Legislating Big Tech: The Effects Amazon Rekognition Technology Has on Privacy Rights

CRYSTAL GODFREY*

INTRODUCTION

Today, privacy faces increased "threats from a growing surveillance apparatus that is often justified in the name of national security."[1] Numerous government agencies were employing Amazon's facial recognition technology ("FRT") to intrude upon the privacy of innocent citizens until June 2020, when Amazon announced a one-year moratorium against police using its FRT.[2] Nearly half of Americans are currently in law enforcement facial recognition networks without their knowledge.[3] Police with body-cameras can identify and save passersby in a facial-recognition database, even though the person may never speak with the police or be a suspect.[4] This kind of technology enables officers to act as sophisticated surveillance mechanisms while unfairly transforming the civilian and officer dynamic.[5]

"The government's collection of sensitive information is itself an invasion of privacy."[6] However, its use of this data, in conjunction with FRT, is "rife with abuse."[7] Historically, FRT disproportionately affects women and people of color and leads to mass surveillance of vulnerable

* Crystal Godfrey earned her Juris Doctorate from the University of San Francisco in 2020. In 2013, Crystal graduated Cum Laude from Oglethorpe University with a Bachelor of Arts Degree in Political Science with a concentration in Urban Leadership. Crystal would like to express her gratitude to Professor Everett Monroe and fellow classmate Shreya Tewari for inspiring this article. Their relentless support, advice, and insight during the writing process were invaluable. Furthermore, she would like to send a very warm thank you to her parents—Arthur and Daveina Godfrey—and close family and friends for their constant encouragement and unconditional love. Lastly, Crystal would like to extend her deepest appreciation to each and every activist, protestor, organizer, and ally of the Black Lives Matter movement. Their actions, calls for change, and expressions of love and justice are moving all of us to a better world.

1. *See Privacy and Surveillance*, AM. C.L. UNION, https://www.aclu.org/issues/national-security/privacy-and-surveillance [https://perma.cc/P53Q-4Y8P].

2. Karen Hao, *The Two-Year Fight to Stop Amazon from Selling Face Recognition to the Police*, MIT TECH. REV. (June 12, 2020), https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/ [https://perma.cc/3JBQ-ED47] (stating the police ban on using Amazon's Rekognition technology will only last for one year, starting June 10, 2020).

3. Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org [https://perma.cc/S9MZ-CB9F].

4. Tom Simonite, *Few Rules Govern Police Use of Facial-Recognition Technology*, WIRED (May 22, 2018, 9:35 PM), https://www.wired.com/story/few-rules-govern-police-use-of-facial-recognition-technology/ [http://perma.cc/8BHJ-4XY3].

5. Patrick Tucker, *Facial Recognition Coming to Police Body Cameras*, DEF. ONE (July 17, 2017), https://www.defenseone.com/technology/2017/07/facial-recognition-coming-police-body-cameras/139472/ [http://perma.cc/QF35-ALKU].

6. *Privacy and Surveillance*, *supra* note 1.

7. *Id.*

communities.[8] Integrating FRT with body-worn cameras presents the probability of chilling free speech in public spaces.[9] While biometric surveillance has become normalized in policing,[10] the legislature must not allow FRT to limit the Fourth, First, and Fifth Amendments' powers.

This paper explores the privacy and policy concerns raised by Amazon's Rekognition's use by law enforcement agencies if Amazon lifts or does not extend the moratorium and its potential impact on the public's privacy expectations. Part I details the history and current state of facial recognition. Part II analyzes how the use of FRT by law enforcement may implicate the Fourth, First, and Fifth Amendments and disproportionately impact women and minorities. Part III then explores the state and federal legislative approaches on how to regulate FRT. Lastly, Part IV concludes with a recommendation for lawmakers regarding the use of FRT by law enforcement.

I. BACKGROUND

A. HISTORY OF FACIAL RECOGNITION TECHNOLOGY

FRT has been in development since the 1960s.[11] Progress remained slow and steady until the arrival of advanced artificial neural networks.[12] These networks are computerized systems that mimic animal brains and can recognize patterns by processing examples.[13] The data from these experiments inevitably prompted programmers to attempt to mimic human intelligence.[14] Like the artificial animal intelligence experiment, programmers feed these neural networks many photos of people's faces and then allow the artificial intelligence ("AI") to take over.[15] Simultaneously, algorithms teach themselves what faces look like and how to tell those faces apart.[16] The system distinguishes between faces by creating a "template" of the target's facial image and then comparing the template to photographs of

8. Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, AM. C.L. UNION (July 26, 2018, 8:00 AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [https://perma.cc/8SDT-6K78].

9. Letter from 18MillionRising.org et al., to Axon AI Ethics Board, Axon Enter., Inc. (Apr. 26, 2018), http://civilrightsdocs.info/pdf/policy/letters/2018/Axon AI Ethics Board Letter FINAL.pdf [http://perma.cc/6YJF-36EC].

10. Gregory Barber & Tom Simonite, *Some US Cities Are Moving into Real-Time Facial Surveillance*, WIRED (May 17, 2019, 7:00 AM), https://www.wired.com/story/some-us-cities-moving-real-time-facial-surveillance/ [https://perma.cc/LD2R-7V5V].

11. Lane Brown, *There Will Be No Turning Back on Facial Recognition*, INTELLIGENCER (Nov. 12, 2019), http://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html [https://perma.cc/DXM9-CPKN].

12. *Id.*

13. *Id.*

14. *Id.*

15. *Id.*

16. *Id.*

preexisting images of a known face or faces.[17] These photographs are found in "drivers' license databases, government identification records, mugshots, or social media accounts, such as Facebook."[18]

Eventually, the algorithms teach themselves how to decide if a face in one photo is the same face in a different photo.[19] The system can identify photographs of people even when a person has "sunglasses or makeup or a mustache" or an image has poor lighting or is blurred.[20] "The more photos an algorithm has to learn from—millions or billions, ideally—the more accurate it becomes."[21]

B. CONTEMPORARY USES FOR FRT

There are two main reasons public and private entities have sought the use of FRT: (1) for identification purposes; and (2) for access, control, or authorization purposes.[22]

1. Identification

Identification is the ability to identify one person from all the biometric patterns that have been recorded.[23] Law enforcement agencies use facial-recognition software to identify criminals and criminal activity after a crime has occurred by taking video surveillance images and using facial recognition software to identify perpetrators.[24] Police forces in Oregon used Rekognition in security surveillance, despite reports of racial disparity.[25] "An inmate was talking to his girlfriend on a jailhouse phone when she [told him] there was a warrant out for her arrest."[26] Oregon police "went to the inmate's Facebook page, found an old video with her singing and ran a facial-recognition search to get her name; officers then arrested her in just a few days.[27] Months later, the same police department used FRT to locate a woman who took an $11.99 tank of welding gas from an Ace Hardware

17. *Id.*

18. Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, A.B.A.: CRIM. JUST. MAG. (2019), https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/ [https://perma.cc/YY55-JRB4].

19. Brown, *supra* note 11.

20. *Id.*

21. *Id.*

22. John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 140 (1997) ("[G]iven the various government agencies involved in evaluating biometric technologies and their many applications, there will likely not be a single dominant technology that emerges. Rather, biometric balkanization will take place; . . . multiple technologies will be deployed. . . .").

23. *Id.*

24. *Id.*

25. Drew Harwell, *Oregon Became a Testing Ground for Amazon's Facial-Recognition Policing. But What if Rekognition Gets It Wrong?*, WASH. POST (Apr. 30, 2019, 2:19 PM), https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/ [https://perma.cc/L66C-Z9WQ].

26. *Id.*

27. *Id.*

store.[28] "Almost overnight, deputies saw their investigative power supercharged" by the Rekognition software.[29] It would traditionally take several days or weeks to identify a person, but, while using FRT, officers could identify suspects within a few days.[30]

2. Access, Control, or Authorization

The second reason entities seek to use FRT is for access, control, or authorization purposes.[31] "Authentication is the ability to verify a person's identity through a comparison with their previously recorded biometric measurements."[32] FRT has proven useful in controlling access and verifying authorization in several different ways. Government agencies can use it to prevent fraud in welfare and other entitlement programs.[33] For example, a state's Department of Motor Vehicles could use the technology to scan databases to ensure that individuals attempting to get a driver's license are who they say they are.[34] This allows FRT users to simultaneously limit access, increase control, and authenticate authorization.

