, protecting privacy, guarding against "too permeating police surveillance," while also preserving reasonable access to an important law enforcement tool. Congress took a similar approach in the USA Freedom Act, requiring national security agencies to secure a court order before accessing telephonic metadata gathered and stored by telephone service providers.[350] Given the privacy issues at stake, and potential for abuse, it may also be necessary to limit access to investigations of particularly serious crimes,[351] where traditional law enforcement techniques have been exhausted,[352] or both.[353]

The *Carpenter* Court's use of a warrant requirement may provide a useful model for bringing many facial recognition programs in line with Fourth Amendment commands; but a warrant requirement would unreasonably compromise government interests at stake in many programs.[354] Consider facial recognition programs deployed in support of government activities outside the law enforcement context that fall within the compass of "special needs." These programs are likely to be narrowly tailored and, due to their nature and

348. *See* Carpenter v. United States, 138 S. Ct. 2206, 2210–11 (2018).

349. *Id.*

350. USA Freedom Act, H.R. 3361, 113th Cong. (2014).

351. Garvie et al., *supra* note 17 (arguing that law enforcement should only have access to facial recognition technologies when investigating serious crimes).

352. This exhaustion requirement is a feature of the Wiretap Act. *See* 18 U.S.C. § 2518(3)(b)–(c) (1998).

353. *See id.* (add "*id.*") § 2518(7) (limiting access to wiretapping to an enumerated list of crimes after investigators have exhausted other investigative means).

354. *See Carpenter*, 138 S. Ct. at 2221.

purpose, unable to meet the demands of the warrant clause.[355] For example, immigration enforcement agents who want to use facial recognition technology to verify the identity of a passport or visa holder at a border checkpoint would not be able to demonstrate probable cause. On the other hand, this kind of program would only ensnare individuals who have knowingly submitted a database image and knowingly presented themselves for comparison. This kind of narrowly contrived program also does not pose a significant threat of broad and indiscriminate surveillance. So, a warrant requirement in this case would not only be inapt, but excessive, and therefore unreasonable.

This does not mean that facial recognition technologies deployed in service of administrative regimes and other special needs should not be subject to constitutional restraints. Quite to the contrary, access to image databases aggregated for these programs should be strictly limited in accordance with the purposes of a program. This may mean limiting access to particular places, such as terminals at border checkpoints, particular persons, such as agents on shift at those checkpoints, or pursuant to supervisory authority according to clearly defined rules, such as assessing the immigration status of an individual arrested on criminal charges. These access limits should have teeth. Those who misuse a technology should be subject to administrative, civil, or criminal consequences.[356]

Regardless of the front-end limits on access to facial recognition databases and analyses, reasonableness dictates the use of audit trails or other means of documenting who gains access, their sources of authority, and the nature of the searches they run.[357] This kind of access control is necessary to preserve accountability before and after the fact. Before the fact, these kinds of controls will limit access. They will also encourage restraint because those accessing a program will know that they are, well, under surveillance. Finally, reliable audit trails will make evaluating program effectiveness much easier while also providing a means for identifying mistake, abuse, or malfeasance.

### E. Use of Results of that Analysis

In addition, other limits on the deployment and use of facial recognition technologies, programs should set limits on how the results of comparisons and analyses can be used. Here, again, the primary concerns are exploitation, which may unreasonably compromise the security of individuals or targeted groups, and mission creep, which may threaten other constitutional interests, such as First Amendment rights, or Fourth Amendment guarantees against broad and indiscriminate surveillance. In order to guarantee focus and tight

355. *Id.*

356. This Court has cited these kinds of consequences in upholding special needs search regimes. *See, e.g.*, Maryland v. King, 569 U.S. 435, 444, 465 (2013).

357. Garvie et al., *supra* note 17 (calling for audits as a means to curb misuse of facial recognition technology).

connections between justification and use, programs must set limits on who can use the results and how. For example, it would be entirely unreasonable to allow the results of a facial recognition program designed to confirm the identities of those entering the country to target members of particular religious groups or to use a technology designed to identify criminal suspects to identify participants in lawful political protests. Absent these kinds of controls, the threat of mission creep and the potential for abuse is simply too strong, threatening the right of the people to be secure against unreasonable searches.

Independent audits and external accountability will play critical roles in setting and enforcing these limits. Although a warrant requirement may not always strike the right balance, the Court's defense of the warrant requirement as a means for insulating critical decisions from the effects of bias, interest, and mission-blindness illuminates the importance of third-party review and accountability for all facial recognition programs. Outside reviewers could measure and adjust internal rules and practices to guarantee that technologies are being used in ways that faithfully reflect the balancing of interests that informed pre-deployment design. They can also make regular assessments of effectiveness to determine whether the goals of a program are being met. External reviews will have important disciplinary effects on agents as well. If individuals accessing the results of a facial recognition analysis know that they will be subject to administrative, civil, or criminal consequences, then they are bound to be more measured in the way they use facial recognition and more cognizant of the constitutional and privacy interests at stake.

Finally, consistent, regular, and rigorous review will allow programs to adjust along the way. Despite their best efforts, designers, legislators, civic groups, and executive agents cannot anticipate all the legitimate uses to which a facial recognition technology or its components might be put. Likewise, they cannot anticipate all the dangers of expansion, mission creep, and misuse. It will therefore be necessary to revisit many of the same questions that drive pre-deployment design in the context of consistent, rigorous programmatic review. If a program turns out not to serve its purpose, or to serve its purpose less well than less intrusive alternatives, then it should be shut down. If an audit reveals that a program is gathering more images than it needs or storing images longer than is reasonably necessary, then adjustments should be made to aggregation and storage practices. As was the case in the pre-deployment stage, these reviews should be open and transparent or, at the very least, accountable to all interested groups through responsible representatives.

## IV. CONCLUSION

We find ourselves at a cusp when it comes to facial recognition technologies. Once science fiction, these technologies have evolved rapidly in recent years, threatening to make the nightmares of George Orwell and Philip K. Dick a reality. The Fourth Amendment guarantees our security against those

threats, but it is, after all, just words on a page. It is the solemn duty of constitutional actors in all three branches of our governments to breathe life into those words by giving effect to our birthright. This article has identified the challenges and has charted a path forward. It now falls to each of us and all of us citizens to take and demand action.