Minnesota Journal of Law & Inequality

Volume 39 | Issue 1 Article 8

February 2021

Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for an Adaptive Legal Framework

Peter N.K. Schuetz
University of Minnesota Law School

Recommended Citation
Peter N. Schuetz, *Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for an Adaptive Legal Framework*, 39(1) LAW & INEQ. (2021).
DOI: https://doi.org/10.24926/25730037.391
Available at: https://scholarship.law.umn.edu/lawineq/vol39/iss1/8

Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for an Adaptive Legal Framework

By: Peter N.K. Schuetz†

Table of Contents

†. J.D. Candidate 2021, University of Minnesota Law School; B.A. Psychology & Legal Studies 2017, University of Wisconsin-Madison. The author would like to thank Prof. Jane Anne Murray for her guidance and support, as well as the staff and editors of the Minnesota Journal of Law & Inequality for their dedication in preparing this article for publication. Finally, the author would like to thank his friends and family for putting up with his tendency to spontaneously write ideas on napkins.

In July 2018, the American Civil Liberties Union (ACLU) ran a sample of photos depicting members of the 115th United States Congress through Amazon's "Rekognition" software,[1] a software designed to provide "highly accurate facial analysis, face comparison, and face search capabilities," among other services.[2] The ACLU compared the congressional members' photos to a database of 25,000 publicly available arrest photos.[3] Despite none of the congressional members actually being depicted in the arrest photo database, Amazon's Rekognition software found twenty-eight matches between the congressional members' photos and the mugshots in the database.[4] Upon human examination, it was clear these twenty-eight matches were caused by mistakes in the Rekognition software.[5] Frighteningly, the twenty-eight mismatches were disproportionally people of color.[6] Despite attaining some of the most honorable positions in the nation, these Congressional Members were confused with criminals.[7]

In recent years, Facial Recognition Technology (FRT), like Amazon's Rekognition, has become increasingly popular in a variety of industries.[8] FRT is revolutionizing many activities that require a form of identification or verification.[9] For example, FRT is

1. Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [perma.cc/PL69-FWQL].

2. *What is Amazon Rekogniton?*, AMAZON, https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html [perma.cc/WHQ4-R55R].

3. Snow, *supra* note 1.

4. *Id.*

5. *Id.*

6. *Id.* ("Nearly 40 percent of Rekognition's false matches in our test were of people of color, even though they make up only 20 percent of [the 115th United States] Congress.").

7. *Id.*

8. *See Facial Recognition: Top 7 Trends (Tech, Vendors, Markets, Use Cases, and Latest News)*, THALES (Sept. 12, 2020), https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition [perma.cc/89ME-RW34].

9. *See, e.g.*, Sintia Radu, *The Technology That's Turning Heads*, U.S. NEWS (July 26, 2019), https://www.usnews.com/news/best-countries/articles/

now a crucial part of how social media companies identify users in photos, how people unlock their phones, and how plane passengers check in to their flight.[10] The recent proliferation of FRT is due to a major boom in artificial intelligence and, specifically, machine learning.[11] Although the increased use of this novel technology may seem exciting and convenient, machine learning systems have been found to harbor forms of bias that can maintain and often increase inequalities.[12] FRT is no exception to this frightening trend of "algorithmic bias," which is defined as systematic errors in a computer program that lead to unfair outcomes.[13] FRT manifests bias through a substantially better identification rate for faces with lighter skin and faces that exhibit traditionally-male facial features than faces with darker skin and faces that exhibit traditionally-female facial features.[14]

FRT's algorithmic bias can be an offensive annoyance when it mistakenly tags people of color as other people[15] or categorizes people of color as inhuman species,[16] but these algorithmic mistakes

---

2019-07-26/growing-number-of-countries-employing-facial-recognition-technology [https://perma.cc/N9QZ-2CNA].

10. *Id.*

11. Nick Statt, *The AI Boom Is Happening All Over the World, and It's Accelerating Quickly*, VERGE (Dec. 12, 2018), https://www.theverge.com/2018/12/12/18136929/artificial-intelligence-ai-index-report-2018-machine-learning-global-progress-research [perma.cc/M2XW-2FQ7].

12. CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION 3 (2016) ("The math-powered applications powering the data economy were based on choices made by fallible human beings. Some of these choices were no doubt made with the best intentions. Nevertheless, many of these models encoded human prejudice, misunderstanding, and bias into the software systems that increasingly managed our lives. Like gods, these mathematical models were opaque, their working invisible to all but the highest priests in their domain: mathematicians and computer scientists. Their verdicts, even when wrong or harmful, were beyond dispute or appeal. And they tend to punish the poor and the oppressed in our society, while making the rich richer.").

13. *See* Nicol Turner Lee, Paul Resnick & Genie Barton, *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms*, BROOKINGS INST. (May 22, 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/ [https://perma.cc/97L9-F2YS].

14. Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classifications*, 81 PROC. MACH. LEARNING RESCH. 71, 88 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf [perma.cc/D24E-9JK6].

15. *See* TED, *How I'm Fighting Bias in Algorithms | Joy Buolamwini*, YOUTUBE (Mar. 29, 2017), https://www.youtube.com/watch?v=UG_X_7g63rY [perma.cc/SGC2-X3L3].

16. For example, in 2015:

> Google came under fire this week after its new Photos app categorized

become a matter of life and liberty when considering law enforcement agencies' increased reliance on FRT in identifying suspects.[17] FRT's utility for law enforcement is undeniable.[18] With FRT, law enforcement can cross-reference camera footage showing a criminal suspect with their database of mugshots and other possible photo databases to identify the suspect.[19] However, law enforcement's increased use of FRT, combined with FRT's demonstrated algorithmic bias, may lead to a stream of disproportionate misidentifications that are deemed correct due to the perception that FRT is "objective."[20] Due to the potential

---

> photos in one of the most racist ways possible. On June 28th, computer programmer Jacky Alciné found that the feature kept tagging pictures of him and his girlfriend as "gorillas."
>
> . . . .
>
> . . . Nikon and other consumer camera companies have also had a history of showing bias to white faces with their facial recognition software. Zunger says that Google has had similar issues with facial recognition due to inadequate analysis of skin tones and lighting.

Loren Grush, *Google Engineer Apologizes After Photos App Tags Two Black People as Gorillas*, VERGE (July 1, 2015), https://www.theverge.com/2015/7/1/8880363/google-apologizes-photos-app-tags-two-black-people-gorillas [perma.cc/MQD3-2ZEQ].

17. FRT adds an additional layer where discrimination can occur in law enforcement:

> [A] demographic group that is underrepresented in benchmark datasets can nonetheless be subjected to frequent targeting. . . . False positives and unwarranted searches pose a threat to civil liberties. Some face recognition systems have been shown to misidentify people of color, women, and young people at high rates (Klare et al., 2012). Monitoring phenotypic and demographic accuracy of these systems as well as their use is necessary to protect citizens' rights and keep vendors and law enforcement accountable to the public.

Buolamwini & Gebru, *supra* note 14, at 2; *see also* CLARE GARVIE, ALVARO M. BEDOYA & JONATHAN FRANKLE, GEORGETOWN LAW CTR. ON PRIV. & TECH., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 2–4 (2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The Perpetual Line-Up - Center on Privacy and Technology at Georgetown Law - 121616.pdf [perma.cc/94GN-SJQ8].

18. *See, e.g.*, Drew Harwell, *Oregon Became a Testing Ground for Amazon's Facial-Recognition Policing. But What if Rekognition Goes Wrong?*, WASH. POST (April 30, 2019), https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/ [perma.cc/M639-KR3M] (providing an example of how law enforcement can utilize FRT to assist in arrests).

19. *See id.*

20. *See* Deven R. Desai & Joshua A. Kroll, *Trust but Verify: A Guide to Algorithms and the Law*, 31 HARV. J.L. & TECH. 1, 4 (2017) ("Both critics and advocates can stray into uncritical deference to the idea that big data and the algorithms used to process the data are somehow infallible science. . . . [A]lthough algorithms are decidedly *not* mystical things or dark magic, algorithms are not well understood outside the technical community."); Nanette Byrnes, *Why We Should*

disparate impact law enforcement's use of FRT may have on communities of color, law enforcement's use of FRT must be carefully scrutinized to support law enforcement's interest in investigative advancements while limiting the misuse of a software that has the potential to severely injure civil liberties.

Part I of this Note will explain the basic science behind machine learning and demonstrate how well-intended programmers can create biased algorithms through the use of program training material that does not represent the United States' diverse population. Part II of this Note will explore FRT's utility for police investigations, then survey various agencies' existing protocols for the use of FRT as well as how FRT is used in conventional practice. Part III of this Note will examine what role, if any, existing constitutional protections and statutory provisions can have in law enforcement use of FRT when considering concerns of algorithmic bias. Part IV of this Note will canvass pending and proposed legislative options for managing law enforcement's use of FRT and curbing algorithmic bias. Part V of this Note will analyze the potential avenues for balancing law enforcement investigative efforts with concerns of disparate infringement on civil liberties and algorithmic misidentification. This Note will conclude by encouraging legislative bodies to adopt adaptive frameworks to constrain the concerning prospects of FRT and algorithmic bias without crippling advancements in police investigative technology.

Part I: Facial Recognition Technology and Algorithmic Bias

A. Facial Recognition Technology: The Basics of Machine Learning

"Machine learning is a method of data analysis that automates analytical model building."[21] The process begins by giving a computer program, or algorithm, a set of test data and then instructing it to perform a specific task with that data.[22] As the algorithm sorts through the data in an attempt to achieve its

Expect Algorithms to Be Biased, MIT TECH. REV. (June 24, 2016), https://www.technologyreview.com/2016/06/24/159118/why-we-should-expect-algorithms-to-be-biased/ [perma.cc/5HNP-KQ8T] ("[A] broader trend that Fred Beneson, Kickstarter's former data chief, calls 'mathwashing': our tendency to idolize programs like Facebook's as entirely objective because they have mathematics at their core.").

21. *Machine Learning: What It Is and Why It Matters*, SAS, https://www.sas.com/en_us/insights/analytics/machine-learning.html [perma.cc/5XA2-3URT].

