



Spring 2022

The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest

T.J. Benedict

Washington and Lee University School of Law, benedict.t22@law.wlu.edu

Follow this and additional works at: <https://scholarlycommons.law.wlu.edu/wlulr>



Part of the [Civil Rights and Discrimination Commons](#), [Criminal Law Commons](#), [Criminal Procedure Commons](#), [Evidence Commons](#), [Fourth Amendment Commons](#), [Law Enforcement and Corrections Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

T.J. Benedict, *The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest*, 79 Wash. & Lee L. Rev. 849 (2022).

Available at: <https://scholarlycommons.law.wlu.edu/wlulr/vol79/iss2/7>

This Note is brought to you for free and open access by the Washington and Lee Law Review at Washington and Lee University School of Law Scholarly Commons. It has been accepted for inclusion in Washington and Lee Law Review by an authorized editor of Washington and Lee University School of Law Scholarly Commons. For more information, please contact christensena@wlu.edu.

The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest

T.J. Benedict*

Abstract

Facial recognition technology (FRT) is a popular tool among police, who use it to identify suspects using photographs or still-images from videos. The technology is far from perfect. Recent studies highlight that many FRT systems are less effective at identifying people of color, women, older people, and children. These race, gender, and age biases arise because FRT is often “trained” using non-diverse faces. As a result, police have wrongfully arrested Black men based on mistaken FRT identifications. This Note explores the intersection of facial recognition technology and probable cause to arrest.

Courts rarely, if ever, examine FRT’s role in establishing probable cause. This Note suggests a framework for how courts can evaluate FRT and probable cause. Case law about drug-sniffing dogs provides a starting point for assessing what role an FRT identification should play in probable cause determinations. But drug dogs are not a perfect analogue for FRT. Two important differences between these two policing tools warrant treating FRT with greater scrutiny than drug dogs. First, FRT has baked-in racial, gender, and age biases that drug dogs lack. Second, FRT is a digital policing tool, which recent

* J.D. Candidate, Class of 2022, Washington and Lee University School of Law; Class of 2017, University of Richmond. Thank you, Professor Alex Klein, for your guidance and insight during all stages of the Note writing process. I’m also grateful to the *W&L Law Review* upper board for their meticulous work and thoughtful editing. Finally, thank you to my parents for your constant support.

Supreme Court precedent suggests merits more judicial scrutiny than non-digital police tools like dogs.

Giving FRT a closer look leads to the conclusion that an FRT identification alone is insufficient to establish probable cause. FRT relies on flawed inputs (non-diverse data) that leads to flawed outputs (demographic discrepancies in misidentifications). These problematic inputs and outputs provide complimentary reasons why an FRT identification alone cannot provide probable cause.

Table of Contents

INTRODUCTION		851
I. BACKGROUND		852
A. <i>What Is Probable Cause?</i>		852
B. <i>Facial Recognition Technology: What It Is, and How Police Use It</i>		854
C. <i>The Supreme Court’s Stringent Approach to Technology in Policing</i>		863
D. <i>The Intersection of FRT and Probable Cause</i> ..		866
II. PROBABLE CAUSE AND DRUG DOGS: A STARTING POINT FOR PROBABLE CAUSE AND FRT		870
A. <i>Drug Dog Case Law Fits FRT</i>		870
B. <i>Applying Drug Dog Case Law to FRT</i>		872
III. FRT MERITS MORE SCRUTINY THAN DRUG DOGS AND SHOULD NOT BE THE SOLE SOURCE OF PROBABLE CAUSE		876
A. <i>Differences Between FRT and Drug Dogs Call for Heightened Judicial Scrutiny</i>		876
1. <i>Race, Gender, and Age Biases Hamper FRT Differently than Drug Dogs</i>		876
2. <i>Digital Policing Tools Like FRT Deserve More Scrutiny than Analog Policing Tools Like Drug Dogs</i>		878
B. <i>An FRT Match Alone Cannot Provide Probable Cause</i>		880
1. <i>Garbage in, Garbage out: Flawed Data, Police Databases, and Probable Cause</i>		880
a. <i>Supreme Court Scrutiny of Police Databases</i>		881

<i>b. Federal Appellate Court Scrutiny of Police Databases</i>	886
2. Race, Gender, and Age Biases	889
3. Public Support for Curtailing FRT in Probable Cause Cases	894
CONCLUSION.....	896

INTRODUCTION

Detroit police arrested Robert Julian-Borchak Williams for a robbery he did not commit.¹ Facial recognition technology (FRT) falsely matched surveillance footage of a culprit’s face to Williams’s driver’s license photo.² After being detained for thirty hours, Williams confronted two detectives on the obvious difference in appearance between himself and the alleged robber.³ One detective turned to the other and said, “I guess the computer got it wrong.”⁴ A prosecutor ultimately dismissed Williams’s case,⁵ but an important question remains: What role did FRT play in establishing probable cause to arrest Williams?

Williams’s case is not unique. FRT misidentifications led to at least two other wrongful arrests in 2019 and 2020.⁶ There are likely many more unreported wrongful arrests, given FRT’s prominence in American policing and the risk of overreliance on FRT due to automation bias.⁷ More than 800 law enforcement agencies across the country conduct thousands of FRT searches

1. Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020) [hereinafter Hill, *Wrongfully Accused*], <https://perma.cc/9W8L-RPRB> (last updated Aug. 3, 2020).

2. *Id.*

3. *Id.*

4. *Id.*

5. *Id.*

6. Anderson Cooper, *Police Departments Adopting Facial Recognition Tech Amid Allegations of Wrongful Arrests*, CBS NEWS (May 16, 2021, 7:08 PM), <https://perma.cc/V3CB-3DGK>.

7. *See id.* (providing the statement of Clare Garvie, an attorney at Georgetown’s Center on Privacy and Technology, that “I have every reason to believe there are more [wrongful arrests]”).

each year.⁸ Courts provide little to no supervision over FRT in policing, especially when police use FRT to establish probable cause.⁹ This lack of judicial oversight opens the door to more citizens ending up in handcuffs because an algorithm mistakenly placed them at a crime scene.¹⁰

This Note presents a framework for assessing FRT's role in probable cause inquiries. Part I provides background on the probable cause standard, what FRT is, and how police use FRT. Part I also examines the Supreme Court's recent misgivings toward digital policing and the current legal relationship between FRT and probable cause. Part II recommends a judicial framework for examining FRT in probable cause inquiries based on *Florida v. Harris*,¹¹ a Supreme Court case explaining when drug dogs can provide probable cause. This Part argues that *Harris* provides a baseline for reviewing probable cause premised on FRT. Part III recognizes that problems that plague FRT but not drug dogs—namely bad data and demographic biases—warrant heightened judicial scrutiny of FRT. As such, this Note argues that an FRT identification, unlike a drug dog alert, should not alone establish probable cause.