While the results of FRT appear to be idealistic, it is equally naïve and unrealistic to assume that these systems are errorless. Naturally, biased humans write these algorithms. As expected, these biases "seep into the way [programmers] frame the analysis that underlies their code."[35] Programmers train artificial intelligence software using data that is tainted with human biases, which in turn appears in the inferences drawn by the program.[36] "What algorithms are doing is giving [us] a look in the mirror . . . . They reflect the inequalities of our society."[37] The algorithms are thus creating an urgent need for computer scientists to expose biases and remove them. Failing to do so can lead to emotional expression matrices furthering discrimination of protected classes.

C. MODERN "ADVANCEMENTS" TO FRT: EMOTIONAL EXPRESSION IN THE HIREVUE CASE STUDY

Modern FRT has advanced beyond simply determining who a person is; rather these algorithms are now learning to recognize how a person feels.[38]

28. *Id.*

29. *Id.*

30. *Id.*

31. Woodward, *supra* note 22.

32. Christopher S. Milligan, Note, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 S. CAL. INTERDISC. L.J. 295, 306 (1999).

33. *Id.* at 302.

34. *Id.* at 306.

35. Jamie Condliffe, *The Week in Tech: Algorithmic Bias Is Bad. Uncovering It Is Good.*, N.Y. TIMES (Nov. 15, 2019), https://www.nytimes.com/2019/11/15/technology/algorithmic-ai-bias.html [https://perma.cc/NX77-D6KU].

36. *Id.*

37. *Id.*

38. Patricia Nilsson, *How AI Helps Recruiters Track Jobseekers' Emotions*, FIN. TIMES (Feb. 28, 2018), https://www.ft.com/content/e2e85644-05be-11e8-9650-9c0ad2d7c5b5 [https://perma.cc/ YNZ9-NZZN].

Companies like Amazon, IBM, and Microsoft, claim their facial recognition software can detect the emotions of an individual based on their facial expressions.[39] Amazon, for example, boasts that Rekognition can estimate whether a face is expressing happiness, sadness, anger, confusion, disgust, surprise, calmness, or fear.[40] Other companies have gone a step further by using algorithms to decipher personality traits based on emotional expressions.[41] Often these algorithms are used to determine an individual's employability.[42]

The Utah based company HireVue, for example, claims its software can determine a person's personality traits based on the results of the HireVue test, which reports their "competencies and behaviors," including their "willingness to learn," "conscientiousness & responsibility" and "personal stability," the latter of which is defined by how well they can cope with "irritable customers or co-workers."[43] The company compares these results to "high achievers" already employed by HireVue.[44] More specifically, "the system uses candidates' computer or cellphone cameras to analyze their facial movements, word choice, and speaking voice before ranking them against other applicants based on an automatically generated 'employability' score."[45] HireVue claims its system determines a candidate's employability score on various competencies in a manner that is consistent, predictable, and without human bias.[46]

By strictly structuring interviews and their accompanying analyses and creating consistency across all hiring practices, companies can begin to address human biases; however, it is unclear to what extent these systems and algorithms are accountable.[47] "How does HireVue's algorithm assess overweight candidates, those who suffer from depression, non-native English speakers . . . [or] candidates with autism who tend to look at people's mouths and avoid direct eye contact?"[48] In fact, FRT "has already faced

39. Brown, *supra* note 11.

40. Saheli Roy Choudhury, *Amazon Says Its Facial Recognition Can Now Identify Fear*, CNBC (Aug. 14, 2019, 11:58 AM), https://www.cnbc.com/2019/08/14/amazon-says-its-facial-recognition-can-now-identify-fear.html [https://perma.cc/2BQN-VUFD].

41. Drew Harwell, *A Face-Scanning Algorithm Increasingly Decides Whether You Deserve the Job*, WASH. POST (Nov. 6, 2019, 9:21 AM), https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/ [https://perma.cc/7X7W-VS72].

42. Nilsson, *supra* note 38.

43. Harwell, *supra* note 41.

44. *Id.*

45. *Id.*

46. *Id.*

47. Vertigo, *HireVue: A Face-Scanning Algorithm Decides Whether You Deserve the Job*, LEADING WITH PEOPLE ANALYTICS (Apr. 12, 2020), https://digital.hbs.edu/platform-peopleanalytics/submission/hirevue-a-face-scanning-algorithm-decides-whether-you-deserve-the-job/ [https://perma.cc/DBD9-RPR4].

48. Patricia Barnes, *Artificial Intelligence Poses New Threat to Equal Employment Opportunity*, FORBES (Nov. 10, 2019, 1:57 PM), https://www.forbes.com/sites/patriciagbarnes/2019/11/10/artificial-intelligence-poses-new-threat-to-equal-employment-opportunity/?sh=5508038b6488 [https://perma.cc/BN5C-SJV2].

criticism for struggling to properly identify and characterize the faces of people with darker skin, women, and trans and non-binary people, among other minority groups."[49] This discrepancy is only worsened by emotion recognition technology which often misjudges a person's emotions based on their facial expressions and scientifically flawed algorithms.[50] For example, a study conducted at the University of Maryland Business School uncovered that facial recognition software consistently reads Black male faces as angrier than white male faces.[51] The same study also reported AI software reads Black male faces as "more contemptuous when their facial expressions are ambiguous."[52]

Research shows that facial expressions are complex and not always indicative of an individual's emotional state.[53] Some experts have pointed out that, while there is scientific evidence suggesting correlations between facial expressions and emotions, the way people communicate primary emotions varies across cultures and situations.[54] There is no present evidence to determine if AI software can or will be able to detect the intricate nuances between cultural expression and facial movements in the near future. Instead, it appears that the unique proposition of the system, analyzing facial expressions, depends on a false assumption of "universal facial expression."[55] This may in part be due to the belief that certain emotions are "revealed by certain facial-muscle configurations."[56] However, studies covering the production of facial expressions during emotional events indicate a lack of support for this theory,[57] like how smiles do not always signal happiness, but could instead signal submission.[58] Also, studies lack data from remote cultures.[59]

Like most AI software, HireVue's "algorithms are not inherently objective, and reflect the data used to train them and the people that design them."[60] The algorithms "inherit, and even amplify, societal biases,

49. Rebecca Heilweil, *Illinois Says You Should Know if AI Is Grading Your Online Job Interviews*, Vox (Jan. 1, 2020, 9:50 AM), https://www.vox.com/recode/2020/1/1/21043000/artificial-intelligence-job-applications-illinios-video-interivew-act.

50. *Id.*

51. Lauren Rhue, Racial Influence on Automated Perceptions of Emotions (Dec. 17, 2018) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765 [https://perma.cc/TK74-EGFU].

52. *Id.*

53. Brown, *supra* note 11.

54. David Matsumoto & Hyi Sung Hwang, *Reading Facial Expressions of Emotion*, AM. PSYCH. ASS'N (May, 2011), https://www.apa.org/science/about/psa/2011/05/facial-expressions [https://perma.cc/LGA5-MDM2].

55. Vertigo, *supra* note 47.

56. Lisa Feldman Barrett et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements*, 20 PSYCH. SCI. PUB. INT. 1, 1–68 (2019) (discussing emotion categories and facial-muscle movement configurations).

57. *Id.*

58. *Id.*

59. *Id.*

60. Heilweil, *supra* note 49.

including racism and sexism."[61] Also, although algorithms can be "instructed not to consider factors like a person's name, it can still learn proxies for protected identities," like discrimination based on women's versus men's colleges and feminine versus masculine language.[62] Historical data has shown that AI has prefers "candidates who described themselves using verbs more commonly [used by men], such as 'executed' and 'captured.'"[63] For instance, a math and economics senior researched HireVue and tailored her application for the job-interview AI technology.[64] "She answered confidently and in the time allotted. She used positive keywords. She smiled, often and wide."[65] Yet, she did not get the position and was not allowed to see how she was rated nor ask for feedback.[66] "I feel like that's maybe one of the reasons I didn't get it: I spoke a little too naturally," she said.[67] While her score is unknown, it leads many critics to believe that these systems are dehumanizing, invasive, and built on flawed science that could perpetuate discriminatory hiring practices.[68]

In November 2019, the Electronic Privacy Information Center ("EPIC"), a public interest research center based in Washington, D.C., asked the Federal Trade Commission to investigate HireVue's business practices because HireVue's use of unproven artificial intelligence systems that scan people's faces and voices constituted a wide-scale threat to American workers.[69] Specifically, the complaint alleged that HireVue's AI system showed bias against women, minorities, older, and disabled workers based on the differences in emotional expressions.[70] In the FTC filing, EPIC officials alleged that HireVue's AI-driven assessments produced "results that are biased, unprovable and not replicable."[71] It could "score someone based on prejudices related to their gender, race, sexual orientation, or neurological differences."[72] The complaint stated that HireVue did not establish "the accuracy, reliability, or validity of its computer-generated

61. *Id.*

62. *Id.*

63. Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*, REUTERS (Oct. 10, 2018, 4:04 PM), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G [https://perma.cc/S7DH-PR9T].

