
Digital Commons@
Loyola Marymount University
LMU Loyola Law School

Loyola of Los Angeles Law Review

Volume 55 | Number 4 Article 3

Fall 10-19-2022

Smile! You're on Camera: Police Departments' Use of Facial Recognition Technology & the Fourth Amendment

Adriana Bass

Follow this and additional works at: https://digitalcommons.lmu.edu/llr

Recommended Citation

Adriana Bass, *Smile! You're on Camera: Police Departments' Use of Facial Recognition Technology & the Fourth Amendment*, 55 Loy. L.A. L. Rev. 1053 (2022).
Available at: https://digitalcommons.lmu.edu/llr/vol55/iss4/3

This Notes is brought to you for free and open access by the Law Reviews at Digital Commons @ Loyola Marymount University and Loyola Law School. It has been accepted for inclusion in Loyola of Los Angeles Law Review by an authorized administrator of Digital Commons@Loyola Marymount University and Loyola Law School. For more information, please contact digitalcommons@lmu.edu.

SMILE! YOU'RE ON CAMERA: POLICE DEPARTMENTS' USE OF FACIAL RECOGNITION TECHNOLOGY & THE FOURTH AMENDMENT

*Adriana Bass**

TABLE OF CONTENTS

* J.D. Candidate, May 2022, LMU Loyola Law School, Los Angeles; B.S. Business Administration, The University of Southern California, May 2018. Thank you to the editors and staff of the Loyola of Los Angeles Law Review for their help in editing this Note. Additionally, thank you to Alexander Moore, Chloe Rome, and Professor Kevin Lapp for your continuous guidance and thoughtful feedback. A special thank you to my family and friends for your constant, unwavering support. Lastly, thank you Owen for listening to me talk about this Note for hours on end.

I. INTRODUCTION

Robert Julian-Borchak Williams is a 42-year-old Black male that lives in Farmington Hills, Michigan, with his wife and two daughters.[1] January 9, 2020, started out like any other Thursday afternoon for Williams.[2] However, that Thursday was different. Unexpectedly, Williams received a phone call from the Detroit Police Department while he was at work. The officer stated that he was required to go to the police station to be arrested.[3] Williams thought this was a prank call, so he hung up the phone and drove home after the workday ended.[4] An hour later, he arrived at home where a police car pulled up behind him.[5] The officers got out of their vehicle and arrested Williams in front of his wife and two young daughters.[6] The police did not tell him why he was being arrested. All they did was show Williams a piece of paper with a photo of him and the words "felony warrant" and "larceny."[7]

Williams was taken to a detention center where he had his mug shot, fingerprints, and DNA taken.[8] He was interrogated by two detectives.[9] One detective asked Williams when was the last time he had visited a Shinola store.[10] He responded that the last time he went to a Shinola store was in 2014 with his wife when the store had first opened.[11]

The detectives placed three pieces of paper, facedown, on the table.[12] The detective turned over one of the pieces of paper and showed Williams a still image of a man taken from surveillance video.[13] The

1. *See, e.g.*, Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/L39H-RL8T]; Bobby Allyn, *'The Computer Got It Wrong': How Facial Recognition Led to False Arrest of Black Man*, NPR (June 24, 2020, 8:00 AM), https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig [https://perma.cc/F37D-XCCS].

2. *See, e.g.*, Hill, *supra* note 1; Sarah Coble, *Lawsuit Filed After Facial Recognition Tech Leads to Wrongful Arrest*, INFO SEC. (Apr. 14, 2021), https://www.infosecurity-magazine.com/news/lawsuit-facial-recognition-tech [https://perma.cc/JD3W-SXE2].

3. *See* Hill, *supra* note 1.
4. *See id.*
5. *See id.*
6. *See id.*
7. *See id.*
8. *See id.*
9. *See id.*
10. *See id.*
11. *See id.*
12. *See id.*
13. *See id.*

man in the image was heavyset, dressed in black, wore a red St. Louis Cardinals cap, and he was standing in front of the watch display.[14] The man in the image had stolen five watches, estimated to be worth $3,800.[15] The police claimed this man was Williams.[16]

Shinola security camera image.

Alan Lengel, *'60 Minutes' Features Man Falsely Arrested By Detroit Police Because Of Flawed Facial Recognition*, DEADLINE DETROIT (May 16, 2021, 10:28 PM), https://www.deadlinedetroit.com/articles/28013/60_minutes_features_man_falsely_arrested_by_detroit_police_because_of_flawed_facial_recognition [https://perma.cc/KZ5D-GVDK].

Photo of Robert Julian-Borchak Williams.

Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

14. *See id.*
15. *See id.*
16. *See id.*

The detective then flipped over another paper.[17] This image was a blurry close-up snapshot of the man.[18] Facial recognition technology had identified the man in the photo as Williams. But the image was very clearly not Williams.[19] Williams picked up the photo and placed it next to his face.[20] He declared that it was not him in the image and that he did not commit this crime.[21] That night, Williams was released on a $1,000 personal bond.[22] At the time Williams was released, his criminal charge was pending.[23]

Despite the risks of false matches and wrongful arrests, facial recognition technology is becoming more prevalent in our society. Congress has introduced legislation to regulate the technology. However, these efforts have not been successful.[24] Law enforcement's use of facial recognition technology to identify protesters following the death of George Floyd in 2020 has brought this topic to the forefront of the national conversation.[25] During the George Floyd protests, activists and protesters feared that the police would retaliate against them since law enforcement could easily identify protesters with facial recognition technology. This is particularly troubling because people may hesitate to participate in protests that are a fundamental aspect of our democracy.

Companies are now reevaluating whether they want to continue to sell their facial recognition technology to police departments because of concerns that police might abuse the technology and the fact that the technology disproportionately impacts people of color.[26] In June 2020, IBM decided that it will "no longer provide facial

17. *See id.*
18. *See id.*
19. *See id.*
20. *See id.*
21. *See id.*
22. *Id.*
23. Complaint at 3, Williams v. City of Detroit, No. 21-cv-10827 (E.D. Mich. Apr. 13, 2021).
24. *See, e.g.*, George Floyd Justice in Policing Act of 2020, H.R. 7120, 116th Cong. (2020); Advancing Facial Recognition Act, H.R. 6929, 116th Cong. (2020); Stop Biometric Surveillance by Law Enforcement Act, H.R. 7235, 116th Cong. (2020).
25. *See* Jordan Williams, *Watchdog: Six Federal Agencies Used Facial Recognition Software to ID George Floyd Protesters*, THE HILL (June 29, 2021, 5:20 PM), https://thehill.com/policy/technology/560805-watchdog-6-federal-agencies-used-facial-recognition-software-to-id-george [https://perma.cc/A34N-SN72].
26. Isobel Asher Hamilton, *Outrage Over Police Brutality Has Finally Convinced Amazon, Microsoft, and IBM to Rule Out Selling Facial Recognition Tech to Law Enforcement. Here's What's Going On*, BUS. INSIDER (June 13, 2020, 2:01 AM), https://www.businessinsider.com/amazon-microsoft-ibm-halt-selling-facial-recognition-to-police-2020-6 [https://perma.cc/TH3A-Y5ZE].

recognition technology to police departments for mass surveillance and racial profiling."[27] However, other companies are waiting for Congress to determine whether law enforcement's use of facial recognition technology is acceptable. As of June 2020, Amazon has paused selling its facial recognition technology, Rekognition, to allow Congress to have the time to place limits on how the technology can be used.[28]

In the words of IBM's chief executive, Arvind Krishna, "now is the time to begin a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies."[29] This Note will partake in this dialogue and will set out a proposal detailing how this technology should be employed. This Note will mainly focus on police departments' use of facial recognition technology as a mechanism of mass surveillance. It will also touch upon other agencies' use of the technology, such as the FBI and ICE.