I. BACKGROUND

A. *What Is Probable Cause?*

Before an officer can arrest an individual, the Fourth Amendment requires that the officer have probable cause “to believe that person committed a crime.”¹² The officer must

8. See *Atlas of Surveillance*, ELEC. FRONTIER FOUND., <https://perma.cc/TKR7-DRUR> (last updated Mar. 11, 2022) (tracking how many law enforcement agencies use FRT); Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1120 (2021) (sharing statistics about how often police conduct FRT searches).

9. See *infra* Part I.D.

10. See *infra* Part I.D.

11. 568 U.S. 237 (2013).

12. *Tennessee v. Garner*, 471 U.S. 1, 7 (1985); see U.S. CONST. amend. IV (“[N]o Warrants shall issue, but upon probable cause . . .”). The probable cause standard also applies to searches and seizures, which use a test that mirrors the test for arrests. See *United States v. Humphries*, 372 F.3d 653, 659 (4th Cir. 2004) (clarifying that, in both arrest cases and search cases, “the quantum of facts required . . . is ‘probable cause,’ and the quantum of evidence needed to constitute probable cause . . . is the same”). Accordingly, this Note

demonstrate probable cause to a magistrate judge, either via an application for an arrest warrant or during a post-arrest preliminary hearing.¹³ The Supreme Court has explained that the probable cause requirement “protects citizens from rash and unreasonable interferences with privacy and from unfounded charges of crime, while giving fair leeway for enforcing the law in the community’s protection.”¹⁴

An officer has probable cause if an “objectively reasonable”¹⁵ officer, considering the “totality of the circumstances”¹⁶ would find a “fair probability” or “substantial chance” that a particular person committed a crime.¹⁷ Probable cause does not require “an actual showing of such activity.”¹⁸ Assessing the totality of the circumstances in probable cause inquiries is “a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.”¹⁹ It is an “all-things-considered approach,”²⁰ in which judges examine “the events leading up to the arrest, and then decide whether these historical facts, viewed from the standpoint of an objectively reasonable police officer, amount to probable cause.”²¹

focuses on probable cause to arrest but relies on cases about searches and seizures.

13. See PETER G. MCCABE, A GUIDE TO THE FEDERAL MAGISTRATE JUDGE 23–25 (2016) (covering how magistrates issue warrants); *Gerstein v. Pugh*, 420 U.S. 103, 114 (1975) (“[T]he Fourth Amendment requires a judicial determination of probable cause as a prerequisite to extended restraint of liberty following arrest.”).

14. *Maryland v. Pringle*, 540 U.S. 366, 370 (2003).

15. *Id.* at 371.

16. *Florida v. Harris*, 568 U.S. 237, 244 (2013).

17. *Illinois v. Gates*, 462 U.S. 213, 238, 243 n.13 (1983); see *Pringle*, 540 U.S. at 371 (“[T]he belief of guilt must be particularized with respect to the person to be searched or seized.”).

18. *Gates*, 462 U.S. at 243 n.13.

19. *Id.* at 232.

20. *Harris*, 568 U.S. at 244.

21. *Pringle*, 540 U.S. at 371 (internal quotations omitted).

Because probable cause leads to arrest, probable cause determinations have far-reaching consequences for arrestees.²² Most seriously, wrongful arrests often lead to wrongful convictions.²³ Even without a conviction, an arrest can carry mandatory fees, trigger professional license suspensions, and lead to eviction from public housing.²⁴

B. *Facial Recognition Technology: What It Is, and How Police Use It*

FRT encompasses a broad array of technologies—from the software that unlocks cellphones to real-time facial monitoring that scans public places.²⁵ This Note concentrates on identification-focused FRT because it is the most prevalent FRT in law enforcement.²⁶ This technology attempts to match one image of a face against a collection of facial images.²⁷ For example, law enforcement agencies use FRT to try to match an image of a suspect against databases of driver’s license photos or mugshots.²⁸ Some FRT databases contain images gathered from social media or other sources without the consent of those photographed.²⁹

22. See Eisha Jain, *Prosecuting Collateral Consequences*, 104 GEO. L.J. 1197, 1206 (2016) (“From the moment of arrest, criminal records create a cascade of noncriminal consequences.”).

23. See NAT’L REGISTRY OF EXONERATIONS, ANNUAL REPORT 7 (2020), <https://perma.cc/6QL5-9884> (PDF) (counting over 2,500 exonerations for wrongful convictions between 1989 and 2019).

24. Jain, *supra* note 22, at 1206–07.

25. See Lindsey Barrett, *Ban Facial Recognition Technologies for Children—and for Everyone Else*, 26 B.U. J. SCI. & TECH. L. 223, 232 (2020) [hereinafter Barrett, *Ban Facial Recognition*] (surveying different uses of FRT); Ferguson, *supra* note 8, at 1112 (discussing the Chinese government’s facial monitoring systems).

26. Ferguson, *supra* note 8, at 1552. This Author uses “FRT” as shorthand for identification-focused FRT unless otherwise specified.

27. See *id.* at 1114 (detailing how this type of FRT “requires searching through thousands (or millions) of images for the appropriate match and finding the ‘best’ match”).

28. See *id.* at 1114–15 (cataloging various datasets police use with FRT).

29. See Olivia Solon, *Facial Recognition’s ‘Dirty Little Secret’: Millions of Online Photos Scraped Without Consent*, NBC NEWS (Mar. 12, 2019, 4:32 AM), <https://perma.cc/5E2F-XLVG> (last updated Mar. 17, 2019, 11:25 AM) (reporting that FRT increasingly uses photos that “com[e] from the internet, where they’re swept up by the millions without the knowledge of the people

FRTs perform this matching exercise using various techniques. Traditionally, FRT identifies facial features, such as the position and shape of one's nose and eyes, and then measures the distances between these features to create a digital "faceprint."³⁰ An algorithm then sets out to find a matching faceprint.³¹ Other FRTs try to match a whole face image, while some newer variants rely on "skin textures, shadows, three-dimensional models, or some combination of all of these types."³²

Some FRTs return only one image match, but many produce a lineup of possible matches that the user must examine to find the "best" match.³³ FRTs that produce multiple potential matches sometimes rank the matches by the likelihood of correct identification.³⁴ Some FRTs produce as many as fifty potential matches per search.³⁵

Researchers first developed algorithms to identify human faces during the 1990s.³⁶ Following the attacks of September 11, 2001, "[t]he federal government invested heavily in FRT," including by giving grants to state and local governments to create databases of images for FRT use.³⁷ Early FRT was not

who posted them"); Os Keyes et al., *The Government Is Using the Most Vulnerable People to Test Facial Recognition Software*, SLATE (Mar. 17, 2019, 8:32 PM), <https://perma.cc/3BHJ-GRJC> (sharing research indicating "that the U.S. government, researchers, and corporations have used images of immigrants, abused children, and dead people to test their facial recognition systems, all without consent").