64. Harwell, *supra* note 41.

65. *Id.*

66. *Id.*

67. *Id.*

68. *Id.*

69. *Id.*

70. *Id.*

71. Complaint and Request for Investigation, Injunction, and Other Relief at 7, ELEC. PRIV. INFO. CTR. (Nov. 6, 2019), https://epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf [https://perma.cc/863J-AHJH].

72. Drew Harwell, *Rights Group Files Federal Complaint Against HireVue, a Hiring Company that Uses Artificial Intelligence*, SEATTLE TIMES (Nov. 6, 2019, 10:56 PM), https://www.seattletimes.com/business/rights-group-files-federal-complaint-against-ai-hiring-firm-hirevue-citing-unfair-and-deceptive-practices/ [https://perma.cc/RJV3-76DB].

scores."[73] Additionally, the complaint said that HireVue never "adequately evaluated whether the purpose, objectives, and benefits of its algorithmic assessments outweigh the risks."[74]

Lastly, FRT algorithms do not consider how much information people convey through their bodies, beyond just facial expressions.[75] People are capable of using their entire bodies to convey emotional information, such as adopting a collapsed posture when depressed or leaning forward to show interest.[76] FRT, on the other hand, focuses primarily on an incredibly small and limited part of this information conveyed through facial expression.[77] Therefore, facial expression does not entirely communicate a person's emotional state. Researchers warn, "It is not possible to confidently infer happiness from a smile, anger from a scowl, or sadness from a frown, as much of current technology tries to do when applying what are mistakenly believed to be scientific facts."[78]

With this in mind, it is possible that companies are not considering the new, unique problems facial expression matrices create through discriminating against underrepresented peoples or, in some cases, are doing very little to alleviate this issue or the slew of other discrimination problems FRT creates; chief among those is Amazon.

D. HOW DOES AMAZON REKOGNITION COMPARE?

Amazon believes its technology is beyond the faults and errors of its competitors. According to the company's site, Amazon Rekognition ("Rekognition") quickly "adds highly accurate image and video analysis to consumer's applications."[79] By uploading an image or video, a customer can request for Rekognition to "identify objects, people, text, scenes, and activities" as well as "any inappropriate content."[80] Some say Rekognition's results are "indistinguishable from magic."[81]

73. *Id.*

74. *Id.*

75. Grace Brennan, *Emotion Analytics Used in AI Recruitment Tools Are Not Only Unethical but Incorrect*, SOCIABLE (Mar. 2, 2020), https://sociable.co/technology/emotion-analytics-ai-recruitment-tools-incorrect/ [https://perma.cc/HG2C-SXUJ].

76. Margaux Lhommet & Stacy C. Marsella, *Expressing Emotion Through Posture and Gesture*, *in* THE OXFORD HANDBOOK OF AFFECTIVE COMPUTING 273–283 (Rafael A. Calvo et al. eds., 2015).

77. Barrett, *supra* note 56.

78. *Id.* at 46.

79. *The Facts on Facial Recognition with Artificial Intelligence*, AMAZON WEB SERVS., https://aws.amazon.com/rekognition/the-facts-on-facial-recognition-with-artificial-intelligence/ [https://perma.cc/X9VY-REPN].

80. Ry Crist, *Amazon's Rekognition Software Lets Cops Track Faces: Here's What You Need to Know*, CNET (Mar. 19, 2019, 5:00 AM), https://www.cnet.com/news/what-is-amazon-rekognition-facial-recognition-software/ [https://perma.cc/H6AY-D5V3].

81. Jeff Barr, *Amazon Rekognition – Image Detection and Recognition Powered by Deep Learning*, AMAZON WEB SERVS. NEWS BLOG (Nov. 30, 2016), https://aws.amazon.com/blogs/aws/amazon-rekognition-image-detection-and-recognition-powered-by-deep-learning/ [https://perma.cc/LDT6-3SM3].

"Rekognition is a developer tool with several functions, including facial recognition, 'pathing' — which involves tracking an object, like a soccer ball, through a video frame — and finding and reading text in images and on video that is hard to see with the naked eye."[82] Customers can use Rekognition for "facial analysis or sentiment analysis, which tags images as showing people who are smiling or frowning to record their projected emotions."[83] Through artificial intelligence, Rekognition learns to determine the faces or objects that are important to each specific customer.[84]

> Like most facial recognition software, Rekognition matches faces based on their visual geometry, including the relationship between the eyes, nose, brow, mouth, and other facial features. When images are analyzed by Amazon Rekognition, there is an outline around the face, called a bounding box, which determines the only part of the image Rekognition considers in its analysis. The analysis then produces object notation numbers for the image that indicate the "location" for the significant elements of the face. When customers are running a face search, the technology [compares] this data from the source image to each of the images it searches. From there, the service assigns each face in the image a similarity score. This approach ensures that Rekognition has no information about the identity of an individual, only the likelihood that one face is a potential match for another.[85]

In response to bias and human error, "Amazon's approach thus far has been one of denial, deflection, and delay."[86] Amazon claims Rekognition is bias-free, despite failing to submit its FRT systems to the National Institute of Standards and Technology ("NIST") for the latest rounds of facial recognition evaluations and after receiving preliminary reports of gender and racial bias.[87] Instead, Amazon reports that the company's internal evaluations prove its technology is not susceptible to bias because its FRT system requires a high confidence threshold.[88]

In theory, facial recognition systems, like Rekognition, require a high-confidence threshold to trigger matches and are likely to produce fewer misidentifications.[89] This means it creates more "false negatives," where Rekognition misses a profile in the database that matches the provided

82. Kate Fazzini, *Amazon's Facial Recognition Service Is Being Used to Scan Mugshots, but It's Also Used to Track Innocuous Things like Soccer Balls*, CNBC (Dec. 6, 2018, 11:13 PM), https://www.cnbc.com/2018/12/06/how-amazon-rekognition-works-and-what-its-used-for.html [https://perma.cc/Z6HF-WKX7].

83. *Id.*

84. *Id.*

85. *The Facts on Facial Recognition with Artificial Intelligence*, *supra* note 79.

86. Joy Buolamwini, *Response: Racial and Gender Bias in Amazon Rekognition—Commercial AI System for Analyzing Faces.*, MEDIUM (Jan. 25, 2019), https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced [https://perma.cc/EA9Q-WF8F].

87. *Id.*

88. *Id.*

89. Jake Laperruque, *About-Face: Examining Amazon's Shifting Story on Facial Recognition Accuracy*, PROJECT ON GOV'T OVERSIGHT (Apr. 10, 2019), https://www.pogo.org/analysis/2019/04/about-face-examining-amazon-shifting-story-on-facial-recognition-accuracy/ [https://perma.cc/RD68-BB7P].

image, and fewer "false positives," where Rekognition misidentifies a profile in the database as a match to the provided image when it is not.[90] On the other hand, systems with a low-confidence threshold give both more identifications and misidentifications.[91] However, "even confidence thresholds at the highest settings can produce misidentifications, especially for women and people of color."[92]

II. AMAZON REKOGNITION SOFTWARE VIOLATES INDIVIDUALS' CONSTITUTIONAL RIGHTS AND TARGETS MINORITIES

A. CONSTITUTIONAL ISSUES

The Constitution of the United States grants certain rights to all people, rights that are being directly impacted by Rekognition. The Fourth Amendment protects citizens from unreasonable searches and seizures.[93] The First Amendment prohibits any law from abridging the freedoms of speech and assembly,[94] and the Fifth Amendment prohibits the deprivation "of life, liberty, or property, without due process of law."[95] The bounds of these protections, as applied to government use of FRT, are untested and unregulated.[96] There are no comprehensive federal statutes to govern the use of FRT in any form, whether by private or public actors.[97] The United States Supreme Court has not directly ruled on the constitutionality of police using FRT but has ruled on using technology to "aggregate data on private citizens."[98] Despite these measures, the law is once again trailing behind the advancements of technology.