22. *Id.*

designated task, the algorithm is able to gradually perceive patterns and categories that allow it to achieve its designated task more efficiently.[23] This process of developing patterns and categories is the crux of machine learning.[24] Through these patterns, a machine learning system is able to determine what products a consumer may like due to their past purchases, who may default on a loan based on past financial choices, and answer many more predictive or analytical questions.[25]

An FRT system functions similarly to other forms of machine learning.[26] During development of an FRT system, like Amazon's Rekognition, the FRT system is given a set of test data—which is composed of a series of images containing things such as scenery, people, and other objects—and then told to sort between the faces and the other things present in these images.[27] Once the FRT system is able to consistently distinguish faces from other objects, then the programmers task the algorithm with distinguishing one person's face from another.[28] The system develops an understanding of how different people's facial features, their facial shape, and various other facial attributes can help the algorithm tell people apart.[29] Eventually, the program will be able to process new photos and compare the featured faces to those already in its memory in order to place a name to the face.[30]

B. Algorithmic Bias: How Seemingly Objective Machines Further Inequality

A machine learning program is only as accurate as its test data trains it to be.[31] A lack of foresight from programmers can inadvertently lead to test data either being unrepresentative of reality or reflective of existing biases.[32] For example, in 2016,

23. Yufeng Guo, *The 7 Steps of Machine Learning*, MEDIUM: TOWARDS DATA SCI. (Aug. 31, 2017), https://towardsdatascience.com/the-7-steps-of-machine-learning-2877d7e5548e [perma.cc/EL7V-JLMY].

24. *See id.*

25. *See, e.g.*, Desai & Kroll, s*upra* note 20.

26. *See* Oleksii Kharkovyna, *An Intro to Deep Learning for Face Recognition*, MEDIUM: TOWARDS DATA SCI. (June 26, 2017), https://towardsdatascience.com/an-intro-to-deep-learning-for-face-recognition-aa8dfbbc51fb [https://perma.cc/4868-BUE6].

27. *Id.*

28. *Id.*

29. *Id.*

30. *Id.*

31. *See* SAS, s*upra* note 21.

32. *See* Karen Hao, *This Is How AI Bias Really Happens—and Why It's So Hard*

ProPublica examined the accuracy of a tool called COMPAS, which has been used in determining an appropriate sentence for convicted criminals.[33] ProPublica found that COMPAS was almost twice as likely to falsely flag Black defendants as recidivists compared to White defendants.[34] These disparities stemmed from questions the COMPAS model used in its recidivism risk evaluation, such as: "Was one of your parents ever sent to jail or prison?"[35] By relying on data hued by existing inequalities,[36] the COMPAS system mistakenly propagated inequalities based on supposedly race-neutral questions like parental incarceration.[37]

As an FRT program is learning, it is presented with test data, which, to achieve accurate results, should feature images of diverse faces that are representative of society.[38] However, recent research suggests FRT test data principally features lighter-skin and

---

to Fix, MIT TECH. REV. (Feb. 4, 2019), https://www.technologyreview.com/s/612876/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix/ [perma.cc/6VE9-3F3S].

33. Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kircher, *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [perma.cc/3VTJ-K5GP].

34. *Id.*

35. *Id.*

36. Smith and Levinson describe these inequalities:

> The disproportionate incarceration of minorities is one of the American criminal justice system's most established problems. In spite of a societal backdrop in which descriptive claims of a 'post-racial' America prosper, the problematic racial dynamics of criminal justice persist. The numbers are stark and clear: one out of every twenty-nine black adult women and men are currently incarcerated compared with only one out of every 194 whites.

Robert J. Smith & Justin D. Levinson, *The Impact of Implicit Racial Bias on the Exercise of Prosecutorial Discretion*, 35 SEATTLE U. L. REV. 795, 795 (2012).

Further:

> [I]mplicit favoritism is important because it helps to drive racial disparities in the criminal justice system. Social scientists have linked implicit favoritism to the ability of jurors to accurately remember damning details of an alleged offense, to the evaluation of whether negative actions taken by another are the result of one's disposition or instead to the circumstances that constrained one's choices, and to the degree of empathic response to human pain. Implicit white favoritism has serious ramifications for criminal law and procedure because it can operate in a range of powerful ways that can be distinguished from traditional race-focused examples: in the way, for example, white drivers are pulled over less often than unseen drivers, in the way legislators might see white "meth" addicts as suffering from an illness and black "crack" addicts as criminals, and in the way prosecutors and jurors view a crime as more aggravated if the victim is white or see a white juvenile offender to be more capable of redemption.

Robert J. Smith, Justin D. Levinson & Zoe Robinson, *Implicit White Favoritism in the Criminal Justice System*, 66 ALA. L. REV. 871, 875–76 (2015) (footnotes omitted).

37. Angwin et al., *supra* note 33.

38. Kharkovyna, *supra* note 26.

traditionally-male facial features.[39] This leads FRT programs to not be appropriately trained on how to identify and/or distinguish people with darker skin or people with traditionally-female facial features.[40] This heightened error rate for people with darker skin or people with traditionally-female facial features was likely not noticed by programmers initially because overall FRT is very accurate.[41] It is only when an algorithm's error rates are dissected along demographic lines that these concerns emerge.[42]

Not all FRT programs exhibit the same magnitude of demographically-based error rates.[43] In December 2019, the National Institute of Standards and Technology (NIST)—a government agency tasked with advancing measurement science, standards, and technology[44]—evaluated 189 different FRT algorithms from ninety-nine developers to see how these programs performed across variations of race, age, and sex.[45] NIST's study tested the programs on both "one-to-one" matching[46] and "one-to-

---

39. *See* Steve Lohr, *Facial Recognition Is Accurate, If You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html [perma.cc/MAV4-8LP8] ("A.I. software is only as smart as the data used to train it. If there are many more white men than black women in the system, it will be worse at identifying the black women.").

40. For example:

> LFW, a dataset composed of celebrity faces which has served as a gold standard benchmark for face recognition, was estimated to be 77.5% male and 83.5% White (Han and Jain, 2014). Although (Taigman et al., 2014)'s face recognition system recently reported 97.35% accuracy on the LFW dataset, its performance is not broken down by race or gender. Given these skews in the LFW dataset, it is not clear that the high reported accuracy is applicable to people who are not well represented in the LFW benchmark.

Buolamwini & Gebru, *supra* note 14, at 3.

41. *See id.* at 12 ("We found that all [three gender] classifiers performed best for lighter individuals and males overall. The classifiers performed worst for darker females."). In the aggregate, gender classification accuracy ranged from 87.9% to 93.7%, within marketable range. *Id.* at 11.

42. *See* Clare Garvie & Jonathan Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, ATLANTIC (Apr. 7, 2016), https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/ [perma.cc/N2QS-K6FC].

43. *See* PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, NAT'L INST. OF STANDARDS & TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 2 (2019).

44. NIST is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce that is tasked with advancing measurement science, standards, and technology. *See NIST Mission, Vision, Core Competencies, and Core Values*, NIST (Jan. 26, 2017), https://www.nist.gov/about-nist/our-organization/mission-vision-values [perma.cc/7KDS-T9P7].

45. GROTHER ET AL., *supra* note 43, at 1.

46. *NIST Study Evaluated Effects of Race, Age, Sex, on Face Recognition Software*, NIST (Dec. 19, 2019), https://www.nist.gov/news-events/news/

many" matching.[47] NIST found that the majority of tested programs exhibited a higher false positive rate across each test, meaning a higher rate of misidentification, when the program was asked to evaluate non-White faces and faces with traditionally-female characteristics.[48] The authors noted, "differentials in false positives in one-to-many matching are particularly important because the consequences could include false accusations."[49] Although some programs exhibited a minimal error rate,[50] NIST expressed a general concern about organizations using FRT not appropriately researching or scrutinizing the specific programs their organization employs.[51] FRT program designers have acknowledged these problems and are working to improve them,[52] but as things stand currently, FRT programs are laced with algorithmic bias.[53]

Part II: Law Enforcement's Use of FRT: Investigative

2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software [perma.cc/3N8U-Q49K] (describing "one-to-one" matching as "confirming a photo matches a different photo of the same person in a database . . . [which] is commonly used for verification work, such as unlocking a smartphone or checking a passport").

47. *Id.* (describing "one-to-many" matching as "determining whether the person in the photo has any match in a database").

48. GROTHER ET AL., *supra* note 43, at 2 (noting the tested programs varied in their false positive error rates "by factors of 10 to beyond 100 times").

49. *E.g.*, NIST, *supra* note 46.

50. MICHAEL MCLAUGHLIN & DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., THE CRITICS WERE WRONG: NIST DATA SHOWS THE BEST FACIAL RECOGNITION ALGORITHMS ARE NEITHER RACIST NOR SEXIST 2 (2020), https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms [perma.cc/MS3N-P2HE] ("[T]he most accurate algorithms—which should be the only algorithms used in government systems—did not display a significant demographic bias . . . . [S]ome highly accurate algorithms had false-positive demographic differentials that were so small as to be 'undetectable' for one-to-many searches.").

.

51. GROTHER ET AL., *supra* note 43, at 3 ("Operational implementations usually employ a single face recognition algorithm. Given algorithm-specific variation, it is incumbent upon the system owner to know their algorithm . . . . Since different algorithms perform better or worse in processing images of individuals in various demographics, policy makers, face recognition system developers, and end users should be aware of these differences and use them to make decisions and to improve future performance.").

52. *See* Sean Hollister, *Google Contractors Reportedly Targeted Homeless People for Pixel 4 Facial Recognition*, VERGE (Oct. 2, 2019), https://www.theverge.com/2019/10/2/20896181/google-contractor-reportedly-targeted-homeless-people-for-pixel-4-facial-recognition [perma.cc/N8FH-25UN].

53. *E.g.*, Buolamwini & Gebru, *supra* note 14.

Potential, Procedures, and Practices

A. FRT's Potential for Criminal Suspect Identification

Law enforcement agencies across the United States have been rapidly adopting FRT as a crucial part of their investigative procedures.[54] Federal, state, and local agencies have partnered with FRT designers like Amazon, Google, and others to increase their capabilities in identifying and tracking suspects.[55] Currently, law enforcement agencies primarily use FRT to identify suspects from images captured by surveillance footage or by a witness's camera, but the uses of FRT will potentially expand in the near future.[56] The government "facial biometrics" market is expected to grow nearly threefold within the next decade.[57] Currently, at least one fourth of state or local police departments have the ability to conduct searches through a face recognition system.[58]

Law enforcement's use of FRT is expected to revolutionize law enforcement's ability to identify suspects in a similar way to the spread of forensic DNA identification in the late 1980s.[59] Like DNA evidence, FRT allows officers to take a small piece of biometric evidence recovered from a crime scene and then cross-reference this

---

54. *See generally* Jon Schuppe, *Facial Recognition Gives Police a Powerful New Tracking Tool. It's Also Raising Alarms.*, NBC NEWS (July 30, 2018), https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936 [perma.cc/8YCS-UYKG] (discussing law enforcement's use of facial recognition).