Facial recognition technology is new, real, invasive, and scary. Part I of this Note will analyze how facial recognition technology works and its different forms. It will also analyze police departments' use of facial recognition technology and the pros and cons of the technology. Part II of this Note will analyze law enforcement agencies' use of facial recognition technology and the potential for Fourth Amendment violations stemming from such use. The Fourth Amendment will not prohibit law enforcement's use of the technology in the forms of face identification and face verification. However, the Fourth Amendment may potentially prohibit law enforcement's use of facial recognition technology in the forms of face tracking and face surveillance. Facial recognition technology is too dangerous for society to wait on courts to confront this issue, if they ever decide to. Therefore, legislative response is necessary, and society must put pressure on

27. Bobby Allyn, *IBM Abandons Facial Recognition Products, Condemns Racially Biased Surveillance*, NPR (June 9, 2020, 8:04 PM), https://www.npr.org/2020/06/09/873298837/ibm-abandons-facial-recognition-products-condemns-racially-biased-surveillance [https://perma.cc/A96H-U658].

28. *See, e.g.*, Rebecca Heilweil, *Big Tech Companies Back Away from Selling Facial Recognition to Police. That's Progress*, VOX (June 11, 2020, 5:02 PM), https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police [https://perma.cc/RC75-9HHG]; Jeffrey Dastin, *Amazon Extends Moratorium on Police Use of Facial Recognition Software*, REUTERS (May 19, 2021, 11:12 AM), https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/.

29. *IBM CEO's Letter to Congress on Racial Justice Reform*, IBM (June 8, 2020), https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/ [https://perma.cc/432G-QQSC].

government and businesses to stop using this technology. Part III of this Note will discuss why legislation is necessary to regulate law enforcement's use of facial recognition technology. It offers specific recommendations for Congress when passing a law regulating facial recognition technology.

II. FACIAL RECOGNITION TECHNOLOGY

A. The Technology and How it Works

Facial recognition technology is a type of software that matches photos of faces to enable identification. Facial recognition technology can identify or verify a person from a digital image or a video.[30] In general, the technology works by "comparing selected facial features from the given image with faces within a database."[31] Typically, the process is broken down into three steps: face detection, face capture, and face match.[32] During the face detection step, one's face is located and captured.[33] Next, the face capture stage transforms the image of the face into digital information.[34] Lastly, during the face match stage, the initial image detected in step one is compared with faces in other images to determine whether the images are of the same person.[35] Facial recognition technology manifests itself in different forms, each serving a different purpose. These forms include face surveillance, face identification, face verification, and face tracking.[36]

1. Face Surveillance

Face surveillance is defined as "generalized monitoring of public places or third-party image sets using facial surveillance technologies to match faces with a prepopulated list of face images held by the government."[37]

30. Relly Victoria Virgil Petrescu, *Face Recognition as a Biometric Application*, 3 J. MECHATRONICS & ROBOTICS 237, 237 (2019).

31. *Id.*

32. *Facial Recognition: Top 7 Trends (Tech, Vendors, Use Cases)*, THALES (June 24, 2021), https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition [https://perma.cc/T39Q-MX9Y].

33. *Id.*

34. *Id.*

35. *Id.*

36. Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1112-13 (2021).

37. *Id.* at 1116.

Face surveillance may take place through stored footage, in real-time, and by way of third-party records.[38] Face surveillance through stored footage allows law enforcement officers to search video footage from networked surveillance cameras.[39] This method of surveillance "allows police to scan through stored footage and identify individuals by their face, aggregate their movements, interests, and patterns, and store and study these pathways for long periods of time."[40] Police may search through stored footage to identify an individual without suspecting that person of any wrongdoing.[41] Furthermore, face surveillance in real time is exactly what it sounds like: real-time public monitoring. Additionally, face surveillance by way of third-party stored images can occur by scanning private photo databases or private digital images stored on Facebook, Instagram, and Twitter.[42]

Face surveillance has already been implemented in Detroit, Michigan through Project Green Light.[43] The Detroit Police Department uses this facial recognition technology to locate and identify individuals with an arrest record using cameras across the city, in real time.[44] One example of an area that has been surveilled by police is the area outside Summit Medical Center, a reproductive and women's health center.[45] Any passerby, patron, or patient that is caught walking outside the Center has their face scanned and compared with the Detroit Police Department's facial recognition database.[46] Patients visiting the health center may now feel uncomfortable to seek out treatment at the clinic knowing that the police are watching them enter and leave the clinic.

38. *Id.*
39. *Id.*
40. *Id.* at 1144.
41. *Id.*
42. *Id.* at 1118.
43. *See, e.g.*, Clare Garvie & Laura M. Moy, *America Under Watch*, GEO. L. CTR. ON PRIV. & TECH. (2019), https://www.americaunderwatch.com/ [https://perma.cc/T39W-UMC2]; Steve Neavling, *Researchers Alarmed by Detroit's Pervasive, Expanding Facial-Recognition Surveillance Program*, DETROIT METRO TIMES (May 17, 2019), https://www.metrotimes.com/news-hits/archives/2019/05/17/researchers-alarmed-by-detroits-pervasive-expanding-facial-recognition-surveillance-program [https://perma.cc/4GMS-R9LH].
44. Garvie & Moy, *supra* note 43.
45. *Id.*
46. *Id.*

2. Face Identification and Face Verification

Face identification's purpose is to identify an unknown face whereas face verification seeks to confirm an individual's identity.[47] Face identification is the most commonly used form of facial recognition technology.[48] Unlike general face surveillance, police use face identification when they have suspicion about an individual, an image of their face, and are attempting to identify the person.[49] For example, police may obtain an image of a suspect from a crime scene through surveillance camera video, and compare that image with photos in databases to check for matches and identify the suspect. The Detroit Police Department used facial recognition technology in the form of face identification in the incident involving Robert Julian-Borchak Williams above. There, the officers used face identification to identify the individual who committed the theft in the Shinola store. However, this identification was clearly a technological error. Furthermore, this error can also be attributed to the officers for not verifying or inspecting the result the technology provided. An example of how police could use face verification would be where a police officer takes a photo of individual and runs it through the police department's facial recognition database to ensure that the individual is who they claim to be.

3. Face Tracking

Face tracking is a combination of face surveillance and face identification.[50] Face tracking utilizes the same facial recognition surveillance technologies, "but with particularized suspicion of a specific target."[51] Like face surveillance, face tracking may take place through stored footage, in real time, and by way of third-party records.[52] Police can monitor past or present movements of the specific target.[53] This aggregated information could reveal an abundance of information about the target, such as their interests, place of employment, hobbies,

47. CLARE GARVIE ET AL., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 10 (2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf [https://perma.cc/XD4S-P8L5].

48. Ferguson, *supra* note 36, at 1152.

49. *Id.* at 1119.

50. *Id.* at 1122.