30. Ferguson, *supra* note 8, at 1110–11.

31. *Id.*

32. *Id.* (footnotes omitted).

33. *Face Recognition*, ELEC. FRONTIER FOUND., <https://perma.cc/H2AJ-M33Z> (last updated Oct. 24, 2017).

34. *Id.*

35. See CLARE GARVIE ET AL., *THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA* 48, 50, 67 (2016), <https://perma.cc/QLK7-QVY2> (PDF) (highlighting an FRT system that "returns between two and 50 candidate mug shots for any given search").

36. Douglas Fretty, *Face-Recognition Surveillance: A Moment of Truth for Fourth Amendment Rights in Public Places*, 16 VA. J.L. & TECH. 430, 432 (2011).

37. Samuel D. Hodge, Jr., *Big Brother Is Watching: Law Enforcement's Use of Digital Technology in the Twenty-First Century*, 89 U. CIN. L. REV. 30, 58 (2020).

very accurate,³⁸ but the technology has notably improved over the years.³⁹

Despite recent technological advances, many FRT programs chronically misidentify people of color and, in particular, females of color, at higher rates than white people. A recent report from the National Institute of Standards and Technology (NIST) found higher rates of false positives among persons of African, Asian, and American Indian descent, as well as “[h]igher false positive identification rates in black women.”⁴⁰ Computer scientists, Dr. Joy Buolamwini and Dr. Timnit Gebru, likewise identified “intersectional error rates” that lead FRT to misidentify women of color.⁴¹ Additionally, “[w]omen invariably give higher false negative rates than men” across racial groups.⁴² In addition to race and gender biases, many FRT programs struggle to identify older people and children.⁴³

These discriminatory discrepancies in error rates stem, in part, from FRT developers training FRT using datasets of non-diverse facial images.⁴⁴ FRTs trained using non-diverse

38. See JOHN D. WOODWARD, SUPER BOWL SURVEILLANCE: FACING UP TO BIOMETRICS 3–4 (RAND 2001), <https://perma.cc/XU29-YCNY> (PDF) (recounting that, in 2001, law enforcement used “far from foolproof and not yet technically perfected” FRT on spectators at Super Bowl XXXV in Tampa, Florida); *Fretty*, *supra* note 36, at 433 (discussing studies from 2002 and 2003 that detailed FRT’s inadequacies).

39. See NAT’L INST. STANDARDS & TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 2: IDENTIFICATION 2 (2019), <https://perma.cc/R7DT-X6N9> (PDF) [hereinafter NIST PART 2] (“[M]assive gains in accuracy have been achieved in the last five years (2013–2018) and these far exceed improvements made in the prior period (2010–2013).”).

40. See NAT’L INST. STANDARDS & TECH., FACIAL RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 7–8, 63 (2019), <https://perma.cc/5JZR-ARMT> (PDF) [hereinafter NIST PART 3].

41. JOY BUOLAMWINI & TIMNIT GEBRU, GENDER SHADES: INTERSECTIONAL ACCURACY DISPARITIES IN COMMERCIAL GENDER CLASSIFICATION 10 (MIT 2018), <https://perma.cc/K9NR-QYF8> (PDF).

42. NIST PART 3, *supra* note 40, at 63.

43. See *id.* at 2 (“We found elevated false positives in the elderly and in children; the effects were larger in the oldest and youngest, and smallest in middle-aged adults.”).

44. See BUOLAMWINI & GEBRU, *supra* note 41, at 1 (“It has recently been shown that algorithms trained with biased data have resulted in algorithmic discrimination . . .” (citations omitted)); NIST PART 3, *supra* note 40, at 10 (recommending “more diverse training data” to remedy demographic differences in FRT error rates).

faces struggle to identify diverse faces.⁴⁵ Human error and misuse can further diminish FRT's accuracy.⁴⁶ For example, eyewitnesses may choose the wrong photo from an FRT-produced lineup or police may enter a hand-drawn composite sketch into an FRT.⁴⁷

Most FRTs perform best when using clear, portrait-style photographs.⁴⁸ Yet, in practice, police usually use whatever photos are available.⁴⁹ Often, these photos are grainy images taken from angles that are not directly in front of the subject, such as security camera footage.⁵⁰ Police also rely on cell phone photos and videos as FRT fodder.⁵¹ In one case, officers posing

45. See MICHELE MERLER ET AL., DIVERSITY IN FACES 4 (IBM Research 2019), <https://perma.cc/G44L-SU2U> (PDF) (“Face recognition systems that are trained within only a narrow context of a specific data set will inevitably acquire bias that skews learning towards the specific characteristics of the dataset.”).

46. See DAVID WHITE ET AL., ERROR RATES IN USERS OF AUTOMATIC FACE RECOGNITION SOFTWARE 1, 10 (PLOS ONE 2015) (“[H]uman performance curtails accuracy of face recognition systems . . .”).

47. See *id.* (“In systems implementing one-to-many algorithm checks, it is human users that are required to make final identity decisions, and so the accuracy of the system as a whole is heavily constrained by human accuracy.”); Clare Garvie, *Garbage In, Garbage Out*, GEO. L. CTR. PRIV. & TECH. (May 16, 2019), <https://perma.cc/3GZD-RCKQ> (reporting on police using artist sketches with FRT). A former NYPD commissioner denounced using composite sketches with FRT. James O’Neill, Opinion, *How Facial Recognition Makes You Safer*, N.Y. TIMES, June 9, 2019, at A23. The National Institute of Justice, however, funded research to bolster this practice. See *History of NIJ Support for Face Recognition Technology*, NAT’L INST. JUST. (Mar. 5, 2020), <https://perma.cc/ANST-RADS> (identifying grants for research “to optimize the potential of automated face recognition using sketches drawn by law enforcement sketch artists”).

48. See NIST PART 2, *supra* note 39, at 2 (presenting certain FRTs’ higher accuracy rates when using high-quality photos).

49. See Garvie, *supra* note 47 (“[I]mages [police use] may be low-quality surveillance camera stills, social media photos with filters, and scanned photo album pictures.”).

50. *Id.*; see *People v. Reyes*, 133 N.Y.S.3d 433, 434 (Sup. Ct. 2020) (recounting how police used security camera footage and FRT to identify a burglary suspect).