1. Fourth Amendment Concerns

The Fourth Amendment prohibits unreasonable searches and seizures.[99] A search is constitutional if it does not violate a person's "reasonable" or "legitimate" expectation of privacy.[100] Over time this expectation has

90. *Id.*

91. *Id.*

92. *Id.*

93. U.S. CONST. amend. IV.

94. U.S. CONST. amend. I.

95. U.S. CONST. amend. V.

96. Memorandum from Majority Staff, House of Representatives, to Members of the Committee on Oversight and Reform (May 20, 2019), https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-20190522-SD002.pdf [https://perma.cc/3SDU-7AND].

97. KELSEY Y. SANTAMARIA, CONG. RSCH. SERV., R46541, FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT: SELECT CONSTITUTIONAL CONSIDERATIONS 2 (2020), https://crsreports.congress.gov/product/pdf/R/R46541 [https://perma.cc/CHE9-5HRF].

98. Memorandum from Majority Staff, *supra* note 96.

99. U.S. CONST. amend. IV.

100. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). *See* United States v. Jones, 565 U.S. 400, 406 (2012) ("Our later cases have applied the analysis of Justice Harlan's concurrence in [*Katz*] said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy.'"); United States v. Jacobsen, 466 U.S. 109, 120 (1984) (explaining that law

changed and, with FRT, it will likely change again. This change began with *Katz*, the famous search and seizure case.

In *Katz v. United States*, the FBI attached a microphone to the inside of a telephone booth that police knew a suspected gambler, Katz, frequently used.[101] By eavesdropping on Katz's phone calls, the FBI confirmed its suspicions and arrested Katz for illegal gambling activities.[102] The issue before the Supreme Court was whether the evidence discovered by eavesdropping on Katz's telephone conversations violated the Fourth Amendment.[103] Through its decision in *Katz*, the United States Supreme Court developed a two-part test for determining whether a person has a "reasonable expectation of privacy," which the government may not violate without a search warrant. The first requirement is that the person must "[exhibit] an actual (subjective) expectation of privacy."[104] The second requirement is that the person's expectation of privacy must be (objectively) reasonable.[105] If both of these requirements are met, then the government may not—as a general rule, there are exceptions—search the person's private space or seize the person's belongings without a warrant.[106] The Court concluded that "the underpinnings of *Olmstead* and *Goldman* [had] been so eroded by [its] subsequent decisions that the 'trespass' doctrine there enunciated [could] no longer be regarded as controlling."[107] Justice Harlan's concurrence in the judgment further afforded citizens additional protection from police uses of technology.[108] Since then, *Katz* has served as the bedrock of Fourth Amendment jurisprudence.

In a later decision, the Supreme Court held that digital aggregation of data could constitute a search, even if individual data points would not have been protected.[109] The Court found that the government placing a GPS device on the undercarriage of a car, which collected locational data for twenty-eight days, comprised a search.[110] Justice Sotomayor, in her concurrence, wrote:

> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, at will, their

enforcement action that does not infringe on a "legitimate expectation of privacy . . . [is] not a 'search' within the meaning of the Fourth Amendment").

101. *Katz*, 389 U.S. at 348.

102. *Id.*

103. *Id.* at 353–54.

104. *Id.* at 361 (Harlan, J., concurring).

105. *Id.*

106. *Id.* at 360–62.

107. *Id.* at 353 (majority opinion).

108. *Id.* at 361 (Harlan, J., concurring).

109. United States v. Jones, 565 U.S. 400, 403–04, 410 (2012).

110. *Id.* at 413 (Sotomayor, J., concurring).

political and religious beliefs, sexual habits, and so on.[111]

In 2018, the Supreme Court, in *Carpenter v. United States*, placed further boundaries on police use of technological surveillance.[112] In *Carpenter*, the Supreme Court ruled on whether a person's expectation of privacy covered the records of historical cell phone data ("historical CSLI"), which revealed the person's physical location or movements.[113] The government charged Timothy Carpenter with aiding and abetting robbery that affected interstate commerce, in violation of the Hobbs Act, using cell site evidence.[114] Carpenter moved to suppress the government's cell-site evidence on Fourth Amendment grounds, arguing that the FBI needed a warrant based on probable cause to obtain the records.[115]

Relying on *Katz*, the *Carpenter* Court held that a person's Fourth Amendment rights were violated when the government received historical CSLI from cell phone companies without first obtaining a search warrant.[116] The Court explained that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CLSI."[117] The Court reasoned that CLSI presents "even greater privacy concerns than the GPS monitoring"[118] considered in *United States v. Jones*[119] because of the constant and near-perfect surveillance that results.[120] "While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time."[121] The Court also considered current technology as well as those that are being developed.[122] It reiterated Justice Frankfurter's warning to tread carefully with new technology to not "embarrass the future."[123] The Court did not provide a bright-line test for determining how far the new protection on privacy in the public extends in future cases.[124]

The *Carpenter* decision is a step forward in privacy rights protection. However, "the most obvious potential expansion of this new protection for privacy in public is something the Supreme Court erred in not addressing as part of the *Carpenter* decision: cellphone tracking in real-time."[125] In

111. *Id.* at 416.
112. Carpenter v. United States, 138 S. Ct. 2206, 2216–17 (2018).
113. *Id.* at 2211, 2216.
114. Hobbs Act, 18 U.S.C. § 1951 (2020); *Carpenter*, 138 S. Ct. at 2212–13.
115. *Carpenter*, 138 S. Ct. at 2206.
116. *Id.*
117. *Id.* at 2217.
118. *Id.* at 2210.
119. United States v. Jones, 565 U.S. 400 (2012).
120. *Carpenter*, 138 S. Ct. at 2218.
121. *Id.*
122. *Id.* at 2218–19.
123. *Id.* at 2220.
124. *See id.*
125. Jake Laperruque, *The Carpenter Decision: A Huge Step Forward for Privacy Rights but Major Problems Remain*, PROJECT ON GOV'T OVERSIGHT (June 28, 2018),

Carpenter, the Court stated its ruling was narrow, thus it would not question whether real-time, ongoing surveillance should also require a warrant.[126] The decision "suggests that an individual's public movements captured by FRT in an isolated incident do not implicate the Fourth Amendment."[127] The legal argument is that an individual does not have a reasonable expectation of privacy when the individual's face is freely exposed to the public. However, this argument does not satisfy the two-prong test created in *Katz*.[128]

> Most people today exhibit subjective and actual expectations of privacy in their identities, even while they are out in public. In walking down the street, we invite "the intruding eye" of strangers to glance at or even examine our faces as we pass by, but we do not invite them to also identify us by our names and addresses, much less occupation, immigration status, criminal history, and other personal information. People do not walk around in public announcing or displaying such identifying information . . . In many places, we expect to be able to take trips to the pharmacy to purchase sensitive items, or private trips to the doctor's office or the therapist's office, or perhaps a quick trip to the grocery store in pajamas, with the minimal risk of being recognized and of being required to identify ourselves in public.[129]

A 2015 Pew Research Center study suggested that, contrary to assertions that people increasingly "do not care" about privacy, Americans value personal information and freedom from surveillance in daily life.[130] The study found that sixty-three percent of participants felt it important to be able to "go around in public without always being identified."[131] The study corroborates the Court's decision in *Carpenter*; "A person does not surrender all Fourth Amendment protection by venturing into the public sphere."[132] With that said, Congress should address the public's opinion and respect that an individual's public movements, viewed using FRT over an extended period, can reveal intimate details about the individual's personal life. The amount of detail FRT gives does equate to a Fourth Amendment search, even though everything takes place in public.[133]

---

https://www.pogo.org/analysis/2018/06/carpenter-decision-huge-step-forward-for-privacy-rights-but-major-problems-remain [https://perma.cc/8T7R-A2E8].