55. *See id.*

56. JENNIFER LYNCH, ELEC. FRONTIER FOUND., FACE OFF: LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECHNOLOGY 1 (Gennie Gebhart ed., 2020) ("Today, law enforcement officers can use mobile devices to capture face recognition-ready photographs of people they stop on the street; surveillance cameras boast real-time face scanning and identification capabilities; and federal, state, and local law enforcement agencies have access to hundreds of millions of images of faces of law-abiding Americans. On the horizon, law enforcement would like to use face recognition with body-worn cameras, to identify people in the dark, to match a person to a police sketch, or even to construct an image of a person's face from a small sample of their DNA.").

57. *See* Jon Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC NEWS (May 11, 2019), https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251 [perma.cc/4JZ5-2758] ("The government 'facial biometrics' market . . . is expected to soar from $136.9 million in 2018 to $375 million by 2025 . . . .").

58. GARVIE ET AL., *supra* note 17, at 2.

59. *See generally* Paul E. Tracy & Vincent Morgan, *Big Brother and His Science Kit*: *DNA Databases for 21st Century Crime Control?*, 90 J. CRIM. L. & CRIMINOLOGY 635, 640 (2000) (discussing different DNA initiatives led by the United States Department of Justice and the Federal Bureau of Investigation in support of law enforcement).

evidence with their department's databases to obtain a comprehensive list of information about the target suspect.[60] Unlike DNA analysis, FRT does not require a suspect to have left some of their bodily tissue, fluids, or other biological material at the crime scene.[61] FRT only requires an image of the suspect captured through closed-circuit television (CCTV) or some other method.[62]

Already, FRT has led to the apprehension of serious criminals that had evaded capture for months or even years. For example, in December 2018, the York Area Regional Police Department was able to identify a man who had electronically manipulated and eventually sexually assaulted a fifteen-year-old girl in July 2016.[63] Despite the suspect leaving his sunglasses at the crime scene, which were processed for DNA and fingerprints, police were unable to identify the suspect until they finally received a match using facial recognition software.[64] After months of cross-referencing the photos the suspect sent the victim with driver's license photos, mugshots, and other sources of facial identification, law enforcement found a match. Law enforcement got a lucky break when the suspect updated his driver's license photo to more closely resemble how he appeared at the time of the assault.[65] The York Area Regional Police Department's successful location of a suspect is just one of many examples of FRT assisting law enforcement when other methods of identifying suspects have failed.[66] FRT can greatly enhance law

60. *See* Schuppe, *supra* note 57.

61. *See id.*

62. *See id.*

63. *See* Daniel Rosler, *Facial Recognition Software Led to the Arrest of a Scranton Man for Alleged Sexual Assault of Teen*, ASSOCIATED PRESS (Dec. 18, 2018), https://apnews.com/article/e0a56374618840cf88e78637428d63d0 [perma.cc/Q2K3-FWKD].

64. *See id.*

65. *See id.*

66. *See* Marco della Cava & Elizabeth Weise, *Capital Gazette Gunman Was Identified Using Facial Recognition Technology That's Been Controversial*, USA TODAY (June 29, 2018), https://www.usatoday.com/story/tech/talkingtech/2018/06/29/capital-gazette-gunman-identified-using-facial-recognition-technology/744344002/ [perma.cc/XH5X-496U] (explaining law enforcement's use of facial identification technology "because the system for getting the identification off his fingerprints was working slowly . . . ."); Ryan Lucas, *How a Tip — and Facial Recognition Technology — Helped the FBI Catch a Killer*, NPR (Aug. 21, 2019), https://www.npr.org/2019/08/21/752484720/how-a-tip-and-facial-recognition-technology-helped-the-fbi-catch-a-killer [perma.cc/BCH5-XNMH]; Amy B. Wang, *A Suspect Tried to Blend in with 60,000 Concertgoers. China's Facial-Recognition Cameras Caught Him.*, WASH. POST (Apr. 13, 2018), https://www.washingtonpost.com/news/worldviews/wp/2018/04/13/china-crime-facial-recognition-cameras-catch-suspect-at-concert-with-60000-people/ [perma.cc/MZ4L-HRVP] (describing the use of FRT to track one individual at a 60,000-person event in China).

enforcement's capabilities,[67] and potentially lead to fewer mistakes.[68]

B. Current Police Procedures and Unadvised Practices

Most agencies follow the same five-step process in using FRT to identify a suspect.[69] First, officers obtain a visual representation of a criminal suspect.[70] Second, officers prepare the visual representation to be entered into the FRT.[71] Third, the FRT compares the visual representation with the system's catalogue of faces, typically composed of mugshots.[72] Fourth, the FRT produces a list of possible facial matches for an inquiring officer to review; each match typically comes with a coinciding confidence level, which demonstrates how certain the system is that the listed person is the targeted suspect.[73] Lastly, an officer reviews the list produced by the FRT and determines if any of the potential matches should be investigated further.[74]

Many law enforcement agencies, including the Federal Bureau of Investigation (FBI)[75] and the New York Police Department

---

67. The use of FRT has been successful in many cases:

> Recently, the work of the facial identification team led to the arrest of a man accused of raping a worker at a day spa, and another charged with pushing a subway passenger onto the tracks. We have made arrests in murders, robberies and the on-air assault of a TV reporter. A woman whose dismembered body was found in trash bags in two Bronx parks was identified. So was a woman hospitalized with Alzheimer's, through an old arrest photo for driving without a license.

James O'Neill, *How Facial Recognition Makes You Safer*, N.Y. TIMES (June 9, 2019), https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html [perma.cc/G6L2-CC6P].

68. *See id.* ("The software has also cleared suspects. According to the Innocence Project, 71 percent of its documented instances of false convictions are the result of mistaken witness identifications. When facial recognition technology is used as a limited and preliminary step in an investigation . . . these miscarriages of justice are less likely.").

69. *See* Schuppe, *supra* note 57.

70. *See id.*

71. *See id.*

72. *See id.*

73. *See id.*; *see also* Matt Leonard, *Why Confidence Matters in Facial Recognition Systems*, GCN (Aug. 6, 2018), https://gcn.com/Articles/2018/08/06/trust-facial-recognition.aspx?Page=1 [perma.cc/U624-34UH] (discussing the importance of setting a high confidence threshold for FRT programs when used by law enforcement because a program's threshold confidence level determines the occurrence of false positives).

74. *See* Schuppe, *supra* note 57.

75. *See Facial Recognition Technology: Part II: Ensuring Transparency in Government Use*: *Hearing Before the H. Comm. on Oversight and Reform*, 116th

(NYPD),[76] treat the results of an FRT inquiry as an "investigative lead only."[77] An "investigative lead" means officers must find additional investigative material to reach the level of probable cause needed for a legitimate arrest.[78] However, the FBI is currently considering dropping the "investigative lead only" protocol and allowing an FRT match to reach the level of probable cause based on confidence in its program and expected expansion.[79] Other law enforcement agencies, like Oregon's Washington County Police Department, will only run a facial recognition search after establishing probable cause that a crime has been committed in order to locate the specific perpetrator.[80]

Although there are currently some discrepancies in procedures related to FRT, there appears to be even larger discrepancies between field usage of FRT and best practice suggestions.[81] A May 2019 report from Georgetown Law's Center on Privacy &

Cong. 4 (2019) (statement of Kimberly J. Del Greco, Deputy Assistant Director, Criminal Justice Information Services, Federal Bureau of Investigation) [hereinafter *Del Greco Hearing Statement*].

76. *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEORGETOWN L. CTR. ON PRIV. & TECH. (May 16, 2019), https://www.flawedfacedata.com/ [perma.cc/99ZP-SSY9].

77. *Id.*

78. *Id.*; *see also* BUREAU OF JUST. ASSISTANCE, U.S. DEP'T JUST., FACE RECOGNITION POLICY DEVELOPMENT TEMPLATE 3 (2017) [hereinafter BJA TEMPLATE] ("[FRT] is not being used as an all-knowing big brother that keeps track of an individual's weekly—or daily—trips to a business. More accurately, it is a lead generator for law enforcement to investigate criminal activity, akin to a more reliable eye witness [sic].").

79. *See* Garvie, *supra* note 76 ("[A]n official for the Federal Bureau of Investigation (FBI), which runs its own face recognition system, has indicated that the agency plans to do away with the 'investigative lead only' limitation altogether. At a conference in 2018, FBI Section Chief for Biometric Services Bill McKinsey said of the FBI: 'We're pretty confident we're going to have face [recognition] at positive ID in two to three years.'").

80. Shirin Ghaffary, *How to Avoid a Dystopian Future of Facial Recognition in Law Enforcement*, VOX: RECODE (Dec. 10, 2019), https://www.vox.com/recode/2019/12/10/20996085/ai-facial-recognition-police-law-enforcement-regulation [perma.cc/U4ZH-FV8V] ("[A public information officer at the Washington County, Oregon Police Department] told Recode that officers only use the [facial recognition] tools when there's probable cause that someone has committed a crime, and only matches it to jail booking photos, not DMV databases. (This sets Washington County apart—several other police departments in the US do use DMV databases for facial recognition searches.) He also said the department doesn't use Rekognition to police large crowds, which police in Orlando, Florida, tried to do—and failed to do effectively, after running into technical difficulties and sustained public criticism.").

81. *See* Bryan Menegus, *Defense of Amazon's Face Recognition Tool Undermined by Its Only Known Police Client*, GIZMODO (Jan. 31, 2019), https://gizmodo.com/defense-of-amazons-face-recognition-tool-undermined-by-1832238149 [perma.cc/K568-CGB7].

Technology expressed concern with the NYPD's FRT practices.[82] The report found that NYPD officers would enter "probe photos" of suspects into their FRT program and then pursue the people their system listed as potential suspects.[83] These "probe photos" included composite drawings as well as "a suspect's celebrity doppelgänger."[84] In addition, when NYPD officers received a sub-par image of a suspect from surveillance footage or a witness's camera, they would modify the picture in order to bring it closer to the style common in mugshots by inserting open eyes, mirroring a partial face to make it full, or substituting other identity points.[85] Georgetown researchers found these procedures to greatly diminish the validity of any inquiry list produced by the NYPD's FRT.[86]

During the summer of 2020, news outlets reported the first documented wrongful arrests caused by FRT. Two Black men from Michigan, Robert Williams[87] and Michael Oliver,[88] both suffered

82. Garvie, *supra* note 76 (criticizing NYPD's facial recognition practices involving "probe photos" and photo edits that "amount to the fabrication of facial identity points").