51. See Elisha Anderson, *Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn’t Commit*, DET. FREE PRESS (July 10, 2020, 11:42 AM), <https://perma.cc/8ZPL-MPMU> (last updated July 11, 2020, 11:03 PM) (reporting the arrest of Michael Oliver, whom FRT incorrectly identified in a cell phone video that showed another man allegedly committing a crime);

as drug buyers “surreptitiously snap[ped] photos” of a distributor leaning into the officers’ car to make a sale.⁵² The officers then used these images, taken in the dark of night, to locate a suspect using FRT.⁵³ These lower-quality images reduce FRT’s accuracy, raising the risk of misidentification.⁵⁴

Notwithstanding FRT’s imperfections, law enforcement across the country use FRT to identify criminal suspects. At least 786 state and local police departments in forty states utilize FRT.⁵⁵ In 2018 alone, NYPD detectives conducted over 7,000 searches for suspects using FRT.⁵⁶ As for federal law enforcement, from 2017 to 2019, the FBI conducted 152,500 FRT searches in law enforcement investigations.⁵⁷ Law enforcement professionals have used FRT to identify suspects in several situations, from alleged robberies to political protests.⁵⁸

Despite FRT’s prominence in law enforcement, arrestees often face an uphill battle in identifying whether FRT played a role in their arrest.⁵⁹ Warrants and affidavits often shroud FRT use behind phrases like “investigative means” or an “attempt to identify,” rather than plainly stating that an investigation used FRT.⁶⁰ As one public defender explained, police and prosecutors

Lynch v. State, 260 So. 3d 1166, 1169 (Fla. Dist. Ct. App. 2018) (discussing an FRT identification based on cell phone photos).

52. Lynch, 260 So. 3d at 1168–69.

53. Id.

54. See NIST PART 3, *supra* note 40, at 15 (“A poor image can undermine detection or recognition . . .”).

55. *Atlas of Surveillance*, *supra* note 8.

56. O’Neill, *supra* note 47.

57. Ferguson, *supra* note 8, at 1120.

58. See Hill, *Wrongfully Accused*, *supra* note 1 (recounting a wrongful arrest for robbery premised on FRT); Connie Fossi & Phil Prazan, *Miami Police Used Facial Recognition Technology in Protester’s Arrest*, NBC 6 S. FLA. (Aug. 17, 2020), <https://perma.cc/UD3T-SMQG> (reporting that police used FRT to identify a protestor); Jake Offenhartz & George Joseph, *De Blasio Will Reassess NYPD’s Use of Facial Recognition Tech After Protester Arrest*, GOTHAMIST (Aug. 17, 2020, 6:08 PM), <https://perma.cc/JY3R-TEE4> (same).

59. Kaitlin Jackson, *Challenging Facial Recognition Software in Criminal Court*, 43 CHAMPION 14, 16 (2019), <https://perma.cc/KQR7-33HS> (PDF) (“The first hurdle to an effective challenge is recognizing the cases in which FR[T] was used.”).

60. See Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), <https://perma.cc/WQH6-H4PF> (lamenting that in some cases, police do “not

also “rely on other incriminating evidence when drafting the charging documents” so that “the use of FR[T] may be so deeply buried that, unless the attorney knows to look for it, she may never discover it.”⁶¹ Thanks to these tactics, FRT use often only comes to light through an attorney’s pointed discovery requests or investigative journalism.⁶²

Even if defendants know that police used FRT in their arrests, discussion of that FRT’s error rates and biases rarely enters the courtroom. Prosecutors typically do not seek to introduce FRT evidence at trial, so defendants cannot successfully challenge FRT on evidentiary grounds.⁶³ In a similar vein, two courts recently rejected arguments that, under *Brady v. Maryland*,⁶⁴ defendants are entitled to other potential match images that FRT produced when identifying the defendant.⁶⁵ *Brady* prohibits prosecutors from suppressing “evidence favorable to an accused” when the evidence is “material either to guilt or to punishment.”⁶⁶ One New York judge posited that images of other potential matches “are not ‘favorable,’ ‘evidence,’ or ‘material to guilt.’”⁶⁷ Instead, the judge concluded that “they are simply relevant to the reliability of the identification procedure.”⁶⁸

mention [FRT] in initial warrants or affidavits” but tally those same cases as “facial recognition wins” in official county records).

61. Jackson, *supra* note 59, at 16.

62. See *id.* at 20–21 (advocating that defense attorneys persistently use discovery to uncover FRT use); Fossi & Prazan, *supra* note 58 (interviewing an attorney who, absent journalists, would not have known that police used FRT to identify his client).

63. See Jackson, *supra* note 59, at 16 (“[I]f the defense requests a *Daubert*, *Frye* or similar hearing, the prosecution will likely respond that it does not intend to introduce FR[T] evidence at trial; and the court is likely to deny the request.”). Notably, Jackson believes that “[e]ventually FR[T] technology will advance to a point where the state seeks to introduce machine identifications in trials. When that happens, the time will be ripe to request *Daubert* and *Frye* hearings.” *Id.*

64. 373 U.S. 83 (1963).

65. *Lynch v. State*, 260 So. 3d 1166, 1169–70 (Fla. Dist. Ct. App. 2018); *People v. Knight*, 130 N.Y.S.3d 919, 923 (Sup. Ct. 2020).

66. *Brady v. Maryland*, 373 U.S. 83, 87 (1963).

67. *Knight*, 130 N.Y.S.3d at 923 (citation omitted).

68. *Id.* For arguments to the contrary and a more robust discussion of *Brady*, see Rebecca Darin Goldberg, Note, *You Can See My Face, Why Can’t I? Facial Recognition and Brady*, 5 COLUM. HUM. RTS. L. REV. ONLINE 261, 289–92

Given FRT's reliability problems, overreliance on FRT in policing is a real risk with drastic consequences. Humans are prone to over-trust automated technology, a phenomenon known as automation bias.⁶⁹ Automation bias reflects individuals' tendency "to rely on the judgments of automated decisions as superior to their own, even when they have reason to believe the technology is flawed."⁷⁰ This bias creates complacency that discourages second-guessing technology.⁷¹ For instance, one study of aviation students found that students in flight simulators were "less vigilant in environments with automated decision or monitoring aids, relative to those without an automated aid."⁷² Automation bias likely affects how police use FRT.⁷³

Three recent wrongful arrests in Detroit and New Jersey illustrate some of the problems with FRT misidentifications.⁷⁴ As discussed above, Detroit police arrested Robert Julian-Borchak Williams and detained him for thirty hours

(2021); and Deborah Won, Note, *The Missing Algorithm: Safeguarding Brady Against the Rise of Trade Secrecy in Policing*, 120 MICH. L. REV. 157, 177–86 (2021). Ostensibly, defendants could also challenge FRT under *United States v. Giglio*, 405 U.S. 150 (1972). *Giglio* violations "occur[] when the prosecution solicits or fails to correct false or perjured testimony and 'the false testimony could . . . in any reasonable likelihood have affected the judgment of the jury.'" *Rodriguez v. Sec'y, Fla. Dep't of Corr.*, 756 F.3d 1277, 1302 (11th Cir. 2014) (quoting *Giglio*, 405 U.S. at 153–54). This Author found no case law or scholarship discussing *Giglio* challenges to FRT.