51. *Id.*

52. *Id.*

53. *Id.* at 1122–23.

and more. For example, face tracking could occur where the police need to identify a suspect who robbed a store, so they track the suspect through surveillance cameras walking through the streets surrounding that store.

4. How Police Use Facial Recognition Technology

Police departments across the United States are using facial recognition technology and are building their own facial recognition databases.[54] Law enforcement uses facial recognition technology for two reasons: (1) face identification and (2) face verification.[55] However, law enforcement could be using the technology in other ways, such as face surveillance and face tracking. If law enforcement agencies are using facial recognition technology in other ways, the public is unaware of those uses.

Little is known about police departments' facial recognition databases. Little is known partially because "there are few laws or regulations governing what databases the systems can tap into, who is included in those databases, the circumstances in which police can scan people's photos, how accurate the systems are, and how much the government should share with the public about its use of the technology."[56] These databases may be comprised of driver's license photos, mugshots, and jail booking records.[57] Some companies, such as Clearview AI, have created their own databases containing more than three billion images that have been taken from Facebook, YouTube, Venmo, and other websites.[58] Law enforcement can pay to access these private databases. Clearview AI's CEO has stated that more than 2,400 police agencies use the software.[59]

54. GARVIE ET AL., *supra* note 47, at 1.

55. *Id.* at 10.

56. Jon Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC NEWS (May 11, 2019, 1:19 AM), https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251 [https://perma.cc/9XA4-PNV3].

57. *Id.*

58. Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/9L7S-MY5B].

59. Elizabeth Lopatto, *Clearview AI CEO Says 'Over 2,400 Police Agencies' Are Using Its Facial Recognition Software*, THE VERGE (Aug. 26, 2020, 4:40 PM), https://www.theverge.com/2020/8/26/21402978/clearview-ai-ceo-interview-2400-police-agencies-facial-recognition [https://perma.cc/RQN9-6R8E].

Research has shown that law enforcement face recognition databases include over 117 million American adults.[60] By one estimate, "one in two American adults is in a law enforcement face recognition network."[61] Who are these 117 million adults that are in these databases? Since little is known about these databases, inferences have to be made based on what information these databases encompass. If these databases are comprised of driver's licenses, anyone who has a license could be in a database. However, if these databases mainly consist of individuals with mugshots and jail bookings, there are likely a disproportionate number of people of color that would be represented in these databases. Arrest rates for Black and White individuals vary significantly. Studies have shown that "Black juveniles [are] arrested at twice the rate of White juveniles."[62] Moreover, "research suggests a similar disparity among the adult population. By the age of 18, Black males are at a 30% risk of arrest compared to 22% for White males, and by the age of 23, Black males are at a 49% risk of arrest, whereas White males are at a 38% risk of arrest."[63] From the outset, these databases may include a disproportionate number of Black and Brown individuals. This technology and its databases will amplify the negative effects of policing that people of color already experience.

B. Pros and Cons of Facial Recognition Technology

Facial recognition technology provides many benefits, but there are also concerns about the negative impacts it has on society.

1. Benefits

Nearly all of the benefits that facial recognition technology provides revolve around preventing or reducing crime. In some ways, facial recognition technology has increased public safety and continues to do so. For example, in 2019, police used the technology to "track down an accused rapist fewer than 24 hours after he tried to force a

60. Angela Chen, *Most Americans Are Fine with Cops Using Facial Recognition on Them*, MIT TECH. REV. (Sept. 5, 2021), https://www.technologyreview.com/2019/09/05/133149/facial-recognition-police-law-enforcement-surveillance-privacy-pew-research-survey/ [https://perma.cc/GD69-KBTT].

61. GARVIE ET AL., *supra* note 47, at 1.

62. Cydney Schleiden et al., *Racial Disparities in Arrests: A Race Specific Model Explaining Arrest Rates Across Black and White Young Adults*, 37 CHILD & ADOLESCENT SOC. WORK J. 1, 1 (2020).

63. *Id.*

woman into sex at knife-point."[64] The suspect was found with Facial Identification Section, a facial recognition technology. The technology compared a video of the suspect from a nearby food store to its database of mugshots.[65] The technology matched the suspect in the video to a prior mugshot of the suspect. Subsequently, the police were able to arrest the suspect. Law enforcement arrest individuals involved "in rape cases at a notoriously low rate because of the resources and manpower it takes to identify a suspect, and the crime is historically repeated—and often escalated."[66] Thanks to the use of facial recognition technology, the police identified and apprehended the suspect quickly, before he could assault more people.

Facial recognition technology may also allow law enforcement to investigate and prevent acts of terrorism. Although no acts of terrorism have been prevented through the use of such technology, law enforcement has the technology available to potentially prevent such acts. For example, in the New York City subway system, police use facial recognition technology to identify whether a subway user is on a terror watch list.[67]

Another benefit of the technology is that it can help law enforcement agencies find missing people and missing children. For example, in 2008, the San Diego County Sheriff's Department launched the Take Me Home Program.[68] Police use facial recognition technology to identify missing or lost citizens with disabilities, such as autism, dementia, Alzheimer's, and Down syndrome.[69] The Take Me Home Program is a voluntary database where individuals can upload their photos or photos of family members. If an individual is missing, facial recognition technology can be used to identify the individual by comparing an image of the person taken by police officers with an image in the database.[70] The technology is also beneficial because it allows

64. Craig McCarthy, *Facial Recognition Leads Cops to Alleged Rapist in Under 24 Hours*, N.Y. POST (Aug. 5, 2019, 6:03 PM), https://nypost.com/2019/08/05/facial-recognition-leads-cops-to-alleged-rapist-in-under-24-hours/ [https://perma.cc/D9WH-F7NK].

65. *Id.*

66. *Id.*

67. Anthony M. Carter, Facing Reality: The Benefits and Challenges of Facial Recognition for the NYPD 55 (Sept. 2018) (M.A. thesis, Naval Postgraduate School) (on file with Homeland Security Digital Library).

68. *Id.* at 59.

69. *Id.*

70. Lauren J. Mapp, *'Take Me Home' Program Helps Find Most Vulnerable Population When They Wander*, SAN DIEGO UNION TRIB. (Feb. 25, 2020, 2:53 PM), https://www.sandiegouniontribune.com/caregiver/news-for-caregivers/story/2020-02-25/take-me-home-program-helps-most-vulnerable-population-when-they-wander [https://perma.cc/JA4P-7EK6].

law enforcement to identify individuals who have trouble communicating or cannot communicate.[71] Moreover, facial recognition technology combined with aging software may in fact enable law enforcement to find individuals who have been missing for years.[72]

2. Concerns

At the same time, there are many concerns about facial recognition technology. Two major concerns are at the forefront of law enforcement's use of this technology: the potential for racial and other biases and concerns revolving around privacy and security.