83. *Id.* ("There are no rules when it comes to what images police can submit to face recognition algorithms to generate investigative leads. As a consequence, agencies across the country can—and do—submit all manner of 'probe photos,' photos of unknown individuals submitted for search against a police or driver license database.").

84. *Id.* ("One detective from the Facial Identification Section (FIS), responsible for conducting face recognition searches for the NYPD, noted that the suspect looked like the actor Woody Harrelson, known for his performances in *Cheers*, *Natural Born Killers*, *True Detective*, and other television shows and movies. A Google image search for the actor predictably returned high-quality images, which detectives then submitted to the face recognition algorithm in place of the suspect's photo. In the resulting list of possible candidates, the detectives identified someone they believed was a match—not to Harrelson but to the suspect whose photo had produced no possible hits.").

85. *Id.* ("Editing photos before submitting them for search is common practice . . . . One technique that the NYPD uses involves replacing facial features or expressions in a probe photo with ones that more closely resemble those in mugshots—collected from photos of other people.").

86. *Id.* (finding that common FRT procedures reflect "at best an attempt to create information that isn't there in the first place and at worst the introduction of evidence that matches someone other than the person being searched for.").

87. Paresh Dave, *Facial Recognition Leads to First Wrongful U.S. Arrest Activists Say*, REUTERS (June 24, 2020), https://www.reuters.com/article/us-michigan-facial-recognition/face-recognition-vendor-vows-new-rules-after-wrongful-arrest-in-u-s-using-its-technology-idUSKBN23V1KJ [https://perma.cc/A88U-5KC7] ("Robert Williams, who is Black, spent over a day in Detroit police custody in January after Rank One's face recognition software connected his driver's license photo to surveillance video of someone shoplifting, the American Civil Liberties Union of Michigan (ACLU) said. . . . In a video shared by ACLU, Williams says officers released him after acknowledging 'the computer' must have been wrong.").

88. Kris Holt, *Facial Recognition Linked to a Second Wrongful Arrest by Detroit*

from flawed investigations. In each case, Detroit Police ran blurry surveillance footage through their department's FRT, then showed the generated lineup to a witness of the offense.[89] Upon minimal examination, it should have been clear these men were misidentified. Michael Oliver, who has extensive tattoos on his neck and arms, noted the surveillance footage which led to his arrest "looked nothing like" him and the actual offender "didn't even have tattoos."[90] Robert Williams—who was arrested in front of his wife and their young daughters in his driveway—stated he felt "empty" and "humiliated" by the experience.[91] After Robert Williams case came to light, Detroit Police Chief James Craig admitted their FRT system is heavily flawed.[92] Chief Craig noted at a public meeting that "[i]f we were just to use the technology by itself, to identify someone, I would say 96 percent of the time it would misidentify."[93] It is unclear at this time how many cases like Robert Williams' and Michael Oliver's have gone unreported.

Like any law enforcement tool or tactic, FRT comes with a substantial list of inspiring prospects and concerning potentials. FRT can revolutionize how law enforcement identifies and locates suspects, but its implementation needs to follow proper procedures

---

Police, ENGADGET (July 10, 2020), https://www.engadget.com/facial-recognition-false-match-wrongful-arrest-224053761.html [https://perma.cc/VJ9C-FLX3] ("[P]olice in the city arrested a man for allegedly reaching into a person's car, taking their phone and throwing it, breaking the case and damaging the screen in the process. Facial recognition flagged Michael Oliver as a possible suspect, and the victim identified him in a photo lineup as the person who damaged their phone. Oliver was charged with a felony count of larceny over the May 2019 incident. He said he didn't commit the crime and the evidence supported his claim.").

89. *Id.*; Paresh Dave, *supra* note 87.

90. Elaisha Stokes, *Wrongful Arrest Exposes Racial Bias in Facial Recognition Technology*, CBS NEWS (Nov. 19, 2020), https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/ [https://perma.cc/7HA5-TZKP].

91. Ahiza García-Hodges, Chiara Sottile & Jacob Ward, *Man Wrongfully Arrested Due to Facial Recognition Software Talks About 'Humiliating' Experience*, NBC NEWS (June 26, 2020), https://www.nbcnews.com/business/business-news/man-wrongfully-arrested-due-facial-recognition-software-talks-about-humiliating-n1232184 [https://perma.cc/25KF-6Q7H] ("Their oldest daughter nearly started hyperventilating and couldn't do her homework without getting emotional since her dad usually helps her with it. The couple also said they'll never forget how Williams missed a small but important milestone while in police custody. 'I wasn't there for her first tooth,' Williams said. 'Even though it was one day, I still missed a milestone in her life.'").

92. Jason Koebler, *Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time*, VICE: MOTHERBOARD (June 29, 2020), https://www.vice.com/en/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time [https://perma.cc/XH55-4JY2].

93. *Id.*

to ensure effective results and avoid misuse. Although some law enforcement agencies have done a satisfactory job of self-regulating their FRT use, it is critical to consider what formal legal approaches can moderate law enforcement use of FRT, especially considering FRT's tendency to harbor algorithmic bias.

Part III: Limits to Law Enforcement Use of FRT and Algorithmic Bias from the Constitution and Existing Civil Rights Statutes

A. Fourth Amendment Protections from Unreasonable Arrest

The Supreme Court recently determined that novel forms of technology may require long-running constitutional doctrines to adapt to circumstances once unimaginable.[94] The Fourth Amendment, which has been one of the primary ways to regulate police action,[95] has had to adapt to modern expectations of privacy and novel methods of police intrusion into those expectations of privacy.[96] Although the Court has made some progress, many scholars have expressed dissatisfaction with the pace at which the Court is choosing to adapt the Fourth Amendment to the realities of technology in modern life.[97] Based on the novelty of law

94. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (uprooting the long-held presumption that defendants forfeit all of their Fourth Amendment privacy interests when they turn over material to a third party).

95. Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 GA. L. REV. 109, 116 (2017).

96. *See, e.g.*, Riley v. California, 573 U.S. 373, 403 (2014) (distinguishing electronic devices from other objects for purposes of the search incident to arrest warrant exception); United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring) (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations . . . . And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'"); Kyllo v. United States, 533 U.S. 27, 33–34, 40 (2001) (holding that the use of advanced technology to examine the internal affairs of a residence constitutes a search under the Fourth Amendment and stating "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology . . . . The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy").

97. *See* Eli R. Shindelman, *Time for the Court to Become "Intimate" with Surveillance Technology*, 52 B.C. L. REV. 1909, 1911–12 (2011) ("These advancements in surveillance technology have far outpaced the evolution of Fourth Amendment jurisprudence. Many scholars have argued that the current state of

enforcement's use of FRT, it is unsurprising that the Supreme Court has yet to tackle the issue of whether, or how, Fourth Amendment protections limit law enforcement's use of FRT as of the writing of this Note.[98]

Due to the current lack of precedent, scholars are left to speculate as to whether an FRT scan constitutes a search in accordance with the Fourth Amendment.[99] Less attention has been given to FRT's role in establishing grounds for an arrest. As stated above, the FBI currently holds that FRT identification can only be used as an "investigative lead."[100] However, with law enforcement's growing confidence in FRT, the question of whether an FRT identification could reach the level of probable cause to support a lawful arrest under the Fourth Amendment will likely soon arise.

Probable cause has been described as a "fluid concept—turning on the assessment of probabilities in particular factual contexts"[101] and thus requires the "totality-of-the-circumstances analysis" in each individual case.[102] Because law enforcement agencies have compared FRT matches to "a more reliable eye witness,"[103] it is useful to compare FRT matches to eyewitness or informant testimony. In the context of police informants, officers must show there are sufficient "indicia of reliability" to trust the testimony of an informant.[104] While an anonymous tip must be supported by facts that can be corroborated, the testimony of a credible informant—who had provided officers with information in the past—can be enough to independently establish probable cause.[105] With this said, the weight of an FRT match toward a

---

Fourth Amendment jurisprudence lacks a genuine understanding of privacy given the realities of modern technology. These scholars argue that because there has been widespread development in forms of technology that are capable of impinging on a person's privacy, courts must interpret the Fourth Amendment broadly to adequately protect individual liberty.").

98. *See* Katelyn Ringrose, *Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns*, 105 VA. L. REV. ONLINE 57, 64 (2019).

99. *See* Kelly Blount, *Body Worn Cameras with Facial Recognition Technology: When It Constitutes a Search*, 3 CRIM. L. PRAC., Fall 2017, at 61. *See generally* Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591 (2017).

100. *Del Greco Hearing Statement*, *supra* note 75, at 4.

101. Illinois v. Gates, 462 U.S. 213, 232 (1983).

102. *Id.* at 238–39.

103. BJA TEMPLATE, *supra* note 78, at 3.

104. Florida v. J. L., 529 U.S. 266, 270 (2000).

105. *See* Adams v. Williams, 407 U.S. 143, 146–47 (1972).

probable cause determination will rest on whether judges believe FRT is sufficiently reliable to justify a showing of probable cause.[106]

In determining the perceived reliability of FRT, an analogy between FRT matches and DNA matches is appropriate because both are founded in biometric identification.[107] The reliability of all DNA matches was widely contested until courts began allowing for judicial notice of DNA's reliability.[108] This holding allowed courts to assume DNA matches are accurate enough to be admissible as long as the expert properly performed the techniques involved in analyzing a specific DNA specimen.[109] In the coming years, FRT matches could progress from being treated in the same way as an eyewitness identification to being seen more like DNA evidence—as inherently reliable absent proof of technical mistakes. However, an important component of courts extending judicial notice to DNA matches' reliability was the near unanimous acceptance of the genetic theories underlying DNA analysis by the relevant scientific community.[110] Currently, there is not a unanimous scientific consensus supporting the validity of FRT due to continuing concerns of algorithmic bias and general efficiency.[111] Therefore, the prospect of informed judicial notice of FRT seems unlikely at the current time. As FRT advances it should be met with the same, if not more, skepticism than DNA evidence underwent during its infancy.[112]

---

106. *Cf.* United States v. Jakobetz, 955 F.2d 786, 799–800 (2d Cir. 1992) (holding that DNA profiling evidence can be reliable enough for a court to take judicial notice).

107. *See* LYNCH, *supra* note 56, at 4 (listing "face recognition" and "DNA" as examples of biometric identification that are becoming more popular).

108. *See Jakobetz*, 955 F.2d at 799–800 ("[I]t appears that in future cases with a similar evidentiary issue, a court could properly take judicial notice of the general acceptability of the general theory and the use of these specific [DNA analysis] techniques . . . . Beyond such judicial notice, the threshold for admissibility should require only a preliminary showing of reliability of the particular data to be offered, i.e., some indication of how the laboratory work was done and what analysis and assumptions underlie the probability calculations.") (citation omitted).