69. See KATE GODDARD ET AL., *AUTOMATION BIAS: A SYSTEMATIC REVIEW OF FREQUENCY, EFFECT MEDIATORS, AND MITIGATORS* 1 (2011) ("Automation bias (AB)—the tendency to over-rely on automation—has been studied in various academic fields.").

70. Lindsey Barrett, *Reasonably Suspicious Algorithms: Predictive Policing at the United States Border*, 41 N.Y.U. REV. L. & SOC. CHANGE 327, 343 (2017) [hereinafter, Barrett, *Reasonably Suspicious*].

71. See Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1271 (2008) ("Studies show that human beings rely on automated decisions even when they suspect system malfunction.").

72. Linda J. Skitka et al., *Does Automation Bias Decision-Making?*, 51 INT'L J. HUM.-COMPUT. STUD. 991, 999 (1999).

73. See Barrett, *Ban Facial Recognition*, *supra* note 25, at 245 (emphasizing that automation bias lowers the prospect of police catching FRT's mistakes).

74. Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Dec. 29, 2020) [hereinafter Hill, *Another Arrest*], <https://perma.cc/XMR8-79BW> (last updated Jan. 6, 2021); Hill, *Wrongfully Accused*, *supra* note 1; Anderson, *supra* note 51.

after FRT errantly matched security footage to Williams's driver's license photo.⁷⁵ The officer's admission that "the computer got it wrong"⁷⁶ suggests automation bias played a role in Williams's arrest.

Automation bias may have been a factor in another case from Detroit. Michael Oliver faced a felony charge after officers relied on FRT that misidentified him in a cell phone video.⁷⁷ Police arrested and charged Oliver despite physical differences between Oliver and the man in the video.⁷⁸ Most notably, Oliver has several tattoos on his forearms and face, whereas the video shows a man with no such tattoos.⁷⁹ The officers trusted the FRT's identification even though Oliver's tattoos proved that he could not be the man in the video.⁸⁰ An eyewitness also misidentified Oliver.⁸¹

Finally, in Woodbridge, New Jersey, FRT misidentified Nijeer Parks from a photo on a fake I.D. left at a crime scene.⁸² "With seemingly no other evidence, according to the police report," officers sought and received a warrant for Parks's arrest.⁸³ After being wrongfully arrested, Parks spent eleven days in jail.⁸⁴

In each of these three cases, police over-relied on FRT in making an arrest, and innocent Black men paid the price. Williams, Oliver, and Parks are the three persons "*known to be falsely arrested based on a bad facial recognition match.*"⁸⁵ Given how hard it is to tell when police use FRT,⁸⁶ additional

75. Hill, *Wrongfully Accused*, *supra* note 1.

76. *Id.*

77. Anderson, *supra* note 51.

78. *Id.*

79. *Id.* For side-by-side photos of Oliver and the man in the video, see Anderson, *supra* note 51.

80. *Id.*

81. *Id.*

82. John General & Jon Sarlin, *A False Facial Recognition Match Sent This Innocent Black Man to Jail*, CNN BUS., <https://perma.cc/6HAU-QDRB> (last updated Apr. 29, 2021, 12:23 PM).

83. *Id.*

84. *Id.*

85. *Id.* (emphasis added).

86. See Valentino-DeVries, *supra* note 60 (documenting how police shroud their FRT use); Jackson, *supra* note 59, at 16, 20–21 (same).

wrongful arrests from FRT have likely occurred and will continue as FRT proliferates in policing.⁸⁷

Automation bias can also affect eyewitnesses on whom police rely to verify FRT identifications. For example, an officer might present a photo of an FRT match to a crime's witness, tell the witness that FRT identified the match, and ask, "Is this who you saw commit the crime?"⁸⁸ Even if the FRT match does not align with the witness's memory, automation bias could push the witness to affirm the FRT match.⁸⁹ This bias may have influenced the eyewitness who misidentified Michael Oliver despite his tattoos.⁹⁰

FRT's role in law enforcement has drawn criticism from legal scholars, journalists, and elected national, state, and local officials.⁹¹ In 2019 and 2020, Congress considered various bills to curtail or ban FRT in policing on a national scale.⁹² Oregon and New Hampshire outlawed use of FRT on videos filmed by police body cameras.⁹³ California banned equipping body cameras with FRT that could make real-time identifications.⁹⁴ At least twenty-one municipalities from Portland, Maine to Portland, Oregon prohibit local law enforcement from using FRT, as do two states—Virginia and Vermont.⁹⁵

FRT's proponents argue that it can be a force for good. Absent biases, Professor I. Bennett Capers predicts that an

87. See Hill, *Another Arrest*, *supra* note 74 (airing an ACLU attorney's fears that "there have been other [wrongful] arrests and even mistaken convictions that have not been uncovered").

88. See Keith A. Findley, *Implementing the Lessons from Wrongful Convictions: An Empirical Analysis of Eyewitness Identification Reform Strategies*, 81 MO. L. REV. 377, 391–92 (2016) (highlighting how police can intentionally and unintentionally influence eyewitness identifications).

89. See Citron, *supra* note 71, at 1284 (recognizing that people "who are influenced by automation bias might endorse inaccurate computer decisions even in the face of contrary evidence").

90. See generally Anderson, *supra* note 51.

91. See generally Barrett, *Ban Facial Recognition*, *supra* note 25.

92. See Hodge, *supra* note 37, at 64–65 (collecting legislation); Charlotte Jee, *A New US Bill Would Ban the Police Use of Facial Recognition*, MIT TECH. REV. (June 26, 2020), <https://perma.cc/SK4Y-QE2P> ("US Democratic lawmakers have introduced a bill that would ban the use of facial recognition technology by federal law enforcement agencies.").

93. Hodge, *supra* note 37, at 65, 65 n.360.

94. *Id.*

95. *Map*, BAN FACIAL RECOGNITION, <https://perma.cc/77FY-U22X>.

improved FRT could result in “race-blind policing” instead of “young + black = probable cause.”⁹⁶ Others point out that FRT’s biases and related issues will likely wane as the technology progresses.⁹⁷ A former New York City Police Commissioner praised FRT’s role in identifying violent offenders and in absolving mistakenly identified suspects.⁹⁸ He reasoned that “[i]t would be an injustice to the people we serve if we policed our 21st-century city without using 21st-century technology.”⁹⁹ Given FRT’s popularity amongst law enforcement, it may be here to stay.¹⁰⁰ FRT’s prominent position as a technological policing tool counsels careful constitutional analysis under recent Supreme Court precedent.