First, facial recognition technology repeatedly shows signs of racial and other biases. The algorithms have higher error rates when identifying individuals of color, specifically Black individuals. Moreover, there are other biases present in this technology's algorithms, specifically regarding gender and age.[73] One study specifically identified lower recognition accuracy in three commercial algorithms on females, Black individuals, and those within the age group of 18 to 30.[74] Another study that analyzed Microsoft, IBM and Face ++'s technology confirmed these results and found that there are higher error rates on Black females.[75] When it comes to Amazon's Rekognition technology, racial bias has been at the forefront of the conversation. Rekongition "managed to confuse photos of 28 members of Congress with publicly available mug shots. . . . 'Nearly 40 percent of Rekognition's false matches . . . were of people of color, even though they make up only 20 percent of Congress.'"[76]

Today, Black individuals are disproportionately harmed by policing practices. People are worried that law enforcement's use of facial recognition technology will exacerbate the discriminatory policing

71. SAN DIEGO CNTY. SHERIFF'S DEP'T, TAKE ME HOME: HELPING AT-RISK SAN DIEGANS GET HOME SAFELY, https://www.sdsheriff.gov/home/showpublisheddocument/729/637460448105530000 [https://perma.cc/DJV6-QS49].

72. David Gargaro, *The Pros and Cons of Facial Recognition Technology*, IT PRO (July 20, 2021), https://www.itpro.com/security/privacy/356882/the-pros-and-cons-of-facial-recognition-technology [https://perma.cc/L3HA-N294].

73. Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 IEEE TRANSACTIONS ON INFO. FORENSICS & SEC. 1789, 1800 (2012).

74. *Id.*

75. Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 1, 11 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf [https://perma.cc/9965-FMNL].

76. Brian Barrett, *Lawmakers Can't Ignore Facial Recognition's Bias Anymore*, WIRED (Jul. 26, 2018, 4:59 PM), https://www.wired.com/story/amazon-facial-recognition-congress-bias-law-enforcement/ [https://perma.cc/4JFX-WZBP].

already faced by the Black community. Facial recognition technology not only performs worse on Black individuals, but also "African Americans [are] more likely to be enrolled in those systems *and* be subject to their processing."[77] These concerns are real. Law enforcement's use of the technology is negatively impacting Black individuals, as depicted in the example above about Robert Julian-Borchak Williams's false arrest.

Second, facial recognition technology poses risks to privacy and security. According to Algorithmic Justice League, "face surveillance threatens rights including privacy, freedom of expression, freedom of association and due process. . . . There is a reason why surveillance has been a tool of authoritarian regimes and facial surveillance risks amplifying this effect further in the twenty-first century."[78] People do not want their faces recorded and "stored in a database for unknown future use."[79] These privacy concerns focus on the idea that "these systems can quickly, cheaply, and easily ascertain where we've been, who we've been with, and what we've been doing. All based on a unique marker that we cannot change or hide: our own faces."[80] Privacy concerns regarding law enforcement's use of facial recognition technology center around the Fourth Amendment and its protections. The following part will discuss how facial recognition technology fits within the meaning of the Fourth Amendment as it is interpreted today.

III. FOURTH AMENDMENT ANALYSIS

The fundamental issue with facial recognition technology is whether its use by law enforcement violates the Fourth Amendment. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and

77. Clare Garvie & Jonathan Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, THE ATLANTIC (Apr. 7, 2016) (emphasis added), https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/ [https://perma.cc/MA2C-HJ5Z].

78. *What Is Facial Recognition Technology?*, ALGORITHMIC JUST. LEAGUE, https://www.ajl.org/facial-recognition-technology [https://perma.cc/J46G-2E34].

79. Gargaro, *supra* note 72.

80. Adam Schwartz, *Resisting the Menace of Face Recognition*, ELEC. FRONTIER FOUND. (Oct. 26, 2021), https://www.eff.org/deeplinks/2021/10/resisting-menace-face-recognition [https://perma.cc/B76U-KAZU].

> particularly describing the place to be searched, and the persons or things to be seized.[81]

The Fourth Amendment limits police surveillance. The Fourth Amendment aims to secure "'the privacies of life' against 'arbitrary power.'"[82] Moreover, as Justice Sotomayor wrote in her concurring opinion in *United States v. Jones*,[83] the "Fourth Amendment's goal [is] to curb arbitrary exercises of police power and prevent 'a too permeating police surveillance.'"[84] Since courts have not determined whether facial recognition technology constitutes a search, this part of the Note will analyze law enforcement's use of facial recognition technology with fundamental Fourth Amendment case law to determine whether law enforcement's use of facial recognition technology is a search. Based on current case law, facial recognition technology used for face identification and face verification would not be deemed to be a search. However, when the technology is used for face surveillance and face tracking, the Court should find this to be a search.

A. Face Identification, Face Verification, and Fourth Amendment Case Law

Katz v. United States[85] redefined what is meant by a "search" for Fourth Amendment purposes.[86] In *Katz*, FBI agents attached an electronic listening and recording device to the outside of a public telephone booth where Katz was making phone calls transmitting illegal wagering information.[87] The FBI was only targeting Katz; they were not listening into other conversations.[88] The Court held that the officer's unwarranted wiretapping of the phone booth violated Katz's Fourth Amendment right.[89] The Court reasoned that the Fourth Amendment "protects people, not places."[90] This outcome overturned the Court's prior cases[91] that ruled that the Fourth Amendment only offers protection when there has been a trespass on physical property.

81. U.S. CONST. amend. IV.
82. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).
83. 565 U.S. 400 (2012).
84. *Id.* at 416-17 (Sotomayor, J., concurring).
85. 389 U.S. 347 (1967).
86. *Id.* at 348.
87. *Id.*
88. *Id.* at 354.
89. *Id.* at 360.
90. *Id.* at 351.
91. *See, e.g.*, Olmstead v. United States, 277 U.S. 438 (1928).

In his *Katz* concurrence, Justice Harlan formulated the "reasonable expectation of privacy" test that concludes a search occurs when police action violates a subjective and reasonable expectation of privacy.[92] Usually, the subjective belief prong is satisfied. Post-*Katz*, it has been "generally understood that the police are free to investigate public places, speak with people consensually, and access information that has already been given to third parties."[93] The Court has often emphasized Congress's role in regulating technological advances and the government's use of such technology. The ruling in *Katz* prompted Congress to pass the Wiretap Act to regulate law enforcement's surveillance of private communications.[94]

It is unlikely that facial recognition technology, specifically in the forms of face identification and face verification, would be deemed a search under the reasonable expectation of privacy test. Under the subjective prong of the test, a person does not have an expectation of privacy in public. People have a general understanding that their person can be seen and even photographed while in public. Especially given cities' use of video surveillance on public streets, individuals are increasingly aware that they are being or can be observed. Furthermore, face identification and face verification involve the police capturing an image of an individual and matching that photo to individuals in databases. It is unlikely that matching photos of suspects lawfully obtained to photos in a database would be considered to violate a subjective and reasonable expectation of privacy.

Sixteen years after *Katz* was decided, in *United States v. Knotts*,[95] the Court determined that there is no reasonable expectation of privacy when a person travels on public roads from one place to another.[96] In *Knotts*, a radio transmitter was placed in a barrel containing chloroform purchased by one of Knotts's codefendants.[97] The transmitter emitted periodic signals that enabled Minnesota law enforcement to trace the location of the vehicle carrying the chloroform from Minneapolis to Knotts's cabin in Shell Lake, Wisconsin.[98] The Court held

92. 389 U.S. at 361.

93. *See* Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 33 (2016) (footnote omitted).

94. *See* Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197.

95. 460 U.S. 276 (1983).

96. *Id.* at 281.

97. *Id.* at 277.