109. *See id.*

110. *Id.* at 799 ("[T]he general theories of genetics which support DNA profiling are unanimously accepted within the scientific community.").

111. *See, e.g.*, Buolamwini & Gebru, *supra* note 14, at 3 (discussing research covering "[f]ace detection and classification algorithms" used by law enforcement that indicates lower accuracy "for people labeled female, Black, or between the ages of 18–30 than for other demographic cohorts").

112. *Cf.* Tracy & Morgan, *supra* note 59, at 636, 638 ("[T]he current proliferation of DNA databases and their likely further expansion raise three significant policy issues and attendant questions. First, how do we utilize this new technology, while protecting against misuse and abuse? . . . Although technology makes certain advances possible, are these advances truly necessary? . . . [W]ill DNA databases provide law enforcement and the subsequent criminal prosecutions with measurable and significant effects on crime?").

The Fourth Amendment has typically not been a respite for those concerned with discriminatory policies.[113] Invasions of privacy or seizures of one's person or belongings that comply with probable cause but are based on discriminatory intent are not considered violations of the Fourth Amendment.[114] The Court has determined the subjective, potentially discriminatory, intent of an arresting officer plays no role in ordinary, probable cause Fourth Amendment analysis.[115] The constitutional basis for objecting to law enforcement's intentionally discriminatory application of laws is the Fourteenth Amendment's Equal Protection Clause, not the Fourth Amendment.[116] It is unclear how precisely the Fourth Amendment would be applied to unintentional discriminatory actions related to programs controlled by algorithmic bias, but it is most likely that algorithmic bias would influence the determination of whether probable cause is actually present in a given case.

B. Equal Protection Clause as a Response to Algorithmic Bias

It is worth considering how the Equal Protection Clause of the Fourteenth Amendment could remedy concerns of algorithmic bias. Plaintiffs pursuing a race-based[117] Fourteenth Amendment Equal Protection Clause claim against the government have one of two routes to prevail on their claim.[118] The first route requires the contested government policy to contain an explicit racial

---

113. *See* Jonathan P. Feingold, *Equal Protection Design Defects*, 91 TEMP. L. REV. 513, 516 (2019).

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

115. *Id.* (quoting Scott v. United States, 436 U.S. 128, 136, 138 (1978) (referencing United States v. Robinson, 414 U.S. 218, 236 (1973))) ("[W]e said that 'subjective intent alone . . . does not make otherwise lawful conduct illegal or unconstitutional.' We described *Robinson* as having established that 'the fact that the officer does not have the state of mind which is hypothecated by the reasons which provide the legal justification for the officer's action does not invalidate the action taken as long as the circumstances, viewed objectively, justify that action.' We think these cases foreclose any argument that the constitutional reasonableness of traffic stops depends on the actual motivations of the individual officers involved.").

116. *Id.* ("We of course agree with petitioners that the Constitution prohibits selective enforcement of the law based on considerations such as race. But the constitutional basis for objecting to intentionally discriminatory application of laws is the Equal Protection Clause, not the Fourth Amendment.").

117. Feingold, *supra* note 113. This article uses race-based Equal Protection Clause doctrine as an example because it is often reviewed with the strictest level of scrutiny, as opposed to, for example, gender-based Equal Protection Clause claims which are only reviewed with intermediate scrutiny. Therefore, race-based Equal Protection Clause analysis provides the best potential for exploring the effectiveness of Equal Protection claims in this area.

118. *Id.* at 516–17.

classification.[119] The plaintiff then must show this racial classification does not withstand strict judicial scrutiny.[120] Strict scrutiny means the government policy containing the racial classification must be shown to lack either a compelling government interest or a narrowly tailored approach to fulfilling the policy's governmental interest.[121]

The second route for an Equal Protection Clause claim requires a plaintiff to show "[p]roof of racially discriminatory intent or purpose"[122] in the adoption or maintaining of the contested government policy.[123] A plaintiff need not demonstrate discrimination was the dominant or primary purpose of the contested governmental policy, but a plaintiff must show discrimination was at least a consideration of those instituting the policy or enforcing the policy.[124] The requirement of discriminatory intent under the Equal Protection Clause means a plaintiff cannot pursue a disparate impact claim under this Clause.[125]

Scholars have critiqued this bifurcated approach to the Equal Protection Clause, which favors facial neutrality and is only concerned with disparate treatment.[126] This judicial approach has led to many societal issues without an appropriate avenue of recourse in the courts.[127] One of the clearest examples is the well-known sentencing disparities between crack cocaine and powder cocaine offenses.[128] Scholars have expressed further concern about

---

119. *See* City of Richmond v. J.A. Cronson Co., 488 U.S. 469, 490 (1989).

120. The Court in *City of Richmond* found:

> Absent searching judicial inquiry into the justification for such race-based measures, there is simply no way of determining what classifications are 'benign' or 'remedial' and what classifications are in fact motivated by illegitimate notions of racial inferiority or simple racial politics. Indeed, the purpose of strict scrutiny is to 'smoke out' illegitimate uses of race by assuring that the legislative body is pursuing a goal important enough to warrant use of a highly suspect tool.

Id. at 493.

121. *Strict Scrutiny*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/strict_scrutiny [perma.cc/YB9Q-2QX8].

122. Vill. of Arlington Heights v. Metro. Hous. Dev. Corp., 429 U.S. 252, 265 (1977).

123. Rogers v. Lodge, 458 U.S. 613, 617 (1982).

124. *Arlington Heights*, 429 U.S. at 265.

125. Adams v. City of Indianapolis, 742 F.3d 720, 726 n.3 (7th Cir. 2014).

126. Feingold, *supra* note 113.

127. Ashlee Riopka, *Equal Protection Falling Through the Crack: A Critique of the Crack-to-Powder Sentencing Disparity*, 6 ALA. C.R. & C.L. L. REV. 121, 122 (2015).

128. *Id.* at 124, 129 (explaining that while the sentencing disparity between crack and powder cocaine was originally 100:1 in the Anti-Drug and Abuse Act of 1986, the Fair Sentencing Act of 2010 still contained a disparity of 18:1). Riopka continues:

the Court's presumption that "facially neutral evaluative tools produce racially neutral results."[129] Scholars have noted that the Equal Protection Clause is not an appropriate avenue for disparities caused by algorithms due to the Court's bifurcated approach solely being concerned with disparate treatment, which requires a showing of discriminatory intent.[130]

C. Civil Rights Statutes as a Response to Algorithmic Bias in Police Systems

Civil rights statutes are often viewed as a set of tools—more flexible than the Equal Protection Clause—that aggrieved plaintiffs can use to seek justice. For police conduct and policy there is a diminished set of tools available compared to discrimination in fields like housing,[131] employment,[132] or public accommodations.[133] Each of these fields of discrimination, besides police conduct and policy,[134] have a simple disparate impact route for aggrieved plaintiffs to pursue.[135] Police conduct and policy, on the other hand, are usually addressed through 42 U.S.C. § 1983,[136] which allows for civil suits against a person acting under color of law stemming from

> Since the Fair Sentencing Act is facially race-neutral, its racially disparate impact provides the most obvious evidence of an equal protection violation. Unfortunately, defendants who rely solely on this method of proof will face a multitude of challenges. While the Supreme Court has not specifically invalidated disparate impact theory as a method of proving discriminatory intent in equal protection challenges, additional hurdles make disparate impact arguments difficult. Under the current trend of equal protection jurisprudence, evidence of racial disparity remains constitutionally insignificant unless it is accompanied by evidence of disparate treatment or intentional discrimination.

Id. at 131.

129. *See* Feingold, *supra* note 113, at 528–29 ("[E]qual protection doctrine rests on the presumption that facially neutral evaluative tools produce racially neutral results. This presumption spans Justices and ideological spectrums . . . . [However] decades of research on implicit bias and stereotype threat reveals that common measures of merit, although facially neutral, fail to produce racially neutral results.").

130. *Id.* at 539–40.

131. *See, e.g.*, David J. Frizell & Ronald D. Cucchiaro, *Fair Housing Act—Disparate Impact*, 36 N.J. PRAC., LAND USE LAW § 20.28 (3d ed. 2019).

132. *See, e.g.*, *Title VII of the Civil Rights Act of 1964—Burden of Proof; Disparate Impact*, OH. EMPL. PRAC. L. § 2:16 (2019).

133. *See, e.g.*, B.E. Witkin, *Economic Criteria and Disparate Impact*, 8 WITKIN SUM. 11TH CONST. L. § 1012 (2020).

134. *See* Alisa Tiwari, *Disparate-Impact Liability for Policing*, 129 YALE L.J. 252 (2019).

135. McDonnell Douglas Corp. v. Green, 411 U.S. 792, 802–04 (1973).

136. Stephen R. McAllister & Peyton H. Robinson, *The Potential Civil Liability of Law Enforcement Officers and Agencies*, 67 J. KAN. B. ASS'N 14, 22 (1998).

the "deprivation of any rights, privileges, or immunities secured by the Constitution and laws."[137]

The protections extended under § 1983 are inherently linked to other laws through the language "secured by the Constitution and laws."[138] An aggrieved plaintiff must pinpoint a violation of either one of their constitutional rights or a right granted by statute to have a chance of prevailing in their § 1983 claim.[139] In terms of police use of investigative tools exhibiting algorithmic bias, there is no clear constitutional right to which a plaintiff suing under § 1983 can point, and only a minimal chance for a statutory right. As discussed above, in sections III(a) and III(b), the Fourth Amendment and the Equal Protection Clause—the two most likely constitutional provisions applicable to algorithmic bias—are not appropriate means for a plaintiff suing under § 1983 in those circumstances. With regard to statutory rights, a likely candidate for plaintiffs to attach their § 1983 claim is Title VI of the Civil Rights Act of 1964.

Title VI, which is codified at 42 U.S.C. § 2000d, prohibits discrimination on the basis of race, color, and national origin in programs and activities receiving federal financial assistance,[140] including many law enforcement organizations.[141] While a private citizen can link a civil claim through § 2000d, this base provision "prohibits only intentional discrimination."[142] Government agencies can promulgate regulations under § 2000d-1 that "may validly proscribe activities that have a disparate impact on racial groups, even though such activities are permissible under" § 2000d.[143] Unfortunately, the Supreme Court determined that private individuals may not sue to enforce disparate-impact regulation promulgated through § 2000d-1.[144] This ruling leaves private actors with no clear method to combat police use of investigative tools

137. 42 U.S.C. § 1983.

138. *Id.*

139. Martin A. Schwartz, *Introduction: Section 1983 Rights Are "Personal"*, SEC. 1983 LITIG. CLAIMS & DEFENSES § 3.01 (4th ed. 2020).