C. *The Supreme Court’s Stringent Approach to Technology in Policing*

In three recent Supreme Court cases, “the Court has signaled that new technology requires new and arguably more protective constitutional analysis.”¹⁰¹ These cases indicate that the rules governing traditional analog policing tools do not neatly apply to digital policing tools like FRT.¹⁰²

In 2014, the Court recognized differences between digital and analog policing in *Riley v. California*.¹⁰³ *Riley* carved out an cell phone exception to the search-incident-to-arrest doctrine.¹⁰⁴ The Court reasoned that “a search of the information on a cell

96. I. Bennett Capers, *Race, Policing, and Technology*, 95 N.C. L. REV. 1241, 1277 (2017).

97. See Law Journal Editorial Board, Commentary, *In Favor of Access to Facial Recognition Technology for Law Enforcement*, N.J.L.J. (Apr. 26, 2020, 10:00 AM), <https://perma.cc/7BYW-CZ7N> (“[I]t is likely that those defects will be worked out by further research and more complete databases, because the demand for a fully accurate product exists.”).

98. O’Neill, *supra* note 47.

99. *Id.*

100. See Elizabeth A. Rowe, *Regulating Facial Recognition Technology in the Private Sector*, 24 STAN. TECH. L. REV. 1, 5 (2020) (remarking on FRT’s popularity amongst law enforcement and other government customers).

101. Ferguson, *supra* note 8, at 1134.

102. See *id.* at 1129–40 (discussing “future-proofing” the Fourth Amendment against FRT).

103. 573 U.S. 373 (2014).

104. See *id.* at 401 (“[A] warrant is generally required before such a search [of a cell phone], even when a cell phone is seized incident to arrest.”).

phone bears little resemblance” to permissible warrantless searches of other small items on an arrestee’s person, like a pack of cigarettes.¹⁰⁵ *Riley* acknowledged that searches of digital data are inherently more intrusive than searches of other objects an officer might find on an arrestee’s person.¹⁰⁶ After all, searching Riley’s cell phone “place[d] vast quantities of personal information literally in the hands” of police officers.¹⁰⁷

In *United States v. Jones*,¹⁰⁸ five Justices expressed concern about digital police technologies. Justice Alito’s concurrence—joined by Justices Ginsburg, Breyer, and Kagan—recognized that technology can quickly complete tedious manual policing tasks.¹⁰⁹ *Jones* concerned long-term surveillance, a practice that once required large “expenditure[s] of law enforcement resources,” but that GPS tracking now makes “relatively easy and cheap.”¹¹⁰ In a separate concurring opinion, Justice Sotomayor also warned against technologies that “evade[] the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility.”¹¹¹

Most recently, in *Carpenter v. United States*,¹¹² the Court found a legitimate expectation of privacy in cell phone data that cataloged the cell-phone user’s physical movements.¹¹³ The Court warned of “seismic shifts in digital technology” that differentiate digital policing from traditional analog policing.¹¹⁴

105. *Id.* at 386.

106. *See id.* at 393 (“A conclusion that inspecting the contents of an arrestee’s pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.”).

107. *Id.* at 386.

108. 565 U.S. 400 (2012).

109. *Id.* at 430 (Alito, J., concurring) (“[S]ociety’s expectation has been that law enforcement agents and others . . . could not [] secretly monitor and catalogue every single movement of an individual’s car for a very long period.”).

110. *Id.* at 429–30.

111. *Id.* at 416 (Sotomayor, J., concurring) (internal quotations omitted).

112. 138 S. Ct. 2206 (2018).

113. *Id.* at 2217.

114. *See id.* at 2219, 2223 (explaining that digital policing tools “risk[] Government encroachment of the sort the Framers, after consulting the lessons of history, drafted the Fourth Amendment to prevent”); *see also* Sonia M. Gipson Rankin, *Technological Tethereds: Potential Impact of*

These new technologies create risks of “arbitrary invasions by governmental officials” of individual privacy and security.¹¹⁵

These three cases illustrate the Supreme Court’s recent reluctance to rubber-stamp advanced technological policing. FRT should trigger similar reticence. FRT, like *Riley*’s cell phone searches or cell-site location data in *Carpenter*, opens the door to broad privacy threats, such as using FRT to track and surveil citizens.¹¹⁶ Prolonged FRT surveillance, like other digital intrusions, gives police a window into someone’s “familial, political, professional, religious, and sexual associations.”¹¹⁷ Like in *Jones*, FRT searches are effortless, making abuse all too easy.¹¹⁸ Whereas a human would tediously compare one photo against thousands in a database, FRT quickly compares photos and identifies a “match.”¹¹⁹ Finally, FRT amplifies *Carpenter*’s concerns about arbitrary government invasions.¹²⁰ For instance, automation bias can lead to arrests based on FRT misidentifications, even in the face of contradictory information.¹²¹ The wrongful arrests of Robert Julian-Borchak Williams, Michael Oliver, and Nijeer Parks are chilling

Untrustworthy Artificial Intelligence in Criminal Justice Risk Assessment Instruments, 78 WASH. & LEE L. REV. 647, 699–710 (2021) (exploring police technology’s unique vulnerability to cyberattacks and hacking, which could produce false arrests).

115. *Carpenter*, 138 S. Ct. at 2213 (internal quotation marks omitted).

116. See Ferguson, *supra* note 8, at 1115 (“Faces can be matched for generalized surveillance purposes, targeted tracking purposes, or just as a means of confirming identity for law enforcement and non-law enforcement purposes. Each potential use raises different Fourth Amendment questions.” (footnote omitted)).

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

118. Compare *id.* at 429–30 (Alito, J., concurring) (commenting how GPS technology makes tracking people “relatively easy and cheap”), with Ferguson, *supra* note 8, at 1153 (remarking on FRT’s speed and ease of use).

119. See Ferguson, *supra* note 8, at 1153 (“A manual search of . . . media . . . would take multiple lifetimes, while a digital search can take mere seconds.” (footnote omitted)).

120. See *id.* at 1139 (“[F]acial recognition technology gives police the power to conduct arbitrary digital searches of its citizens.”).

121. See Barrett, *Reasonably Suspicious*, *supra* note 70, at 343 (providing the example of “a law enforcement officer’s reliance on the technology in the field, despite mitigating circumstances that might have swayed his or her judgment otherwise”).

examples of how FRT can lead to arbitrary invasions of privacy and security.