98. *Id.*

that the use of the radio transmitter did not violate Knotts's Fourth Amendment right because law enforcement agents monitoring the radio transmitter's signals did not invade any legitimate expectation of privacy.[99]

Through the Court's analysis in *Knotts*, the Court provides some indication as to how facial recognition technology could potentially be viewed under the Fourth Amendment. The Court stated there is no reasonable expectation of privacy extending to a "visual observation" of an object on private property.[100] The Court also specified, "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[101] The Court declared that it "never equated police efficiency with unconstitutionality."[102] Following the Court's reasoning in *Knotts*, if the Court found that facial recognition technology fell under the category of a "visual observation," the technology could be viewed as a technological enhancement that makes policing more efficient, and thus, would not be deemed a search under the Fourth Amendment.

However, the Supreme Court has limited police use of new technology during criminal investigations. In *Kyllo v. United States*,[103] law enforcement used thermal imaging technology to confirm that Kyllo was growing marijuana in his house.[104] The Court has always valued the privacy of an individual in their home. Consequently, the Court ruled in favor of Kyllo and deemed the warrantless search of the house to be unreasonable, violating the Fourth Amendment.[105] The Court also reasoned that this was a violation of the Fourth Amendment because law enforcement used a device that is not in general public use "to explore details of the home that would previously have been unknowable without physical intrusion."[106]

Arguably, *Kyllo* would not have the same outcome if it were before the Court today because thermal imaging technology is available for the public to use. Similarly, it can be argued that facial recognition technology is also available for the general public to use since some

99. *Id.* at 285.
100. *Id.* at 282.
101. *Id.*
102. *Id.* at 284.
103. 533 U.S. 27 (2001).
104. *Id.* at 30.
105. *Id.* at 40.
106. *Id.*

facial recognition technology companies make their services available to the public to purchase.

B. Face Surveillance, Face Tracking, and Fourth Amendment Case Law

The Supreme Court has likewise protected privacy expectations by limiting the ability of police to amass bits of information about a person's travels in public. In *United States v. Jones*, the government suspected Jones of trafficking narcotics.[107] The government had initially obtained a warrant authorizing the installation of a GPS tracking device on a vehicle registered to Jones's wife within ten days.[108] However, the government placed the GPS tracking device on the eleventh day and tracked Jones for 28 days.[109] The Court held that the attachment of the GPS tracking device to the vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets violated the Fourth Amendment.[110] In his concurrence, Justice Alito reasoned that short-term monitoring of a person's movements on public streets does not constitute a search while long-term GPS monitoring constitutes a search.[111] In her concurrence, Justice Sotomayor reasoned that she "would take [the] attributes of GPS monitoring into account" when determining if there was a reasonable expectation of privacy "in the sum of one's public movements."[112] Moreover, Justice Sotomayor stated "[she] would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[113]

In *Carpenter v. United States*,[114] cell-site location information was used to position Timothy Carpenter at the scene of a series of robberies around Detroit.[115] One of the men arrested identified several accomplices, one being Carpenter.[116] The prosecutors applied for court orders under the Stored Communications Act to obtain

107. United States v. Jones, 565 U.S. 400, 402 (2012).
108. *Id.* at 402–03.
109. *Id.* at 403.
110. *Id.* at 413.
111. *Id.* at 430 (Alito, J., concurring).
112. *Id.* at 416 (Sotomayor, J., concurring).
113. *Id.*
114. 138 S. Ct. 2206 (2018).
115. *Id.* at 2212.
116. *Id.*

Carpenter's cell phone records.[117] Federal Magistrate Judges issued orders directing Carpenter's wireless carriers to disclose cell-site location information.[118] Through this information, the government obtained 12,898 of Carpenter's location points. The Court held that the "government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements."[119]

The Court was faced with the challenge of "how to apply the Fourth Amendment to a new phenomenon."[120] The Court reasoned that this digital data did not fit "neatly under existing precedents" and instead lay "at the intersection of two lines of cases."[121] The first line of cases addressed "a person's expectation of privacy in his physical location and movements."[122] The Court explained that in *United States v. Knotts*, the use of the beeper "'augment[ed]' visual surveillance,"[123] whereas in *United States v. Jones*, the Court considered "more sophisticated surveillance"[124] that could "track 'every movement' a person makes in that vehicle."[125] The second line of cases addressed information that "a person keeps to himself and what he shares with others."[126] The Court did not extend the third-party doctrine to cover cell-site location information.[127] In his majority opinion, Justice Roberts states that "[a] majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements."[128] The Court held that the Government accessing Carpenter's cell site location information "invaded [his] reasonable expectation of privacy in the whole of his physical movements."[129] Such holding has implications for face surveillance and face tracking.

Although an individual does not have a reasonable expectation of privacy in public, a person also "does not surrender all Fourth

117. *Id.*
118. *Id.*
119. *Id.* at 2215.
120. *Id.* at 2216.
121. *Id.* at 2214.
122. *Id.* at 2215.
123. *Id.* (alteration in original) (quoting United States v. Knotts, 460 U.S. 276, 282 (1983)).
124. *Id.*
125. *Id.* (quoting United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring)).
126. *Id.* at 2216.
127. *Id.* at 2217.
128. *Id.* (citing *Jones*, 565 U.S. at 430 (Alito, J., concurring); *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).
129. *Id.* at 2219.

Amendment protection by venturing into the public sphere."[130] Face surveillance and face tracking can disclose information regarding an individual's physical movements. The *Carpenter* Court stated that its decision does not cover "conventional surveillance techniques and tools, such as security cameras."[131] However, facial recognition technology in the form of face surveillance and face tracking are not conventional surveillance techniques. Face surveillance and face tracking enable police to learn information about an individual through the aggregation of data. The aggregation of data, particularly videos, reveals one's detailed physical movements over a period of time that can provide police with additional information about a person. Individually, each face surveillance and face tracking occurrence probably does not amount to a Fourth Amendment search. However, these occurrences added together should be deemed to be a search under the Fourth Amendment.

C. Litigating Facial Recognition Technology

As of November 2021, although there have been a number of complaints filed against facial recognition technology companies alleging that facial recognition technology violates the Fourth Amendment, no court in the United States has published an opinion regarding the constitutionality of the technology.[132] However, it would be helpful for our courts and members of Congress to know how courts in other countries have handled the issue of police's use of facial recognition technology.

In August 2020, a court of appeal in South Wales ruled that the South Wales Police Force's use of live automated facial recognition technology breached privacy rights and broke equalities law. The South Wales police department used facial recognition technology to find individuals on the department's "watchlist."[133] Therefore, the

130. *Id.* at 2217.

131. *Id.* at 2210.