126. *Id.*

127. Hamann & Smith, *supra* note 18.

128. Katz v. United States, 389 U.S. 347 (1967).

129. Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1601–02 (2017). *See* Hiibel v. Sixth Jud. Dist. Ct., 542 U.S. 177 (2004). The Supreme Court held that state law might require a person to identify themselves when the police stop the person as a result of reasonable suspicion that a person may be involved in criminal activity. *Id.*

130. Claire Cain Miller, *Americans Say They Want Privacy, but Act as if They Don't*, N.Y. TIMES (Nov. 12, 2014), https://www.nytimes.com/2014/11/13/upshot/americans-say-they-want-privacy-but-act-as-if-they-dont.html [https://perma.cc/9K5V-SNS8].

131. Mary Madden & Lee Rainie, *Americans' Views About Data Collection and Security*, PEW RSCH. CTR. (May 20, 2015), https://www.pewresearch.org/internet/2015/05/20/americans-views-about-data-collection-and-security/ [https://perma.cc/ E2BU-YSQG].

132. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

133. *See, e.g.*, Riley v. California, 573 U.S. 373 (2014); Jones v. United States, 565 U.S. 400 (2012); United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (concerning surveillance through cell phones or GPS, not specifically stating FRT).

2. First Amendment Concerns

Critics of Rekognition have also argued that FRT software may implicate the First Amendment right to freedom of association.[134] Courts have upheld the right to anonymous speech and association, which protect the ability to advocate effectively for minority positions.[135] Within the context of identification, facial recognition is more threatening to privacy rights than other biometric techniques.[136] In a University of Texas study, respondents most often ranked facial recognition as the biometric technique with which they were least comfortable.[137] The public's mistrust and sensitivity towards surveillance techniques inform legal scholarship, suggesting that the constant surveillance of individuals' activities leads to privacy harms and the "chilling" of social interactions.[138] Social science research demonstrates that—when watched—individuals change their activities, avoiding "experiment[ing] with new, controversial, or deviant ideas."[139]

For instance, scholar Jonathon Penney believes that online surveillance has a chilling effect on individuals' activities.[140] Penney states that, when watched, individuals self-censor and actively abstain from risky activities that would either cause embarrassment or be used for nefarious purposes.[141] Other scholars, such as Julie E. Cohen, Daniel Solove, and Joel Reidenburg, echo Penney's theory on the polarizing effects of technological surveillance. Cohen argues that the chilling effect caused by online surveillance homogenizes social interaction where the "[p]ervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream."[142] Daniel Solove theorizes that continual monitoring deters the individuals' right to freely choose, thus resulting in ubiquitous forms of social control that are anti-democratic.[143]

Lastly, Joel Reidenberg stressed the dangers that can occur when public anonymity is not protected. Reidenberg argues, "anonymity in public is a

134. Snow, *supra* note 8.

135. Hamann & Smith, *supra* note 18. *See* NAACP v. Alabama, 357 U.S. 449, 466 (1958). *See also* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995); Talley v. California, 362 U.S. 60, 64−65 (1960).

136. Mike Elgan, Opinion, *It's Time to Face the Ugly Reality of Face Recognition*, COMPUTERWORLD (Mar. 18, 2017, 4:01 AM), https://www.computerworld.com/article/3182269/its-time-to-face-the-ugly-reality-of-face-recognition.html [https://perma.cc/X3JJ-26QY].

137. RACHEL L. GERMAN & K. SUZANNE BARBER, CTR. FOR IDENTITY, U. of TEX. AT AUSTIN, CONSUMER ATTITUDES ABOUT BIOMETRIC AUTHENTICATION 7 (2018), https://identity.utexas.edu/sites/default/files/2020-09/Consumer%20Attitudes%20About%20Biometrics.pdf [https://perma.cc/Q4JE-MCXN].

138. Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117, 170 (2016).

139. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013).

140. Penney, *supra* note 138.

141. *Id.* at 126–27.

142. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000).

143. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

critical feature for an open society because it protects individuals from stalking and violence, which enables them to hold and advocate unpopular ideas."[144] The possible adverse effect of stifling individual freedom, while more problematic in governmental surveillance, are replicated in part through private sector surveillance.[145] "As a result, facial recognition may frustrate the ability to blend into the 'obscurity' of a crowd by lowering the transaction costs of finding and identifying people and ultimately restricting individuals' expressive and social capacities."[146]

In view of this, Rekognition poses a direct threat to an individual's First Amendment rights based on its invasive features. Unlike other FRT, Rekognition can detect objects, scenes, text, emotions, and even activities protected under the First Amendment, such as protesting and public worship.[147] While some courts have considered law enforcement's use of photography or video at public demonstrations as not violating the First Amendment right to freedom of association,[148] "specific, targeted surveillance of a group may cross the line and violate First Amendment association protections."[149] For example, the District Court in *Raza v. City of New York* determined that the New York Police Department's targeted use of undercover surveillance of Muslim Americans was a violation of the First Amendment.[150] The aggressive surveillance tactics "forced religious leaders to self-censor, limit their religious counseling, and record their sermons, for fear that their statements could be taken out of context by police officers or informants."[151]

Privacy advocates have criticized the widespread use of FRT by law enforcement against protestors.[152] The Baltimore police department has been accused of using FRT to identify and arrest protestors of Freddie Gray's death.[153] Many criticized Baltimore's law enforcement for using FRT

144. Joel R. Reidenberg, *Privacy in Public*, 69 U. MIA. L. REV. 141, 157 (2014).

145. Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1031 (2014) (noting that coercive tendencies of private actors with a profit-maximizing motive are more acceptable than "the dangers that attend tyranny").

146. Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 611, 628 (2019), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1718&context=iplj/ [https://perma.cc/AAQ9-3DFY].

147. Regina Munch, *In Tech We Trust?*, COMMONWEAL (May 9, 2019), https://www.commonwealmagazine.org/tech-we-trust [https://perma.cc/5EK3-RZZU].

148. Donohoe v. Duling, 465 F.2d 196, 202 (4th Cir. 1972).

149. Hamann & Smith, *supra* note 18.

150. Raza v. City of New York, 998 F. Supp. 2d 70, 70 (E.D.N.Y. 2013).

151. Shomial Ahmad, *Historic Settlement on NYPD Spying*, PRO. STAFF CONGRESS CITY U. N.Y.: CLARION (2017), https://psc-cuny.org/clarion/april-2017/historic-settlement-nypd-spying [https://perma.cc/PLD3-WE8M].

152. Hamann & Smith, *supra* note 18.

153. Shirin Ghaffary, *San Francisco's Facial Recognition Technology Ban, Explained*, VOX (May 14, 2019, 7:06 PM), https://www.vox.com/recode/2019/5/14/18623897/san-francisco-facial-recognition-ban-explained [https://perma.cc/T59A-9B44].

surveillance against protestors because of the fear that African Americans were overrepresented in the facial recognition repository.[154]

3. Due Process Concerns

Perhaps the constitutional right most vulnerable to the adverse effects of FRT is the right to due process, specifically, the unenumerated right for a defendant to receive exculpatory evidence. In a recent decision, a Florida state appellate court held that Willie Allen Lynch, a Black male convicted for selling crack cocaine to two undercover officers, had no right to view photos of other suspects identified by the facial recognition search that led to his arrest.[155] At trial, Lynch maintained that the State misidentified him.[156] Lynch contended that the facial recognition algorithm used by the analyst also gave the photos of other men, who could have been responsible for the crime.[157] Those other photos would have cast doubt on the State's case and, by not providing those photos, the State violated *Brady* requirements.[158] However, both the trial and the appellate courts rejected this argument, believing the State did not have an obligation to disclose the photos of the other suspects to Lynch.[159]

This dispute about the government's duty to disclose such evidence is in actuality a dispute about the scope of *Brady* and its relationship to FRT. In Lynch's case, the error-prone facial recognition program's results should have been characterized as both favorable and material within *Brady's* definition. The American Civil Liberties Union ("ACLU") wrote a friend-of-the-court brief to the Florida Supreme Court supporting Lynch's argument that the State violated his due process.[160] In their brief, the ACLU compared the output of facial recognition software to eyewitness identification.[161] "If [the facial recognition algorithm] were a human witness who expressed a low level of confidence in his or her eyewitness identification, or admitted to a mistake in that identification, those facts

154. Kevin Rector & Alison Knezevich, *Maryland's Use of Facial Recognition Software Questioned by Researchers, Civil Liberties Advocates*, BALT. SUN (Oct. 18, 2016, 12:01 AM), https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html [https://perma.cc/2EPU-PS9N].