D. *The Intersection of FRT and Probable Cause*

Some law enforcement agencies instruct officers not to rely on FRT as the sole basis of probable cause.¹²² But most agencies give officers little to no guidance on using FRT in probable cause inquiries.¹²³ The *New York Times* uncovered instances of police making arrests based solely on an FRT identification.¹²⁴ Relying solely on FRT to provide probable cause for an arrest is dangerous given FRT's risk of misidentification,¹²⁵ especially for racial minorities, women, the elderly, and the young.¹²⁶ Premising an arrest on an FRT misidentification alone can put someone in handcuffs for a crime they did not commit.¹²⁷ These wrongful arrests interrupt lives, stigmatize innocent arrestees, and perpetuate injustices in the criminal justice system.¹²⁸

Because it is difficult to identify when police use FRT to identify a suspect, courts rarely, if ever, consider FRT's role in probable cause inquiries.¹²⁹ Courts might examine FRT's role in

122. See NYPD, PATROL GUIDE: FACIAL RECOGNITION TECHNOLOGY 1 (2020), <https://perma.cc/4NAN-3HP5> (PDF) (“The facial recognition process does not by itself establish probable cause to arrest or obtain a search warrant, but it may generate investigative leads”); DEP’T OF HOMELAND SEC., ICE USE OF FACIAL RECOGNITION SERVICES 26 (2020), <https://perma.cc/GTN2-GGWW> (PDF) (“Candidate returns [from FRT] are not used as an indicator of unlawful activity or used to establish probable cause.”).

123. See Garvie, *supra* note 47 (“[I]n most jurisdictions, officers do not appear to receive clear guidance about what additional evidence is needed to corroborate a possible face recognition match.”).

124. See Valentino-DeVries, *supra* note 60 (investigating how police in Florida use FRT in practice).

125. See *infra* Part III.B.2.

126. See NIST PART 3, *supra* note 40, at 2, 63 (highlighting FRT's demographic biases); BUOLAMWINI & GEBRU, *supra* note 41, at 10 (same).

127. See Fretty, *supra* note 36, at 458 (“[F]alse positives necessarily subject innocent civilians to unwarranted police scrutiny”); Cooper, *supra* note 6 (documenting the wrongful arrests of Robert Williams, Nijeer Parks, and Michael Oliver).

128. See Barrett, *Ban Facial Recognition*, *supra* note 25, at 245 (“A false positive can endanger someone’s freedom or even their life”).

129. See KELSEY Y. SANTAMARIA, CONG. RSCH. SERV., R46541, FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT: SELECT CONSTITUTIONAL CONSIDERATIONS 19 (2020) (“[A] survey of case law suggests that courts have

probable cause in civil suits that stem from wrongful arrests, but only if those cases do not settle.¹³⁰ The absence of a judicial framework for evaluating FRT's role in probable cause is dangerous given FRT's widespread use and the attendant risks of demographic biases stemming from its flawed data.

Few scholars have examined FRT's place in establishing probable cause.¹³¹ In a 2011 article surveying FRT's Fourth Amendment implications, Douglas Fretty discussed “[w]hether identification by an FRT system establishes probable cause to search or detain a person.”¹³² Fretty compared FRT's error rates against those of other policing tools like drug dogs and field sobriety tests, searching for a “tolerable rate of error” to sustain probable cause.¹³³ Fretty recognized that “FRT enthusiasts have a strong argument that an FRT algorithm need only be right a substantial percentage of the time in order to establish probable cause for a search or seizure.”¹³⁴ He countered that unlike drug dogs and field sobriety tests, police can use FRT on persons who are not otherwise lawfully stopped.¹³⁵ As such, FRT's “tolerable

rarely considered probable cause challenges to police work that relied on purportedly unreliable FRT matches.”). This Author found one opinion mentioning probable cause and FRT. *See* Bah v. Apple Inc., No. 19-cv-3539, 2021 WL 4084500, at *9–10 (S.D.N.Y. Sept. 8, 2021) (dismissing a § 1983 wrongful arrest claim involving an FRT identification because the officers also relied on a warrant, which “is presumed to be reasonable and to have been issued on probable cause”). Challenges to FRT on other grounds are more common. *See* Jackson, *supra* note 59, at 20 (“[T]here are some forms of relief that attorneys should be requesting in every FR[T] case: discovery, Brady material, and suppression of identifications (related to FR[T]).”).

130. *See* Law Journal Editorial Board, Commentary, *Use of Facial Recognition Following Capitol Siege Highlights Issues Seen in NJ Case*, N.J.L.J. (Jan. 17, 2021, 9:00 AM), <https://perma.cc/6YPJ-56LD> (predicting that if Nijeer Parks's civil suit “does not settle, the town will undoubtedly defend on the ground that the facial recognition match, though mistaken, constituted probable cause for the arrest”).

131. Scholars have examined whether the law should require probable cause *before* using FRT to search for a suspect. *See generally* Ferguson, *supra* note 8; Ari B. Rubin, *A Facial Challenge: Facial Recognition and the Carpenter Doctrine*, 27 RICH. J.L. & TECH. 1 (2021).

132. Fretty, *supra* note 36, at 458.

133. *Id.* at 459–60.

134. *Id.* at 460.

135. *Id.* at 461.

rate of error” should be lower than the rates of error for drug dogs and sobriety tests.¹³⁶

Fretty next recognized that fingerprint analysis, like FRT’s face-matching, “filters through the fingerprints of millions of innocent civilians before finding a match.”¹³⁷ Fingerprint technologies are far more accurate than drug dogs or sobriety tests.¹³⁸ Fretty concluded that only when FRT’s error rates compare to digital fingerprint-recognition’s error rates should FRT’s “society-wide use survive probable-cause scrutiny.”¹³⁹

The legal landscape around FRT has shifted in the decade since Fretty’s article. The Supreme Court issued notable rulings about technology in policing¹⁴⁰ and an opinion discussing whether drug dogs can provide probable cause.¹⁴¹ Outside the courtroom, recent research brought FRT’s racial, gender, and age biases into focus.¹⁴² This research also demonstrated that not all FRTs are created equal.¹⁴³ Their error rates vary across demographic groups and based on image quality, making uniform judicial rules based solely on error rates hard to apply.¹⁴⁴

Some scholars promote assigning a numerical value to probable cause that law enforcement and judges can compare

136. See *id.* at 461–62 (“Until face-based surveillance can be shown to combat a public harm of comparable magnitude, the probable cause standard should not allow error-prone technology to turn every civilian’s outing into a potential police encounter.”).

137. *Id.* at 462.

138. *Id.* at 461–62.

139. *Id.* at 462.

140. See *United States v. Jones*, 565 U.S. 400, 404 (2012) (finding that placing a GPS tracking device on a suspect’s car constitutes a Fourth Amendment search); *Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018) (concluding that acquiring digital cell-site location information requires a warrant supported by probable cause).

141. See *Florida v. Harris*, 568 U.S. 237, 244 (2013) (examining whether a drug dog’s alert creates probable cause). For a more thorough discussion of *Harris*, see *infra* Part II.B.