132. Complaint at 18, Mutnick v. Clearview AI, Inc., No. 20-cv-00512 (N.D. Ill. Jan. 22, 2020).

133. Bridges v. The Chief Constable of South Wales Police [2020] EWCA Civ 1058, [13] (Eng.).

> The watchlist is created from images held on databases maintained by SWP as part of its ordinary policing activities, primarily from a database of custody photographs held on SWP's Niche Record Management System. The images selected for inclusion on a watchlist will depend on the purpose of each specific deployment. The watchlists used in the deployments in issue in this case have included (1) persons wanted on warrants, (2) individuals who are unlawfully at large (having escaped from lawful custody), (3) persons suspected of having committed crimes, (4)

technology was targeted to find specific individuals while surveilling all individuals that appeared in the surveillance cameras. The appellant, Edward Bridges, based his appeal on the notion that the technology was "unlawfully intrusive, including under Article 8 of the European Convention on Human Rights ('ECHR') (right to respect for private and family life) and data protection law in the UK."[134]

Bridges challenged the police's use of facial recognition technology on five bases.[135] First, the court looked at whether the interference with individuals' right to privacy was in accordance with the law under Article 8(2) of the ECHR.[136] The court found that the police's use of the technology was not in accordance with the law because police were left too much discretion to use the technology, and there was little guidance concerning who can be placed on a watchlist and where the technology could be used.[137] Second, the court looked at whether the police's use of the technology constituted a proportionate interference with Article 8 rights within Article 8(2).[138] The interference must satisfy a four-part test to be considered proportionate; the test was satisfied in this case.[139] The court found that "the impact on each of the

---

> persons who may be in need of protection (*e.g.* missing persons), (5) individuals whose presence at a particular event causes particular concern, (6) persons simply of possible interest to SWP for intelligence purposes and (7) vulnerable persons. To date, the watchlists used by SWP have comprised between 400-800 people. The maximum capacity for a watchlist is 2,000 images but, as we understand it, this is because of the limits of the technology used rather than any limitation of principle.

Id.

134. *UK Court of Appeals Finds Automated Facial Recognition Technology Unlawful in Bridges v South Wales Police*, HUNTON ANDREWS KURTH (Aug. 12, 2020), https://www.huntonprivacyblog.com/2020/08/12/uk-court-of-appeal-finds-automated-facial-recognition-technology-unlawful-in-bridges-v-south-wales-police/ [https://perma.cc/8FN3-82ZJ].

135. *Id.*

136. *Id.*; Bridges v. The Chief Constable of South Wales Police [2020] EWCA Civ 1058, [53] (Eng.). Article 8 of the European Convention on Human Rights states:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

137. Bridges v. The Chief Constable of South Wales Police [2020] EWCA Civ 1058, [129], [130] (Eng.).

138. *Id.* at [53].

139. *Id.* at [132]. The four-part test takes into account the following questions:

> (1) whether the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right; (2) whether it is rationally connected to the objective; (3) whether a less intrusive measure could have been used without

other members of the public who were in an analogous situation to [Bridges] . . . was as negligible as the impact on the Appellant's Article 8 rights."[140] Third, the court considered whether South Wales Police Force's Data Protection Impact Assessment complied with the requirements of section 64 of the Data Protection Act.[141] The court found that it did not.[142] Fourth, the court considered whether South Wales Police Force complied with the requirements of section 42 of the Data Protection Act.[143] The court found that it did.[144] Lastly, the court considered whether the South Wales Police's Equality Impact Assessment complied with the Public Sector Equality Duty under the Equality Act 2010.[145] The court found that the South Wales Police's Equality Impact Assessment did not comply with the Equality Act because the South Wales Police Force failed to demonstrate that the software used does not have racial or gender biases.[146]

The underlying theme of Bridges' argument was that "there is a balance to be struck between their need to fight crime and the public's need to feel reassured, and that their rights are being respected."[147] This is a core theme within criminal procedure case law in the United States: what is the proper balance between the public's right of privacy, liberty, and dignity, and public and officer safety, crime control, and crime prevention? This ruling should be a signpost for courts, members of Congress, and state and city legislatures that police departments' use of facial recognition technology, especially in the forms of face surveillance and face tracking, do not strike the proper balance among the competing values.

IV. PROPOSAL

"That the Fourth Amendment does not regulate . . . early stages of investigation draws on well-established Supreme Court case

---

> unacceptably compromising the objective; and (4) whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.

Id.

140. *Id.* at [143].
141. *Id.* at [53].
142. *Id.* at [153]–[154].
143. *Id.* at [53].
144. *Id.* at [161].
145. *Id.* at [53].
146. *Id.* at [201].
147. *Facial Recognition: What Led Ed Bridges to Take on South Wales Police?*, BBC NEWS (Aug. 11, 2020), https://www.bbc.com/news/uk-wales-53742099 [https://perma.cc/45VZ-MA89].

law."[148] When police investigate a crime, they have some discretion on what methods of surveillance they choose to use and who they choose to observe, whether that be a specific individual or group of individuals. As long as the surveillance of an individual or several individuals remains in a public setting, police are not required to suspect that such individuals have engaged in criminal activity in order to observe them.[149] The Fourth Amendment does not usually apply to considerations such as "[h]ow long the police watch a person, why the police decide to investigate one person rather than another, and why they decide to investigate a crime" because these "all are matters for police discretion."[150]

The Supreme Court has not yet determined whether law enforcement's use of facial recognition technology constitutes a search under the Fourth Amendment. Moreover, "because the Fourth Amendment does not regulate surveillance discretion"[151] and "courts have had little to say about"[152] regulating surveillance discretion, it is unlikely that the issue will reach the Supreme Court anytime soon. So, if the Fourth Amendment does not limit the use of facial recognition technology, what can?

The first potential limit may be the price of facial recognition technology. The price could deter police departments or agencies from investing their money in the technology. However, as the technology becomes more available, prices will decrease. Furthermore, police departments, especially in big cities like New York, Los Angeles, and Chicago, have big budgets. Police department budgets "range from just over $100 million a year (Virginia Beach, Virginia) to $5 billion a year (New York City)."[153] Thus, this doesn't seem to be a likely restraint.

Second, external oversight from communities may be the check that could limit facial recognition technology's use. Arguably, if it were not for the George Floyd protests in the summer of 2020, Microsoft, IBM, and Amazon would not have stopped or paused selling

148. Joh, *supra* note 93, at 33.
149. *See id.*
150. *Id.*
151. *Id.* at 34.
152. *Id.*
153. Carl Sullivan & Carla Baranauckas, *Here's How Much Money Goes to Police Departments in Largest Cities Across the U.S.*, USA TODAY (June 26, 2020, 7:00 AM), https://www.usatoday.com/story/money/2020/06/26/how-much-money-goes-to-police-departments-in-america-largest-cities/112004904/ [https://perma.cc/S4NJ-G7ZD].

their products to police departments. When communities vocalize their opinions and desires, they can create significant change. However, as discussed below, individuals cannot be a check on the technology's use if they do not know how the technology is being used.

There seems to be only one way to effectively limit law enforcement's use of facial recognition technology—legislation. As Justice Alito indicated in *United States v. Jones*, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[154]

Regulation through legislation is incredibly important and is not used enough to regulate policing.[155] Legislation, at both the state and federal levels, must be utilized to regulate policing in America because the Fourth Amendment does not provide enough protection. Police departments are often times left to regulate themselves. Yet, most police departments do not publish their police manuals for the public to access.[156] This lack of transparency creates a lack of trust. Based on numerous studies, "individuals are far more likely to comply with the law and to cooperate with law enforcement authorities when they perceive their actions as legitimate—and that one critical component of legitimacy is the perception that police officials are responsive to community demands."[157]

Although several cities have passed their own laws attempting to regulate facial recognition technology, no federal regulation currently exists. There have been efforts on behalf of several members of Congress to attempt to regulate this technology, yet none of these efforts have been successful. One proposal, the George Floyd Justice in Policing Act of 2021, would have placed some restrictions on law enforcement's use of facial recognition technology.[158] The main restriction was that body cameras could not be equipped with or employ any facial recognition technologies.[159] The law passed the House by a

154. United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J. concurring).

155. *See* Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1843 (2015).