155. Somil Trivedi & Nathan Freed Wessler, *Florida Is Using Facial Recognition to Convict People Without Giving Them a Chance to Challenge the Tech*, AM. C.L. UNION (Mar. 12, 2019, 5:15 PM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/florida-using-facial-recognition-convict-people [https://perma.cc/8N5H-SJRM].

156. *Id.*

157. *Id.*

158. *Id. See generally* Brady v. Maryland, 373 U.S. 83 (1963) (ruling the prosecution in a criminal case must hand over exculpatory evidence, evidence that is favorable and material to the defense, to the defendant along with other evidence during discovery).

159. Brief for American Civil Liberties Union et al. as Amici Curiae Supporting Petitioner at 14, Lynch v. Florida, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018) (No. 1D16-3290), https://efactssc-public.flcourts.org/casedocuments/2019/298/2019-298_notice_86166_notice2dappendix2fattachment20to20notice.pdf [https://perma.cc/QBJ6-9B7N].

160. *Id.*

161. *Id.*

would be *Brady* material."[162] The ACLU added that this same principle should have allowed Lynch to review information about the facial recognition algorithm used by the Florida police.[163] This information, including "the algorithm's underlying model; training data; source code; operating manual and other explanatory documentation; any other results from which the final, reported result was chosen; and any validation studies," is required to interpret "how uncertain a [low] rating is, what physical attribute-matches might have resulted in that rating, why the algorithm listed Mr. Lynch first, and why the analyst chose Mr. Lynch's photo over other photos returned as matches."[164]

This holding highlights the ambiguities and uncertainty around FRT and its role in the legal system.[165] Privacy and civil liberties advocates have already criticized how little restraint officers meet when using facial recognition software.[166] Now the dangers associated with FRT have seeped their way into prosecutorial conduct and could potentially limit criminal defendants.[167] Without judicial oversight, prosecutors can commit *Brady* violations with the help of the judicial system.

In 2013, Chief Judge Alex Kozinski of the Ninth Circuit summarized the *Brady* violation problem in his dissent in *United States v. Olsen*.[168] Chief Kozinski stated, "There is an epidemic of *Brady* violations abroad in the land. Only judges can put a stop to it."[169] He concluded that the judiciary is the only body that can systematically remedy prosecutorial misconduct.[170] Nevertheless, while he champions for an active judicial role as the solution, he also calls out the role the judiciary has played in allowing misconduct to run rampant. He concludes that, because courts do not force prosecutors to comply with *Brady*, prosecutors simply do not care about *Brady* violations.[171] Chief Judge Kozinski proposes that judges "send prosecutors a clear message: Betray *Brady*, give short shrift to *Giglio* [and] you will lose your ill-gotten conviction."[172] This is precisely how the judicial system should treat FRT evidence, ensuring the integrity of the criminal justice system by guiding what information is due to defendants under *Brady* and related rules.

162. *Id.*

163. *Id.* at 15.

164. *Id.*

165. Ben Conarck, *Florida Court: Prosecutors Had no Obligation to Turn Over Facial Recognition Evidence*, JACKSONVILLE.COM: FLA. TIMES-UNION (Jan. 23, 2019, 9:06 PM), https://www.jacksonville.com/news/20190123/florida-court-prosecutors-had-no-obligation-to-turn-over-facial-recognition-evidence [https://perma.cc/6VXL-GK48].

166. *Id.*

167. *See id.*

168. United States v. Olsen, 737 F.3d 625, 627–33 (9th Cir. 2013) (Kozinski, C.J., dissenting).

169. *Id.* at 626.

170. *Id.*

171. *Id.* at 631.

172. *Id.* at 633.

B. AMAZON REKOGNITION SOFTWARE CAN BE USED BY LAW ENFORCEMENT TO DISCRIMINATE, TARGET, AND RACIALLY PROFILE AFRICAN AMERICANS

The government, the courts, and the public are ill-equipped to deal with the dangers of allowing law enforcement to use FRT in their investigation process. The potential for officers to abuse FRT is inevitable.[173] Because officers can rely so heavily on technology, an officer "may make misinformed decisions about whether to pull [someone] over . . . to make an arrest . . . and potentially even about whether to use lethal force. That can be a life and death consequence because of a failed, inaccurate technology."[174] The reality of these consequences frequently occur in the African American community where African Americans are already disproportionately harmed by police practices.[175] Black men are at the highest risk, with "about a 1 in 1,000 chance of being killed by police," which is "2.5 times more likely" than white men.[176] Additionally, Black people who were fatally shot by police were twice as likely as white people to be unarmed.[177] Based on these statistics and the inherent bias associated with FRT, it is easy to see how Rekognition could exacerbate that problem.[178] A recent incident in New York provides a troubling illustration of that risk. A young Black teenager was handcuffed and forced to leave his family home at four in the morning by the New York Police Department because Apples' facial recognition system falsely connected him to a series of store thefts.[179] The traumatic arrest led the once excellent student to miss classes and to experience severe anxiety and fear.[180]

173. Hiawatha Bray, *Mistaken ID: Facial-Recognition Tool Falsely Matches Famous Athletes to Police Mugshots*, BOS. GLOBE (Oct. 21, 2019, 4:35 PM), https://www.bostonglobe.com/business/2019/10/21/athletes-outlaws-the-software-not-sure/lCwfZSCyzlymLzX3NCwasK/story.html [https://perma.cc/EF97-BSEU].

174. Patt Morrison, Opinion, *Column: Facial ID Recognition Can Help on Your Phone, but Not So Much in Law Enforcement Hands*, L.A. TIMES (Oct. 30, 2019, 2:00 AM), https://www.latimes.com/opinion/story/2019-10-30/matt-cagle-aclu-facial-id-recognition-hong-kong.

175. *See, e.g.*, NAT'L ACAD. OF SCI. ENG'G & MED. ET AL., PROACTIVE POLICING: EFFECTS ON CRIME AND COMMUNITIES 251–01 (David Weisburd & Malay K. Majmundar eds., 2018). *See also* Andrew C. Gray & Karen F. Parker, *Race and Police Killings: Examining the Links Between Racial Threat and Police Shootings of Black Americans*, 18(4) J. ETHNICITY CRIM. JUST. 315, 315–40 (2020).

176. Frank Edwards, Hedwig Lee & Michael Esposito, *Risk of Being Killed by Police Use of Force in the United States by Age, Race—Ethnicity, and Sex*, 116 PROC. NAT'L ACAD. SCI. U.S. 16793, 16793–98 (2019).

177. Justin Nix, Bradley A. Campbell, Edward H. Byers, & Geoffrey P. Alpert, *Bird's Eye View of Civilians Killed by Police in 2015*, 16 CRIMINOLOGY & PUB. POL'Y 309, 325–26 (2017).

178. *See* Maggie Fox, *Police Killings Hit People of Color Hardest, Study Finds*, NBC NEWS (May 8, 2018, 5:00 AM), https://www.nbcnews.com/health/health-news/police-killings-hit-people-color-hardest-study-finds-n872086 [https://perma.cc/KD3D-9C7A].

179. Aaron Mak, *What's Going On with the Teenager Suing Apple Over Facial Recognition Technology?*, SLATE (Apr. 23, 2019, 3:10 PM), https://slate.com/technology/2019/04/a-teenager-is-accusing-apple-of-misidentifying-him-with-a-facial-id-system.html [https://perma.cc/WD8W-HFYT].

180. Complaint at 9–10, Bah v. Apple, Inc., No. 19-cv-3539, 2020 U.S. Dist. LEXIS 143824 (S.D.N.Y. Aug. 11, 2020).

Incidents such as this do not come as a surprise given the history of FRT. FRT is more prone to error when identifying Black faces.[181] "Algorithms used in new technology may appear unbiased at first, but according to researchers, [t]he deeper we dig, the more remnants of bias we will find in our technology."[182] While Amazon refuses to acknowledge any record of bias in its software, the company cannot continue to hide behind the false assumption of machine neutrality, especially when lives are at stake.