140. 42 U.S.C. § 2000d.

141. INIMAI CHETTIAR, LAUREN-BROOKE EISEN & NICOLE FORTIER, BRENNAN CTR. FOR JUST., REFORMING FUNDING TO REDUCE MASS INCARCERATION 3 (2013) ("Washington spends billions of dollars each year to subsidize state and local criminal justice systems. Specifically, the Justice Department administers dozens of criminal justice grants. In 2012, just some of the largest programs, including the Community Oriented Policing Services and Violence Against Women Act grants, received more than $1.47 billion.").

142. Alexander v. Sandoval, 532 U.S. 275, 280 (2001).

143. *Id.* at 281.

144. *Id.* at 282.

exhibiting algorithmic bias. Although § 2000d-1 cannot assist private actors in their complaints, it does provide a potential course for federal departments and agencies to regulate police use of investigative tools exhibiting algorithmic bias through disparate impact regulation.

Part IV: Novel Legislative Responses to Law Enforcement Use of FRT and Algorithmic Bias

A. Moratoriums on Law Enforcement Use of FRT and Legislators' Expressed Concerns

Concerns about law enforcement use of FRT has led several municipalities to pass moratoriums, or outright bans, on law enforcement's use of the technology to pursue suspects or monitor crowds.[145] In May 2019, San Francisco became the first U.S. city to ban law enforcement use of FRT.[146] Advocates for the ban stated FRT "as it exists today is unreliable, and represent[s] an unnecessary infringement on people's privacy and liberty."[147] Additionally, advocates for the ban argued FRT is "error prone, particularly when dealing with women or people with darker skin."[148] The lead sponsor for a similar piece of legislation, which passed in Somerville, Massachusetts near the end of 2019, stated many of his constituents "are worried about the consequences of [FRT] whose capabilities are outpacing the public's understanding of its power."[149] A small but growing number of cities have passed similar bans as San Francisco and Somerville.[150]

---

145. *See* Nicole Martin, *The Major Concerns Around Facial Recognition Technology*, FORBES (Sept. 25, 2019), https://www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology/#256162984fe3 [perma.cc/BA6V-LFEL].

146. Dave Lee, *San Francisco Is First US City to Ban Facial Recognition*, BBC (May 14, 2019), https://www.bbc.com/news/technology-48276660 [perma.cc/5W6X-ASH4].

147. *Id.*

148. *Id.*

149. Sarah Wu, *Somerville City Council Passes Facial Recognition Ban*, BOSTON GLOBE (June 27, 2019), https://www.bostonglobe.com/metro/2019/06/27/somerville-city-council-passes-facial-recognition-ban/SfaqQ7mG3DGulXonBHSCYK/story.html [perma.cc/RL5E-PN9T].

150. *See* Nikolas DeCosta-Klipa, *Cambridge Becomes the Largest Massachusetts City to Ban Facial Recognition*, BOSTON (Jan. 14, 2020), https://www.boston.com/news/local-news/2020/01/14/cambridge-facial-recognition [perma.cc/JL76-G7Z3]; Sarah Ravani, *Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns*, S.F. CHRON. (July 17, 2019), https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php#:~:text=The# [perma.cc/XHQ2-4CV5].

Concern about the proliferation of FRT is a surprisingly bipartisan issue considering our polarizing time.[151] Democrats have shown apprehension toward FRT due to FRT's algorithmic bias.[152] Senator Cory Booker clearly expressed this concern in proposing the "No Biometric Barriers to Housing Act" when he stated "[u]sing facial recognition technology in public housing without fully understanding its flaws and privacy implications seriously harms our most vulnerable communities . . . ."[153] Republicans have concerns about government expansion, a sentiment made clear by a spokesperson for Rep. Jim Jordan, who stated "[f]acial recognition is concerning from the perspective of government having too much power . . . . It's an instinctive civil libertarian and constitutionalist perspective."[154] These bipartisan concerns demonstrate both the breadth of unease towards FRT as well as the real possibility of a joint, productive legislative response to FRT at the federal level.

B. Algorithmic Accountability Laws: Bringing Machine Bias into the Light

For many years, companies and law enforcement agencies operated and distributed their FRT programs in a secretive way.[155] Only recently have companies and law enforcement agencies become slightly more transparent when it comes to their relationship and the joint use of FRT.[156] A recent troubling example

---

151. *See* Shirin Ghaffary, *How Facial Recognition Became the Most Feared Technology in the US*, VOX: RECODE (Aug. 9, 2019) https://www.vox.com/recode/2019/8/9/20799022/facial-recognition-law [perma.cc/EV9E-2CCR].

152. *See, e.g.*, Chris Mills Rodrigo, *Booker Introduces Bill Banning Facial Recognition Tech in Public Housing*, THE HILL (Nov. 1, 2019), https://thehill.com/policy/technology/468582-booker-introduces-bill-banning-facial-recognition-tech-in-public-housing [perma.cc/34UR-6DKE] ("Sen. Cory Booker (D-N.J.) on Friday introduced a bill banning the use of facial recognition technology in public housing, mirroring legislation proposed in the House in July . . . . [House legislation was] introduced by Reps. Yvette Clarke (D-N.Y.), Ayanna Pressley (D-Mass.) and Rashida Tlaib (D-Mich.) . . . .").

153. *Id.*

154. Ghaffary, *supra* note 151.

155. *Accord* Amrita Khalid, *Microsoft and Amazon Are at the Center of an ACLU Lawsuit on Facial Recognition*, QUARTZ (Nov. 4, 2019), https://qz.com/1740570/aclu-lawsuit-targets-amazons-rekognition-and-microsofts-azure/ [perma.cc/UWB7-KBR4] ("The government has not disclosed which companies are providing these dystopian tools to spy on the public.").

156. *Cf.* Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. TIMES (Feb. 10, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [perma.cc/7SL8-YWKC] (documenting an investigation into a company that sells FRT, which at first remained very private but eventually has been more willing to discuss their software with journalists).

of this secrecy, and at times overt deception, is the small tech start-up called Clearview AI.[157] Clearview AI devised a groundbreaking facial recognition app, which became subject to public scrutiny in January 2020 after the publication of a New York Times article by technology reporter Kashmir Hill.[158] Despite having limited knowledge about how Clearview AI works or who is behind it, hundreds of law enforcement agencies have begun using Clearview AI.[159] Clearview AI has now been shown to purposefully obfuscate investigations into its practices and to deceive its partners.[160] As Hill was investigating Clearview AI, it became apparent that Clearview AI was purposefully trying to inhibit her from finding information.[161] Additionally, Clearview AI has claimed that they only intend to provide their powerful tool to law enforcement agencies, but ample reporting has demonstrated this is untrue.[162] In response to public outcry, Clearview AI has tried to display more transparency. One such effort included Clearview AI releasing a study that claims they found no algorithmic bias in their system,[163]

---

157. *Id.*

158. *Id.*

159. *Id.* ("Federal and state law enforcement officers said that while they had only limited knowledge of how Clearview works and who is behind it, they had used its app to help solve shoplifting, identity theft, credit card fraud, murder and child sexual exploitation cases . . . . But without public scrutiny, more than 600 law enforcement agencies have started using Clearview in the past year, according to the company, which declined to provide a list.").

160. *Id.*

161. The Daily, *The End of Privacy as We Know It*, N.Y. TIMES, at 11:08 (Feb. 10, 2020) https://www.nytimes.com/2020/02/10/podcasts/the-daily/facial-recognition-surveillance.html? [perma.cc/KG6E-PJYZ] (describing how Clearview AI specifically made it so no facial recognition matches would appear when law enforcement searched for Kashmir Hill and that Clearview AI would call law enforcement agents if they ran a search for her).

162. *See, e.g.*, Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, N.Y. TIMES (Mar. 6, 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html [perma.cc/R3KP-UL7Q] ("[F]or more than a year before the company became the subject of public scrutiny, the app had been freely used in the wild by the company's investors, clients and friends. Those with Clearview logins used facial recognition at parties, on dates and at business gatherings, giving demonstrations of its power for fun or using it to identify people whose names they didn't know or couldn't recall."); Caroline Haskins, Ryan Mac & Logan McDonald, *Clearview's Facial Recognition App Has Been Used By the Justice Department, ICE, Macy's, Walmart, and the NBA*, BUZZFEED NEWS (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement [perma.cc/K5YJ-P5YP] ("Clearview AI has also been aggressively pursuing clients in industries such as law, retail, banking, and gaming and pushing into international markets . . . .").

163. Caroline Haskins, Ryan Mac & Logan McDonald, *The ACLU Slammed a Facial Recognition Company that Scrapes Photos from Instagram and Facebook*,

however some groups have taken issue with the methodology used in these self-evaluations and call for third-party oversight.[164]

Cases of private companies, like Clearview AI, falsely claiming to self-regulate have caused some lawmakers to demand more transparency and accountability for the implementation of increasingly common algorithmic systems.[165] One method of legislating the AI field is the use of "Algorithmic Impact Statements," similar to environmental impact statements, which demand private organizations and government agencies to self-evaluate the efficacy and potential discriminatory effects of their algorithms.[166] In April 2019, three members of Congress proposed the first federal legislation following the Algorithmic Impact Statement Model.[167] Their bill, titled the Algorithmic Accountability Bill of 2019, would authorize the Federal Trade Commission (FTC) to create regulations requiring companies under its jurisdiction to conduct impact assessments of highly sensitive automated decision systems.[168] In supporting the bill, Representative Yvette D. Clark stated that "[a]lgorithms shouldn't have an exemption from our anti-discrimination laws. Our bill recognizes that algorithms have authors, and without diligent oversight, they can reflect the biases of those behind the keyboard."[169]

The Algorithmic Accountability Bill of 2019 would only cover private companies through the FTC's oversight capacity,[170] but subsequent legislation has been introduced to address government use of algorithms. One example in the field of law enforcement is Representative Mark Takano's Justice in Forensic Algorithms Act.[171] In expressing concern for criminal defendants' due process rights, Representative Takano has stated:

> Forensic algorithms are black boxes, and we need to be able to look inside to understand how the software works and to give

---

BUZZFEED NEWS (Feb. 10, 2020), https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-accurate-aclu-absurd [perma.cc/4LFB-4SD9].

164. *Id.*

165. *See* Press Release, U.S. Sen. Cory Booker of N.J., Booker, Wyden, Clarke Introduce Bill Requiring Companies to Target Bias in Corporate Algorithms (Apr. 10, 2019), https://www.booker.senate.gov/?p=press_release&id=903 [perma.cc/U8XT-35GU].