156. *Id.* at 1848–49.

157. *Id.* at 1881.

158. George Floyd Justice in Policing Act of 2021, H.R. 1280, 116th Cong. (2021).

159. *Id.*

220–212 vote and has not passed the Senate.[160] Yet, this law rarely mentioned facial recognition technology and did not go in depth into law enforcement's use of the technology. Until a federal law is passed that places overarching restrictions on law enforcement's use of facial recognition technology, communities will face the negative consequences of law enforcement's unmonitored use of the technology.

A. Facial Recognition Technology's Unregulated Use Today

If unregulated, facial recognition technology's use could fundamentally alter the way society functions. The world has already witnessed the impact that uncontrolled public and private mass surveillance may have. A prime example of such mass surveillance is occurring in China.

In China, almost every single citizen is in a facial recognition database.[161] That amounts to images of about 1.4 billion people.[162] Moreover, there are about 200 million surveillance cameras across the country watching individuals' movements.[163] These cameras can identify jaywalkers and students sleeping in classrooms.[164] Police in China have even started wearing sunglasses equipped with facial recognition technology to identify individuals, and the technology is capable of comparing images in a database to the individual the police officer sees in one tenth of a second.[165]

Racial profiling facilitated by facial recognition technology has resulted in a mass incarceration of Uyghur Muslims in China.[166] In just one month in February 2019, law enforcement scanned individuals' faces in the city of Sanmenxia 500,000 times to identify whether

160. *Actions Overview: H.R. 1280 – 117th Congress (2021-2022)*, CONGRESS.GOV, https://www.congress.gov/bill/117th-congress/house-bill/1280/actions (last visited Aug. 25, 2022).

161. *See, e.g.*, Amanda Lentino, *This Chinese Facial Recognition Start-Up Can Identify a Person in Seconds*, CNBC (May 17, 2019, 1:14 PM), https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html; Seungha Lee, *Coming into Focus: China's Facial Recognition Regulations*, CTR. FOR STRATEGIC & INT'L. STUD. (May 4, 2020), https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations [https://perma.cc/EZC3-QMXQ].

162. Lentino, *supra* note 161.

163. *Id.*

164. *Id.*

165. Abby Norman, *Chinese Police Add Facial Recognition Glasses to Their Surveillance Arsenal*, FUTURISM (Feb. 8, 2018), https://futurism.com/chinese-police-facial-recognition-glasses-surveillance-arsenal [https://perma.cc/XN4K-V35D].

166. Alfred Ng, *How China Uses Facial Recognition to Control Human Behavior*, CNET (Aug. 11, 2020, 5:00 AM), https://www.cnet.com/news/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/ [https://perma.cc/P62K-2NCG].

or not they were Uyghurs.[167] Clare Garvie, an associate at the center of Privacy and Technology at Georgetown Law, stated that "[i]f you make a technology that can classify people by an ethnicity, someone will use it to repress that ethnicity."[168] China's government justifies the repression of their Uyghur population under the guise of safety. However, the identification of Uyghurs through facial recognition technology has enabled the placement of thousands in reeducation camps just because they are a minority ethnicity, not because they pose an actual threat to the society. China's authoritarian use of such technology shows the rest of the world the extent that this technology can be used and is seen to be an "existential threat to democracy."[169]

The United States has never been a surveillance society, nor should it be. It is doubtful that the United States would ever mimic this level of surveillance, but this is an extreme example of the negative effects unregulated use of facial recognition technology can have on society.

B. Cities and States Take Action

Since 2019, at least twenty cities have already taken steps to control facial recognition technology. But these efforts must be more expansive in order to robustly protect individual privacy.[170] In 2019, San Francisco was one of the first cities to ban the use of facial recognition technology.[171] 2020 was a major milestone for passing regulations concerning facial recognition technology. Beginning in January 2020, New Jersey's attorney general demanded that law enforcement stop using Clearview AI.[172] Clearview AI is a "web-based intelligence platform for law enforcement to use as a tool to help generate high-quality investigative leads."[173] Its "platform, powered by facial recognition

167. Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. TIMES (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html [https://perma.cc/69A9-8XUV].

168. *Id.*

169. *Id.*

170. *See generally* Complaint at 15, Williams v. City of Detroit, No. 21-cv-10827 (E.D. Mich. Apr. 13, 2021).

171. Jack Morse, *Here's Why San Francisco's Vote to Ban Facial-Recognition Tech Matters*, MASHABLE (May 14, 2019), https://mashable.com/article/san-francisco-bans-facial-recognition-technology/ [https://perma.cc/68QS-YNCC].

172. Jack Morse, *New Jersey Halts Police Use of Creepy Clearview AI Facial-Recognition App*, MASHABLE (Jan. 24, 2020), https://mashable.com/article/clearview-ai-facial-recognition-app-ban-police-new-jersey/ [https://perma.cc/WJ93-2JYH].

173. *Company Overview*, CLEARVIEW AI, https://www.clearview.ai/overview [https://perma.cc/WLY9-YAW4].

technology, includes the largest known database of 10+ billion facial images."[174] In June 2020, elected officials in Boston passed an ordinance prohibiting "both the city of Boston and any official in the city of Boston from using 'face surveillance' and 'information derived from a face surveillance system.'"[175] In September 2020, Portland, Oregon, moved to ban the city's and private business's use of facial recognition technology.[176] In November of 2020, voters in Portland, Maine, strengthened an existing ban on facial recognition technology giving residents the right to sue "the city if its employees violate the face surveillance ban."[177] Under the strengthened law, if an individual finds that "'any person or entity acting on behalf of the City of Portland, including any officer, employee, agent, contractor, subcontractor, or vendor' used facial recognition on them, that person is entitled to no less than $100 per violation or $1,000 (whichever is greater)."[178] Virginia followed suit and banned the technology in February 2021. Although these cities and states are moving in the right direction, federal laws regulating cities' and states' use of facial recognition technology would afford more protection for individuals across the United States, not only in the cities or states that decide to pass legislation.

C. What Should Be Done

1. Complete Ban

One potential solution to regulating facial recognition technology would be to completely ban its use. Generalized mass surveillance is undesirable. Many cities and states, as mentioned above, have already passed laws that ban facial recognition technology's use, and the federal government must also take this step.

As discussed above, facial recognition technology's signs of racial and gender biases are a few of the main reasons why there should be a complete ban of its use. Since the technology has been shown to

174. *Id.*

175. Jack Morse, *Boston Bans Most City Use of Facial-Recognition Tech in Privacy Win*, MASHABLE (June 24, 2020), https://mashable.com/article/boston-bans-facial-recognition-technology/ [https://perma.cc/57ZS-JF5S].

176. Tom Simonite, *Portland's Face-Recognition Ban Is a New Twist on 'Smart Cities,'* WIRED (Sept. 21, 2020, 9:00 AM), https://www.wired.com/story/portlands-face-recognition-ban-twist-smart-cities/ [https://perma.cc/388S-CUFH].

177. Jack Morse, *Maine Voters Double Down on Facial Recognition Ban in Win for Privacy*, MASHABLE (Nov. 4, 2020), https://mashable.com/article/portland-maine-passes-facial-recognition-ban-fines/ [https://perma.cc/E8RY-ETGF].