In 2018, the ACLU tested the accuracy of Rekognition software.[183] With Rekognition, researchers created a mugshot database from arrest photos that are available to the public.[184] Once completed, photos of Congress members were then run through the database.[185] Researchers used the default settings Amazon created for its Rekognition software.[186] "The software incorrectly matched 28 members of Congress, identifying them as other people who have been arrested for a crime."[187] These false matches of Congresspeople included members along both sides of the political aisle, "men and women, and legislators of all ages," but "were disproportionately people of color, including six members of the Congressional Black Caucus."[188] This alone should convince Congress to ban the use of face recognition software by police.[189]

In response, Amazon criticized the ACLU's application of its software, claiming the ACLU set their confidence threshold too low, which resulted in the high error rate.[190] "When using facial recognition for law enforcement activities," an Amazon spokesperson told Buzzfeed News, "*we guide customers* to set a higher threshold of at least 95% or higher."[191] Amazon further criticized the ACLU's test in its company blog post, saying, "We continue to recommend that customers do not use less than 99% confidence

181. Matt O'brien, *Face Recognition Researcher Fights Amazon Over Biased AI*, AKRON BEACON J. (Apr. 3, 2019, 4:20 PM), https://www.beaconjournal.com/ZZ/news/20190403/face-recognition-researcher-fights-amazon-over-biased-ai?template=ampart [https://perma.cc/GW85-BU4K].

182. Katelyn Ringrose, Note, *Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns*, 105 VA. L. REV. 57, 62 (2019).

183. Snow, *supra* note 8.

184. *Id.*

185. *Id.*

186. *Id.*

187. *Id.*

188. *Id.*

189. *Id.*

190. *See* Matt Wood, *Thoughts on Machine Learning Accuracy*, AMAZON WEB SERVS. NEWS BLOG (July 27, 2018), https://aws.amazon.com/blogs/aws/thoughts-on-machine-learning-accuracy/ [https://perma.cc/6XNM-2V7E].

191. Davey Alba, *Amazon Rekognition Falsely Matched 28 Members of Congress with Arrest Mugshots*, BUZZFEED NEWS (July 26, 2018, 2:32 PM),

https://www.buzzfeednews.com/article/daveyalba/amazon-rekognition-facial-recognition-congress-false [https://perma.cc/E5J2-U9CA].

levels for law enforcement matches."[192] The company recommended human review for any match the system provides.[193]

Nonetheless, criticism of Rekognition did not end there. In 2019, a study from researchers at the Massachusetts's Institute of Technology's ("MIT") Media Lab found:

> Rekognition[] had much more difficulty in telling the gender of female faces and of darker-skinned faces in photos than similar services from IBM and Microsoft. . . .Rekognition made no errors in recognizing the gender of lighter-skinned men. But, it misclassified women as men 19 percent of the time . . . and mistook darker-skinned women for men 31 percent of the time. Microsoft's technology mistook darker-skinned women for men just 1.5 percent of the time.[194]

Once again, Amazon rejected the MIT critique of its software.[195] In another company blog post, Amazon criticized the MIT study, reiterating that "when using facial recognition to identify persons of interest in an investigation, law enforcement should use our recommended 99 percent confidence threshold."[196] This suggests that Amazon believes using the recommended confidence threshold would make misidentification unlikely.

However, a Gizmodo report revealed:

> an Amazon police client was using the company's facial recognition system below the recommended 99 percent confidence thresholds—and that Amazon had worked with the client to design use-practices for the system. Further, the police department did not have any minimum confidence threshold to trigger individuals being displayed as potential matches—increasing the likelihood of misidentification—which could potentially lead to police action based on false identifications. The system was set to return the top five potential matches, regardless of how low the confidence thresholds for these possible matches were. Notably, the system presented these low-confidence-threshold matches to the police to identify persons of interest in cold-case investigations, just two days after Amazon said police "using facial recognition to identify persons of interest in an investigation" should be required to use a 99 percent threshold.[197]

Amazon Web Services' general manager of artificial intelligence responded on Twitter to the news report by defending the police department's use of low confidence thresholds, arguing "every lead is reviewed, and the investigation is 100% human driven."[198] This argument

192. Wood, *supra* note 190.

193. Alba, *supra* note 191.

194. Natasha Singer, *Amazon Is Pushing Facial Technology that a Study Says Could Be Biased*, N.Y. TIMES (Jan. 24, 2019), https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html [https://perma.cc/7TNP-5NJW].

195. *See* Wood, *supra* note 190.

196. *Id.*

197. Laperruque, *supra* note 89. *See* Bryan Menegus, *Defense of Amazon's Face Recognition Tool Undermined by Its Only Known Police Client*, GIZMODO (Jan. 31, 2019, 4:55 PM), https://gizmodo.com/defense-of-amazons-face-recognition-tool-undermined-by-1832238149 [https://perma.cc/8FVG-XYPE].

198. Matt Wood (@mza), TWITTER (Jan. 31, 2019, 4:50 PM), https://twitter.com/mza/status/1091136552195973120 [https://perma.cc/XJ4C-PSS2].

was an obvious about-face from Amazon's earlier blog.[199] A few days later, the company contradicted itself again by returning to the 99% confidence threshold," for identification, or in a way that could threaten civil liberties" when used by law enforcement.[200] Additionally, Amazon claimed the ACLU and MIT "'refused to make their training data and testing parameters publicly available'—though the methodology for the MIT study had been publicly available since 2008."[201]

Before the moratorium, Amazon adamantly encouraged law enforcement to adopt their Rekognition software into investigation practices without regard or concern of racial bias, so Congress must take conscious and deliberate steps in protecting its citizens in the likelihood that Amazon will continue these practices after the moratorium is lifted. These automated systems show their coders' "priorities, preferences, and prejudices."[202] Their "coded gaze" can lead to higher imprisonment and lethal consequences for the African American community.[203]

III. THE NEED FOR LEGISLATIVE REGULATION

A. STATE LEGISLATION

There is some movement towards regulating FRT in the states.[204] Across the United States, states have followed differing strategies in addressing the issues of biometric surveillance. Connecticut, Iowa, Nebraska, North Carolina, Oregon, Wisconsin, and Wyoming have included biometric information in their statutory definitions of "personal information" in their data security laws.[205] Other states, including New York, Connecticut, and Alaska, have proposed legislation seeking to regulate biometric data collection, but the proposals have failed in each respective legislature so far.[206]

There are three states that have passed legislation that specifically regulates biometric information privacy.[207] In 2007, Texas enacted a statute governing biometric information: the Capture or Use of Biometric Identifier

199. Laperruque, *supra* note 89.

200. *Id.*

201. *Id.*

202. *See generally* Joy Buolamwini, *Fighting the "Coded Gaze"*, FORD FOUND. (June 26, 2018), https://www.fordfoundation.org/just-matters/just-matters/posts/fighting-the-coded-gaze/ [https://perma.cc/WR4X-JKYW].

203. *Id.*

204. SANTAMARIA, *supra* note 97.

205. *See* Hannah Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information*, 66 U. KAN. L. REV. 637, 648 (2018).

206. Kathryn E. Deal, Justin O. Kay & Meredith C. Slawe, *Four More States Propose Biometrics Legislation*, FAEGRE DRINKER (Feb. 14, 2017), https://www.faegredrinker.com/en/insights/publications/2017/2/four-more-states-propose-biometrics-legislation [https://perma.cc/JP6E-Y2M6]. *See also* Assemb. A9793, 2017–18 Leg. Sess. (N.Y. 2018). This bill replicates the language of the Illinois BIPA. Deal, Kay & Slawe, *supra*.