166. Selbst, *supra* note 95, at 110.

167. Press Release, U.S. Sen. Cory Booker, *supra* note 165.

168. Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong. (2019).

169. Press Release, U.S. Sen. Cory Booker, *supra* note 165.

170. Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong. (2019).

171. Justice in Forensic Algorithms Act of 2019, H.R. 4368, 116th Cong. (2019).

> defendants the ability to challenge them. My legislation will open the black box of forensic algorithms and establish standards that will safeguard our Constitutional right to a fair trial.[172]

Notably, the Justice in Forensic Algorithms Act would amend the Federal Rules of Evidence to prohibit the use of trade secret privileges to prevent defendants from accessing algorithms used in their prosecution.[173] The Justice in Forensic Algorithms Act would also direct NIST to establish Computational Forensic Algorithms Standards and a Computational Forensic Algorithms Testing Program.[174] In developing these standards, NIST would be directed to consider a variety of factors including algorithms' potential for disparate impact across protected classes in standards and testing.[175] After NIST establishes their standards, federal law enforcement would then be required to follow them.[176] These pieces

---

172. Press Release, U.S. Congressman Mark Takano of Cal.'s 41st Dist., Rep. Takano Introduces the Justice in Forensic Algorithms Act to Protect Defendants' Due Process Rights in the Criminal Justice System (Sept. 17, 2019), https://takano.house.gov/newsroom/press-releases/rep-takano-introduces-the-justice-in-forensic-algorithms-act-to-protect-defendants-due-process-rights-in-the-criminal-justice-system [perma.cc/K38E-32MN].

173. The bill provides:

> In any criminal case, evidence that is the result of analysis by computational forensic software is admissible only if—
>
> (1) the computational forensic software used has been submitted to the Computational Forensic Algorithm Testing Program of the Director of the National Institute of Standards and Technology and there have been no material changes to that software since it was last tested; and
>
> (2) the developers and users of the computational forensic software agree to waive any and all legal claims against the defense or any member of its team for the purposes of the defense analyzing or testing the computational forensic software.

Justice in Forensic Algorithms Act of 2019, H.R. 4368, 116th Cong. (2019).

174. Press Release, U.S. Congressman Mark Takano, *supra* note 172.

175. *Id.* ("In developing standards NIST is directed to: collaborate with outside experts in forensic science, bioethics, algorithmic discrimination, data privacy, racial justice, criminal justice reform, exonerations, and other relevant areas of expertise identified through public input; address the potential for disparate impact across protected classes in standards and testing; and gather public input for the development of the standards and testing program and publicly document the resulting standards and testing of software.").

176. Justice in Forensic Algorithms Act of 2019, H.R. 4368, 116th Cong. (2019) ("Any Federal law enforcement agency or crime laboratory providing services to a Federal agency using computational forensic software may use only software that has been tested under the National Institute of Standards and Technology's Computational Forensic Algorithm Testing Program and shall conduct an internal validation according to the requirements outlined in the Computational Forensic Algorithm Standards and make the results publicly available. The internal validation shall be updated when there is a material change in the software that triggers a retesting by the Computational Forensic Algorithm Testing Program.").

of proposed legislation allow for some degree of oversight, but as of the writing of this Note it is unclear if they will actually become law.

C. Legislative Suggestions from Scholars on FRT and Algorithmic Bias

University-affiliated experts[177] and non-profit groups[178] have drafted model legislation calling for a variety of reforms related to the use of algorithms generally and specifically as they apply to FRT. Clare Garvie, a senior associate at the Georgetown University Center on Privacy and Technology, believes a moratorium on the use of FRT should be put in place until FRT regulations are passed requiring "minimum photo quality standards, accuracy testing, and publicly available reports . . . on how the government uses facial recognition tech."[179] Garvie further calls for a private right of action if law enforcement did not follow these best practices.[180] In addition to suggesting formal legislation, Garvie also provided a list of thirty recommendations for a variety of actors involved in the production, utilization, and potential regulation of FRT.[181] Of note, Garvie recommended that NIST "[r]egularly include tests for algorithmic bias along the lines of race, gender, and age in facial recognition competitions," along with four other recommendations for NIST.[182]

Kartik Hosanagar, a University of Pennsylvania technology professor, takes a more expansive view on algorithmic accountability. Hosanagar proposes an "Algorithmic Bill of Rights" to manage the many risks and benefits that come with continued proliferation of algorithms in the United States' most vital

177. GARVIE ET AL., *supra* note 17, at 102–19.

178. *Community Control over Police Surveillance*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance?redirect=feature/community-control-over-police-surveillance [perma.cc/5UJV-5H33].

179. Khari Johnson, *Facial Recognition Regulation Is Surprisingly Bipartisan*, VENTURE BEAT (Nov. 11, 2019), https://venturebeat.com/2019/11/11/facial-recognition-regulation-is-surprisingly-bipartisan/ [perma.cc/7NQB-X9JG].

180. GARVIE ET AL., *supra* note 17, at 114 ("Any person who is subject to targeted identification or attempted identification through targeted continuous face recognition in violation of this Act may in a civil action recover from the [state] investigative or law enforcement officer or the state or [federal law] enforcement agency which engaged in that violation such relief as may be appropriate.") (alterations in original).

181. *Id.* at 62–71.

182. *See also id.* ("Recommendation 24: Increase the frequency of face recognition competitions, ideally testing on an annual or biennial basis . . . . Recommendation 25: Continue to update tests to reflect state-of-the-art advances in face recognition and mobile biometrics . . . . Recommendation 26: Develop tests that closely mirror law enforcement workflows, and issue best practices for accuracy testing . . . . Recommendation 27: Develop and distribute diverse datasets of photos.").

systems.[183] Sigal Samuel from Vox News spoke with ten experts in the field of AI, including Kartik Hosanagar and Joy Buolamwini,[184] to compose a formal list of ten rights Americans would have under an "Algorithmic Bill of Rights."[185] This composite of rights echoes the themes of transparency and redress emphasized in the proposed Algorithmic Accountability Act of 2019 and the Justice in Forensic Algorithms Act of 2019. Two specific rights proposed—"Freedom from Bias"[186] and "Independent Oversight"[187]—are critical to the management of algorithmic bias and FRT. The two rights would ensure algorithms were regularly tested for bias and that the tests were performed by third-party organizations in real-world situations.[188] This collaborative list from a variety of concerned experts in the field of AI could provide legislators with a substantial framework for future legislative proposals.

Part V: Finding the Balance Between Investigative Advancements and Civil Liberties

Like forensic DNA before it, FRT will revolutionize law enforcement's investigative effectiveness.[189] Law enforcement's increased capacity to identify, and potentially locate, suspects with only a photo or a still image from a video is expected to lead to an increase in the apprehension of evasive criminals,[190] prevention of

183. KARTIK HOSANAGAR, A HUMAN'S GUIDE TO MACHINE INTELLIGENCE: HOW ALGORITHMS ARE SHAPING OUR LIVES AND HOW WE CAN STAY IN CONTROL 218 (2019).

184. *See generally* Buolamwini & Gebru, *supra* note 14.

185. Sigal Samuel, *10 Things We Should All Demand from Big Tech Right Now*, VOX (May 29, 2019), https://www.vox.com/the-highlight/2019/5/22/18273284/ai-algorithmic-bill-of-rights-accountability-transparency-consent-bias [https://web.archive.org/web/20201107235745/https://www.vox.com/the-highlight/2019/5/22/18273284/ai-algorithmic-bill-of-rights-accountability-transparency-consent-bias].

186. *Id.* ("We have the right to evidence showing that algorithms have been tested for bias related to race, gender, and other protected characteristics — before they're rolled out. The algorithms must meet standards of fairness and nondiscrimination and ensure just outcomes.").

187. *Id.* ("We have the right to expect that an independent oversight body will be appointed to conduct retrospective reviews of algorithmic systems gone wrong. The results of these investigations should be made public.").

188. *Id.* ("Eric Topol, a physician and the author of *Deep Medicine*, told me too many algorithms are validated only on computers, not in real-world clinical environments. 'We have already learned that there is a chasm between the accuracy of an algorithm, especially determined this way, and a favorable impact on clinical outcomes' he said, explaining that just because an algorithm appears to work great in a computer simulation doesn't mean it'll work as intended in all doctors' offices.").

189. Tracy & Morgan, *supra* note 59.

190. O'Neill, *supra* note 67.

acts of mass violence,[191] and recovery of victims of human trafficking.[192] As with most law enforcement processes, the express intent of law enforcement's increased reliance on FRT is to protect our society and achieve a feeling of justice for the victims of criminal behavior.[193] However, these intended objectives need to be reconciled with the fact that powerful police efforts often affect historically marginalized communities more than others.[194] Although law enforcement may have the best of intentions, human

191. Ivan Moreno, *AI-Powered Cameras Become New Tool Against Mass Shootings*, ABC NEWS (Aug. 30, 2019), https://abcnews.go.com/Technology/wireStory/threat-mass-shootings-give-rise-ai-powered-cameras-65285382 [perma.cc/P2CC-T35E] ("There was no threat, but Hildreth's demonstration showed what's possible with AI-powered cameras. If a gunman were in one of his schools, the cameras could quickly identify the shooter's location and movements, allowing police to end the threat as soon as possible, said Hildreth, emergency operations coordinator for the Fulton County School District. AI is transforming surveillance cameras from passive sentries into active observers that can identify people, suspicious behavior and guns, amassing large amounts of data that help them learn over time to recognize mannerisms, gait and dress. If the cameras have a previously captured image of someone who is banned from a building, the system can immediately alert officials if the person returns. At a time when the threat of a mass shooting is ever-present, schools are among the most enthusiastic adopters of the technology . . . .").

192. Tom Simonite, *How Facial Recognition Is Fighting Child Sex Trafficking*, WIRED (June 19, 2019), https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/ [perma.cc/NTN6-JTYZ] ("One evening in April, a California law enforcement officer was browsing Facebook when she saw a post from the National Center for Missing and Exploited Children with a picture of a missing child. The officer took a screenshot of the image, which she later fed into a tool created by nonprofit Thorn to help investigators find underage sex-trafficking victims. The tool, called Spotlight, uses text- and image-processing algorithms to match faces and other clues in online sex ads with other evidence. Using Amazon's facial recognition technology, Spotlight quickly returned a list of online sex ads featuring the girl's photo. She had been sold for weeks. The ads set in motion some more traditional police work. 'Within weeks that child was recovered and removed from trauma,' Julie Cordua, CEO of Thorn, said, recounting the case at an Amazon conference in Las Vegas this month.").