178. *Id.*

be inaccurate, it is unfair to subject individuals, especially people of color, to the risk of being falsely arrested. As seen above with the story of Robert Julian-Borchak Williams, this is not a hypothetical situation. Individuals are already being falsely arrested for crimes they have not committed. It would be unfair, knowing the inaccuracies of this technology, to permit its use when it can negatively impact so many individuals that have done nothing wrong.

Another driving force warranting a complete ban of facial recognition technology is its chilling effect on First Amendment activity.[179] Above all else, the Constitution was intended to "safeguard fundamental values."[180] These fundamental values include the freedom of speech and the right of people to peaceably assemble, both protected by the First Amendment.[181] In *NAACP v. Alabama*[182] and *Talley v. California*,[183] the Supreme Court held that the First Amendment protects the right to anonymous speech. The Court in *Talley* found "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance."[184] Yet, unrestricted use of facial recognition technology removes the protection afforded by First Amendment case law to participate in anonymous speech because the technology removes the anonymity. If individuals know that they could be observed and identified by law enforcement while exercising their right to peaceably assemble, it could dissuade individuals from exercising their rights. Consequently, this could lead to a society that refuses to engage in important civil matters. As discussed above, this is going on in China today. The technology has already begun to control individuals' behavior, and that will not stop until the technology ceases to be used.

179. For a greater discussion on Facial Recognition Technology and the First Amendment, see Katja Kukielski, Note, *The First Amendment and Facial Recognition Technology*, 55 LOY. L.A. L. REV. 231 (2022).

180. United States v. Chadwick, 433 U.S. 1, 9 (1977).

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

182. 357 U.S. 449 (1958). In *NAACP v. Alabama*, the Court held that Alabama could not compel the NAACP to reveal their membership list to the State's Attorney General. *Id.* at 451. The Court reasoned that requiring the NAACP to produce their membership list would substantially restrain members' right to freedom of association. *Id.* at 462.

183. 362 U.S. 60 (1960). In *Talley v. California*, the Court held that a Los Angeles City ordinance prohibiting the distribution of handbills that did not have printed on them the names and addresses of individuals who prepared, distributed, or sponsored the handbill was unconstitutional because it abridged "freedom of speech and of the press secured against state invasion by the Fourteenth Amendment of the Constitution." *Id.* at 60–61, 65.

184. *Id.* at 65.

There should be a complete ban until the technology is proven to be equally accurate on individuals of all races and genders. This technology is too powerful and susceptible to abuse to go unchecked and unregulated.

2. Full Transparency

Short of a ban, there are multiple safeguards that can be put in place to regulate facial recognition technology's use. The first safeguard available in regulating facial recognition technology is for the departments and agencies using the technology to be fully transparent that first, they use the technology, and second, how exactly they use it. There is a secrecy that revolves around the way police departments conduct their work, and the mechanisms police departments use to police. As Barry Friedman states, "[t]ransparency and democratic accountability are not optional. They are requisites of American governance."[185]

Sometimes, the secrecy may come from the private nature of doing business between the companies selling facial recognition technology and law enforcement agencies or police departments. When police are secretive, it limits external oversight. Some companies selling facial recognition technology do not only sell their product to law enforcement agencies and police departments; they have many other private customers and businesses that purchase their products. Therefore, some facial recognition technology companies may not want police or law enforcement to disclose to the public how their products work, which could limit the possibility of transparency. However, when individuals are impacted by the use of such technology, and yet, the extent of that impact is unknown, companies must make an effort to be fully transparent with communities that are the subject of this technology. If a company does not want details of their technology to be disclosed to the public, that company should not sell their technology to police departments or law enforcement agencies.

Knowing what technology police departments and agencies are using is the first step to achieving the necessary level of transparency. Cities and states should put regulations in place that require local officials to approve their police department's use of facial recognition technology. These regulations should be similar to the ordinance that

185. Friedman & Ponomarenko, *supra* note 155, at 1881.

passed in Seattle, Washington, that required the city council to approve any city department's acquisition of surveillance equipment.[186]

Knowing how these departments and agencies use the technology and plan to use it in the future is the second step to achieving full transparency. This second step is arguably more important than the first. If individuals only know what technology is at the police's disposal and not how each police department uses it, it does not allow for proper external oversight. Thus, if police departments or law enforcement agencies use facial recognition technology, they must be transparent with their communities as to how they use the technology. Police departments must disclose whether facial recognition technology is used in cases where individualized suspicion of a person is not required. Moreover, law enforcement agencies and police departments must reveal the different forms of facial recognition technology they use.

Although full transparency as to how police and law enforcement agencies use this technology should be mandatory, it alone does not fully achieve the necessary level of restriction required to limit the potential abuse of this technology.

3. Court Approval

If the legislature is unwilling to place a complete ban on the technology, another safeguard to control the use of facial recognition technology would be to require law enforcement to obtain a court order to use the technology. Such court approval would be similar to obtaining a search warrant. The officers or federal agents requesting to use this technology should be able to articulate why they need to use facial recognition technology and how it would further their investigation of a specific suspect. Moreover, if this technology will be used, there is a need for a magistrate or judicial officer, a clear third-party neutral, to approve or decline the requests made by officers. The rationale behind this proposal is that a neutral judge can better assess the law enforcement priorities balanced against the privacy interest impacted by issuing a warrant.

4. Incentivizing Companies Selling Facial Recognition Technology

Finally, one way Congress can control law enforcement's use of facial recognition technology is by putting guidelines in place and

186. *See generally* SEATTLE, WASH., ORDINANCE 124142 (Mar. 26, 2013).

incentivizing companies to better the technology's accuracy. Legislation can be passed that regulates the technology law enforcement purchases. Such legislation can dictate that the technology must have a specific level of accuracy among individuals of all races. Legislation that mandates a specific level of accuracy in order for police departments to purchase the facial recognition technology will incentivize facial recognition technology companies to enhance their technology's accuracy. Moreover, if legislatures find this technology to be indispensable to policing, they may also provide an R&D tax credit to companies to improve their technology, so it meets their required accuracy standards. However, it is important to note that facial recognition technology's increased accuracy will not make this technology any less harmful to communities who are already over-policed, over-arrested, and over-incarcerated.[187]

V. CONCLUSION

Law enforcement's use of facial recognition technology in the form of face identification, face verification, face surveillance, and face tracking can have and currently are having detrimental effects on our society as we know it. These effects include individuals that are being wrongfully arrested, activists and protesters that are afraid to be identified due to the fear that police will retaliate, and women that may feel uncomfortable to seek care at a reproductive center because they are being watched by police. Not only is this technology's inaccuracy a major issue that can lead to wrongful arrests of people of color, but it also has the ability to transform the United States into a surveillance state. Although facial recognition technology can provide many benefits, the concerns of the technology's racial biases and decreased privacy strongly outweigh the benefits of the technology. While the courts can find the use of some forms of this technology to be unconstitutional, members of Congress have the ability to implement change faster. Our members of Congress need to act, and society must put pressure on government and businesses to stop using facial recognition technology in all its forms.

187. *See* Johana Bhuiyan, *Clearview AI Uses Your Online Photos to Instantly ID You. That's a Problem, Lawsuit Says*, L.A. TIMES (Mar. 9, 2021, 11:02 AM), https://www.latimes.com/business/technology/story/2021-03-09/clearview-ai-lawsuit-privacy-violations [https://perma.cc/566N-DEZL].