207. Zimmerman, *supra* note 205.

("CUBI").[208] CUBI permits collection of biometrics for a commercial purpose based on informed consent and for the sale or disclosure of biometric data under limited circumstances.[209] However, CUBI does not explicitly regulate law enforcement's use of biometric data collection or permit consumers to launch a private action against companies.[210] In 2017, Washington enacted legislation applicable to biometrics.[211] The Washington law provides a broad definition of biometric identifiers, including any "data generated by automatic measurements of an individual's biological characteristics . . . that is used to identify a specific individual."[212] Similar to the Texas statute, companies are required to provide notice of collection for a commercial purpose and obtain consent.[213] Nevertheless, the regulation of private consumption of biometric data inevitably crossed over to the public sector. The first city to ban governmental facial recognition technology was San Francisco, including the ban in an anti-surveillance ordinance approved in 2019 that "requires city agencies to get city approval before purchasing other kinds of surveillance technologies, such as automatic license plate readers and camera-enabled drones."[214] The process requires a public hearing and disclosures about the proposed uses, and even requires disclosure if such technology is already being used.[215] The agencies regulated include the police department, which has not used FRT beyond a test from 2013 to 2017.[216]

San Francisco has always led legislation, from "topics like legalizing gay marriage and setting a higher minimum wage."[217] So it comes as no surprise that San Francisco is once again taking the lead by banning the use of surveillance technology. Most importantly, this ban could easily lead other local governments to enact bans of their own.[218] Matt Cagle, an attorney in the ACLU, nicely sums the potential effect of the ban: "When San Francisco, which is the center of innovation, sounds the alarm bell and takes facial recognition off the table for government use, that's something we should listen to."[219] However, the ban does not affect federal operations

208. TEX. BUS. & COM. CODE ANN. § 503.001 (West 2019).

209. *Id.*

210. Zimmerman, *supra* note 205.

211. WASH. REV. CODE § 19.375.010 (2020).

212. *Id.*

213. WASH. REV. CODE § 19.375.020 (2020).

214. Ghaffary, *supra* note 153; Rachel Metz, *San Francisco Just Banned Facial-Recognition Technology*, CNN BUS. (May 14, 2019, 7:15 PM), https://www.cnn.com/2019/05/14/tech/san-francisco-facial-recognition-ban/index.html [https://perma.cc/U6AP-VKHL].

215. Metz, *supra* note 214.

216. *Id.*

217. Shirin Ghaffary, *How Facial Recognition Became the Most Feared Technology in the US*, VOX (Aug. 9, 2019, 4:00 PM), https://www.vox.com/recode/2019/8/9/20799022/facial-recognition-law [https://perma.cc/8LXA-PC7L].

218. Metz, *supra* note 214.

219. Ghaffary, *supra* note 153.

in San Francisco nor private use by businesses or citizens, or even police confiscation of those private videos.[220]

B. NATIONAL RESPONSE

Unlike many other areas, FRT is a legal issue that cuts across party lines. Following the lead of local politicians in San Francisco and Oakland, California, and Somerville, Massachusetts, Congress held two oversight hearings in November of 2019, triggering the start of at least four federal legislations.[221] Representatives Elijah Cummings (D-MD) and Jim Jordan (R-OH), drafted a bipartisan bill to stop federal purchases of new FRT.[222] However, the bill did not pass, in part due to the untimely death of Cummings in October of 2019.[223]

Nonetheless, Congress continued its pursuit to regulate FRT. Senators Christopher Coons (D-Del.) and Mike Lee (R-Utah) introduced the Facial Recognition Technology Warrant Act in November of 2019.[224] The act would "require that law enforcement obtain court orders to use facial recognition software for extended surveillance as a balanced first step amid local pushes to suspend the technology entirely," which would prevent police from using FRT for innocuous purposes like catching terrorists and locating people with dementia.[225] This would prevent warrants from stretching any longer than thirty days, minimize data collection, and require notice to the Administrative Office of the U.S. Courts for archiving.[226] Senator Coons argued that "[t]he United States . . . has long had to strike a balance between civil liberties and public safety," so the United States must "understand the real costs that come with these increases and advances in technology today."[227]

Critics, including civil rights groups, have "pointed to carveouts in the legislation, specifically one which allows for 'exigent circumstances' where a court order would not be needed to make use of the technology."[228] The ambiguity of exigent circumstances extends law enforcement the opportunity to exploit circumstances to use the technology without a warrant. Opponents of the bill also continue to stress that FRT "exacerbates racial discrimination because of a tendency to be inaccurate, especially for people

220. Metz, *supra* note 214.

221. Ghaffary, supra note 217.

222. Ghaffary, *supra* note 153.

223. Khari Johnson, *Congress Moves Toward Facial Recognition Regulation*, VENTUREBEAT (Jan. 15, 2020, 11:27 AM), https://venturebeat.com/2020/01/15/congress-moves-toward-facial-recognition-regulation/ [https://perma.cc/WR2F-BXZ7].

224. Facial Recognition Technology Warrant Act of 2019, S. 2878, 116th Cong. (2019).

225. Chris Mills Rodrigo, *Senators Defend Bipartisan Bill on Facial Recognition as Cities Crack Down*, HILL (Dec. 5, 2019, 12:55 PM), https://thehill.com/policy/technology/473222-senators-defend-bipartisan-bill-on-facial-recognition-as-cities-crack-down [https://perma.cc/ZT93-V3X3].

226. *Id.*

227. *Id.*

228. *Id.*

of color,"[229] which would mean that any allowance by the law should be unconstitutional.

Yet, Senator Coons and Senator Lee believe the bill is a good first step, "striking a balance between outright moratoriums on the technology and unlimited law enforcement access."[230] Other lawmakers are still deliberating over how regulations against FRT should apply.[231] "France and India are creating national facial recognition databases, while China leans toward uninhibited, dystopian deployment in public spaces such as subways and crosswalks."[232] The European Union also plans to roll out regulations on biometrics, including FRT, in April of 2021.[233]

IV. RECOMMENDATIONS

Perhaps the most logical solution for protecting individuals' privacy rights from FRT software is for every face recognition company, including Amazon, to permanently stop selling the technology to law enforcement agencies and private entities. As mentioned previously, studies conducted by ACLU and MIT researchers highlighted the bias facial recognition has towards African Americans and women.[234] MIT researchers noted that "darker-skinned faces are underrepresented in the datasets used to train [FRT], leaving facial recognition more inaccurate when looking at dark faces."[235] These algorithms "miscategorized dark-skinned women as men up to 34.7 percent of the time."[236] The maximum error rate for light-skinned males, on the other hand, was less than one percent.[237]

Microsoft's gender classifier had a 20.8% error rate for dark-skinned women.[238] To address this, Microsoft "announced it was recalibrating the training data through diversifying skin tones in facial training images, applauding itself for balancing the racial discrepancies in gender classification rates."[239] However, this only speaks to one kind of bias in facial recognition and does not entirely resolve the issue. Even if more images of

229. *Id.*

230. *Id.*

231. Khari Johnson, *Facial Recognition Regulation Is Surprisingly Bipartisan*, VENTUREBEAT (Nov. 11, 2019, 5:08 AM), https://venturebeat.com/2019/11/11/facial-recognition-regulation-is-surprisingly-bipartisan/ [https://perma.cc/CYD6-ZDMG].

232. *Id.*

233. Ella Jakubowska, Opinion, *Mass Facial Recognition Is the Apparatus of Police States and Must Be Regulated*, EURONEWS (Feb. 17, 2021), https://www.euronews.com/2021/02/17/mass-facial-recognition-is-the-apparatus-of-police-states-and-must-be-regulated [https://perma.cc/6744-D2MW].

234. *See supra* Part II.B.

235. Sidney Fussell, *Can We Make Non-Racist Face Recognition?*, GIZMODO (July 25, 2018, 4:55 PM), https://gizmodo.com/can-we-make-non-racist-face-recognition-1827639249 [https://perma.cc/FP58-NHWZ].

236. *Id.*

237. *Id.*

238. Erin Corbett & Jonathan Vanian, *Microsoft Improves Biased Facial Recognition Technology*, FORTUNE (June 27, 2018, 10:32 AM), https://fortune.com/2018/06/27/microsoft-biased-facial-recognition/ [https://perma.cc/6TPN-L9JW].

239. Fussell, *supra* note 235.

people of color or women were incorporated into the database that FRT is trained on, it is still impossible to escape the inherent bias of coders.

Furthermore, local cities are creating "smart city" infrastructure, through such new technologies as "5G connectivity, which will put more local government functions online and increase data collection," facilitating facial recognition.[240] This type of infrastructure also opens the door to other new or future ways of tracking people, including other biometrics, "smart pavement" that "track movement based on a person's gait," and lasers that can track people by their heartbeat, even if FRT is banned.[241] Thus, the best solution to protect an individual's privacy rights is to ban the use of FRT and similar software permanently and altogether from the government and private sector, which will fully protect citizens from government abuses.

240. *Id.*

241. *Id.*