193. O'Neill, *supra* note 67.

194. Selbst, *supra* note 95 at 119–20 ("Police act with incredible discretion. They choose where to focus their attention, who to arrest, and when to use force. They make many choices every day regarding who is a suspect and who appears to be a criminal. Examined in the aggregate, all of those choices exhibit disproportionate impacts on poor people and people of color. This is the result of bias built into policing as an institution, as well as unconscious biases of individual police officers. Thus, where police use predictive policing technology, the purpose is not only to detect hidden patterns, but also to inject a 'neutral,' data-driven tool into the process to prevent unconscious police biases from entering the equation. Predictive policing promises both to provide auditable methods that will prevent invidious intentional discrimination and to mitigate the unconscious biases attending police officers' daily choices. But at the moment, such a promise amounts to little more than a useful sales tactic.").

implicit bias, and now algorithmic bias, can result in atrocious disparities and mistreatment.[195]

The Equal Protections Clause's jurisprudence, as it currently stands, is not designed to remedy the modern problem of police use of systems containing algorithmic bias. The requirement to prove discriminatory intent under the Equal Protection Clause makes it difficult to apply to a seemingly unintended and unexpected source of discrimination, namely algorithmic bias.[196] The misleading perception that machines are inherently objective and "infallible"[197] further complicates this issue and may actually conceal discriminatory human intent behind mechanical objectivity.[198]

The Fourth Amendment also does not appear to be a likely avenue to address algorithmic bias. The Court's decision in *Whren v. United States* makes it clear that the Fourth Amendment's probable cause analysis should not factor in an officer's subjective intent.[199] The Court's ruling in *Whren* makes it appear that discriminatory undertones have no role in determining the presence of a Fourth Amendment violation.[200] However, algorithmic bias may affect the Fourth Amendment's probable cause analysis by drawing into question the reliability of FRT matches in meeting the necessary standard of proof.[201] Police use of FRT matches could be compared to the police consulting with an informant known to be unreliable.[202] However, because the Fourth Amendment's probable cause analysis is so flexible, it is unlikely judges will find an FRT match, combined with other minor information, does not reach the level of probable cause, even given FRT's algorithmic bias.[203]

Legislative or agency action is the most fitting way to address the quickly evolving prospects associated with law enforcement's increased use of FRT because of the adaptive approach these routes can provide. Constitutional solutions, even if they were viable, may be too rigid to appropriately balance the nuanced and ever-changing

195. *Id.*

196. *See* Vill. of Arlington Heights v. Metro. Hous. Dev. Corp., 429 U.S. 252, 264–65 (1977) (noting that *Washington v. Davis*, 426 U.S. 229 (1976), has been repeatedly relied on to reaffirm the need for "proof of racially discriminatory intent or purpose" in a variety of contexts).

197. Desai & Kroll, *supra* note 20.

198. *See* Buolamwini & Gebru, *supra* note 14.

199. 517 U.S. 806, 813 (1996).

200. *Id.*

201. *See* Illinois v. Gates, 462 U.S. 213, 232 (1983) (discussing the standard of proof for finding probable cause).

202. *See, e.g.*, Florida v. J.L., 529 U.S. 266, 270 (2000).

203. *See Gates*, 462 U.S. at 232.

interests at play with law enforcement's use of FRT.[204] The Court has admitted when discussing the canon of constitutional avoidance that settling an issue through a constitutional decision can limit legislative flexibility.[205] Additionally, if the legislature assigned regulatory power to an executive agency, as proposed in the Algorithmic Accountability Bill of 2019[206] or the Justice in Forensic Algorithms Bill of 2019,[207] then the assigned agency could use its expertise to generate fitting responses to advancements in technology and investigative tactics.[208]

Specifically, NIST must have the authority to set clear standards about algorithmic bias and FRT specifically, which federal law enforcement and local law enforcement receiving federal funds would be required to follow. It is in the best interest of the United States for Congress to follow the suggestions of Representative Mark Takano[209] and Clare Garvie[210] in assigning power to NIST. As algorithms proliferate in American society, and more concerningly, the criminal justice system, there needs to be a central regulator that guides these rapid advancements. NIST has made some advancements in this role through studies like the Facial Recognition Vendor Test, which showed the majority of FRT programs exhibit bias.[211] However, NIST needs greater authority to act on these sorts of findings. For example, NIST should be able to: (1) mandate federal law enforcement to use those FRT programs that exhibit the lowest demographically-based error rate;[212] (2) draft strict protocol outlining best practices for law enforcement use of FRT;[213] (3) perform regular audits of law enforcement use of FRT;[214] and (4) require law enforcement agencies to be transparent

204. *See* NLRB v. Catholic Bishop of Chi., 440 U.S. 490, 508–09 (1979) (Brennan, J., dissenting).

205. *See id.* at 509 (quoting Yu Cong Eng v. Trinidad, 271 U.S. 500, 518 (1926)) ("[A]mendment may not be substituted for construction, and that a court may not exercise legislative functions to save [a] law from conflict with constitutional limitation.").

206. Press Release, U.S. Sen. Cory Booker, *supra* note 165.

207. Press Release, U.S. Congressman Mark Takano, *supra* note 172.

208. *See generally* Mark Seidenfeld, *Bending the Rules: Flexible Regulation and Constraints on Agency Discretion*, 51 ADMIN. L. REV. 429 (Spring 1999).

209. Press Release, U.S. Congressman Mark Takano, *supra* note 172.

210. GARVIE ET AL., *supra* notes 17, 180–182.

211. GROTHER ET AL., *supra* note 43 (finding bias in the form of demographic differentials in contemporary face recognition algorithms).

212. *See id.*

213. GARVIE ET AL., *supra* note 17.

214. Justice in Forensic Algorithms Act of 2019, H.R. 4368, 116th Cong. (2019).

in their use of FRT and their partnerships with manufacturers.[215] NIST could also use 42 U.S.C. § 2000d-1 to establish regulations that would allow NIST to enforce disparate impact theories related to FRT. Until this sort of authority is given to a responsible government agency or the legislature imposes some clear regulatory system, we are left hoping that FRT companies and law enforcement behave themselves,[216] because existing legal frameworks are not suitable to this new wave of invasive discrimination.[217]

Conclusion

Law and technology have always been engaged in a cat and mouse chase, with law unsuccessfully trying to catch up to advancements in technology. FRT and algorithmic bias are some of the most recent examples of technology evolving just outside the reach of judicial precedent. The more adaptive portions of government, namely the legislature and government agencies, need to work towards creating a comprehensive framework to deal with FRT and algorithmic bias before the proliferation of these systems reaches a critical mass. There are examples worldwide of countries

---

215. Samuel, *supra* note 185 ("We have the right to know when an algorithm is making a decision about us, which factors are being considered by the algorithm, and how those factors are being weighted.").

216 *Compare* 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), https://www.businessinsider.com/amazon-microsoft-ibm-halt-selling-facial-recognition-to-police-2020-6 [https://perma.cc/WYJ4-8JNQ] ("Three of the world's biggest tech companies have backed off selling facial recognition to law enforcement amid ongoing protests against police brutality."), *with* Julia Horowitz, *Tech Companies Are Still Helping Police Scan Your Face*, CNN BUS. (July 3, 2020) https://www.cnn.com/2020/07/03/tech/facial-recognition-police/index.html#:~:text=Tech%20companies%20are%20still%20helping%20police%20scan%20your%20face&text=As%20Black%20Lives%20Matter%20protests [https://perma.cc/DAS2-A62R] ("[IBM, Amazon, and Microsoft] aren't the top suppliers of facial recognition software used by law enforcement, meaning police departments will still be able to buy from plenty of vendors. Clearview AI, Japan's NEC and Ayonix, Germany's Cognitec and Australia's iOmniscient have all said they intend to maintain their relationships with US police forces.").

217 Hamilton *supra* note 216 ("'From a US perspective, these announcements confirm the serious harm that unregulated facial recognition technology in the hands of law enforcement has already caused Black and other [minority] groups to suffer' . . . [Dr. Nakeema Stefflbauer] added: 'In my opinion, this is the moment when US and EU governments must take technology regulation seriously and pass comprehensive legislation: failure to do so is nothing less than giving permission for an unchecked assault on human rights.'").

already using FRT at a near dystopian level.[218] In the United States, we need to cultivate an adaptive legal framework before FRT, and its underlying algorithmic bias, get further out of hand.[219] Proactive solutions, like the proposed and model legislation described above, must be instituted to reduce the gap between legal theory and technological realities.

218. Emily Feng, *How China Is Using Facial Recognition Technology*, NPR (Dec. 16, 2019), https://www.npr.org/2019/12/16/788597818/how-china-is-using-facial-recognition-technology [perma.cc/QN64-P2PB] ("In the dataset Wethington found, people were indexed by information, like their criminal history, with facial recognition data, like if they were bearded or wearing a mask, and even what ethnicity they were, Han, the ethnic majority here in China, or Uighur, a predominantly Muslim ethnic minority China has detained by the hundreds of thousands in the region of Xinjiang in the name of anti-terrorism."); Kelvin Chan, *UK Police Use of Facial Recognition Tests Public's Tolerance*, ABC NEWS (Jan. 16, 2020), https://abcnews.go.com/Technology/wireStory/uk-police-facial-recognition-tests-publics-tolerance-68321764 [perma.cc/BD28-5PJD] ("Police in Britain are testing the real-time use of facial recognition to scan crowds for wanted people and then detain any suspects for questioning. . . . The real-time surveillance being tested in Britain is among the more aggressive uses of facial recognition in Western democracies and raises questions about how the technology will enter people's daily lives."); Laura Mackenzie, *Surveillance State: How Gulf Governments Keep Watch on Us*, WIRED (Jan. 21, 2020), https://wired.me/technology/privacy/surveillance-gulf-states/ [perma.cc/49XE-JXX5] ("[Dubai] police have been rolling out a program called Oyoon (Eyes) that implements facial recognition technology and analysis across the city. They basically have thousands of video feeds from cameras across the emirate that feed back into a central command center.").

219. Lane Brown, *There Will Be No Turning Back on Facial Recognition*, N.Y. MAG: INTELLIGENCER (Nov. 12, 2019), https://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html [perma.cc/WH3Z-W35Z] ("We also heard that spooked lawmakers banned police use of facial recognition in Oakland; Berkeley; Somerville, Massachusetts; and San Francisco, of all places, where Orwellian tech products are the hometown industry. But everywhere else and in all other contexts, facial recognition is legal and almost completely unregulated—and we heard that it's already being used on us in city streets, airports, retail stores, restaurants, hotels, sporting events, churches, and presumably lots of other places we just don't know about.").