142. See NIST PART 3, *supra* note 40, at 2, 63; BUOLAMWINI & GEBRU, *supra* note 41, at 10.

143. See NIST PART 3, *supra* note 40, at 58 (documenting variations in accuracy across different FRTs).

144. See *id.* at 2, 63 (demographic biases); BUOLAMWINI & GEBRU, *supra* note 41, at 10 (same); NIST PART 2, *supra* note 39, at 2 (image quality).

against an FRT's error rate.¹⁴⁵ For instance, in a 2013 article, Professor Erica Goldberg suggested that if probable cause requires a 51 percent certainty of criminal activity, then FRT with a 42 percent accuracy rate could not establish probable cause.¹⁴⁶

However, an FRT's error rate for a particular match is hard to deduce. Error rates fluctuate based on demographic biases and image quality.¹⁴⁷ These shifting error rates complicate probable cause analyses based solely on numerical values.¹⁴⁸ Moreover, quantifying probable cause is unlikely to gain traction given judicial distaste for "rigid rules, bright-line tests, and mechanistic inquiries" in probable cause determinations.¹⁴⁹

Most recently, a 2020 report from the Congressional Research Service (CRS) surveyed potential constitutional challenges to law enforcement's use of FRT.¹⁵⁰ Among other things, this report recognized that "[r]eliance on inaccurate FRT when seeking an arrest warrant may raise questions about whether the warrant is supported by probable cause."¹⁵¹ The report analogized FRT with drug dogs and human informants, analyzing Supreme Court cases that discussed whether drug

145. See Erica Goldberg, *Getting Beyond Intuition in the Probable Cause Inquiry*, 17 LEWIS & CLARK L. REV. 789, 813–15 (2013) (arguing that "quantified error rates should be included in the probable cause inquiry"); Max Minzner, *Putting Probability Back into Probable Cause*, 87 TEX. L. REV. 913, 920–21 (2009) (same).

146. Goldberg, *supra* note 145, at 829–33.

147. See NIST PART 3, *supra* note 40, at 2, 63 (demographic biases); BUOLAMWINI & GEBRU, *supra* note 41, at 10 (same); NIST PART 2, *supra* note 39, at 2 (image quality).

148. See Orin Kerr, *Why Courts Should Not Quantify Probable Cause, in THE POLITICAL HEART OF CRIMINAL PROCEDURE: ESSAYS ON THEMES OF WILLIAM J. STUNTZ* 131, 139–42 (Michael Klarman et al. eds., 2012) (explaining how cognitive biases arise when multiple quantified variables inform a probable cause decision).

149. *Harris*, 568 U.S. at 244; see *United States v. McClain*, 444 F.3d 556, 568–69 (6th Cir. 2005) (Boggs, J., concurring) ("[C]ourts have resisted mightily putting a number on probable cause . . .").

150. See Santamaria, *supra* note 129, at 3 ("The Constitution may provide some restrictions on government use of FRT. One constitutional consideration concerns the applicability of the Fourth Amendment to law enforcement's use of FRT in criminal investigations.").

151. *Id.* at 19.

dogs and informants can provide probable cause.¹⁵² The report concluded that “the Supreme Court’s probable cause jurisprudence suggests that a reviewing court would consider the totality of the circumstances surrounding the face match using FRT.”¹⁵³

II. PROBABLE CAUSE AND DRUG DOGS: A STARTING POINT FOR PROBABLE CAUSE AND FRT

As the CRS report recognizes, probable cause case law about drug dogs and anonymous informants can inform probable cause analyses of FRT.¹⁵⁴ However, drug dog case law provides the best analogy for analyzing FRT’s role in probable cause. These cases explore legal nuances about drug dogs that overlap with some of FRT’s unique characteristics.¹⁵⁵ Applying case law about drug dogs to FRT creates a robust probable cause analysis that can sharpen judicial scrutiny of FRT’s flaws and of how police use FRT.¹⁵⁶

A. *Drug Dog Case Law Fits FRT*

Drug dogs, informants, and FRT are all policing tools that identify criminal suspects.¹⁵⁷ The same probable cause standard applies to arrests and seizures based on all three tools.¹⁵⁸ Nonetheless, drug dog case law provides the best framework for

152. See *id.* at 19–21 (surveying *Florida v. Harris*, 568 U.S. 237 (2013); *Aguilar v. Texas*, 378 U.S. 108 (1964); and *Illinois v. Gates*, 462 U.S. 213 (1983)).

153. *Id.* at 21.

154. See *id.* at 19–21.

155. See *infra* Part II.A.

156. See *infra* Part II.B.

157. See WAYNE R. LAFAYE, *Time and Investigative Method Limits*, in 4 SEARCH & SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 9.2(f) (2020) (cataloging cases in which police used drug dogs to identify criminal suspects); Jessica A. Roth, *Informant Witnesses and the Risk of Wrongful Convictions*, 54 AM. CRIM. L. REV. 737, 738–41 (2016) (critiquing informant identifications); SANTAMARIA, *supra* note 129, at 19 (“[I]nvestigative officers have deployed FRT to identify suspects . . .”).

158. See SANTAMARIA, *supra* note 129, at 19 (“[I]nformants and canine alerts . . . may offer insight into how a court may rule on a probable cause challenge to an arrest or search based on inaccurate or unreliable FRT results.”).

FRT and probable cause because it can account for FRT's complexities in a way that informant case law cannot.

*Illinois v. Gates*¹⁵⁹ is “[t]he foundational case for the probable cause standard,” particularly concerning informants.¹⁶⁰ *Florida v. Harris*, the central case about probable cause from drug dogs, adapted *Gates*'s methods to the nuances of drug dog identifications.¹⁶¹ *Harris*'s adaptation of *Gates* better applies to FRT's idiosyncrasies than *Gates* and other informant-centered cases. FRT and drug dogs are policing tools owned and operated by police,¹⁶² whereas informants are independent human actors who choose to interact with police.¹⁶³ As such, drug dogs and FRT raise unique risks of misuse and abuse that informants do not.¹⁶⁴ Cases examining probable cause from drug dogs account for this risk of misuse.¹⁶⁵ Cases about informants focus instead on an informant's “veracity, reliability, and basis of knowledge.”¹⁶⁶ Although those factors

159. 462 U.S. 213 (1983).

160. 1 CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 52 (4th ed. 2020); see Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259, 289 (2012) (noting *Gates*'s prominence in informant cases).

161. See David J. Robinson, *Admissibility of Dog-Sniff Evidence: Evaluating Probable Cause After Florida v. Harris*, 101 ILL. BAR J. 194, 210 (2013) (“Relying heavily on *Gates*, the Supreme Court [in *Harris*] noted that the post-*Gates* probable-cause showing was a ‘practical and common-sensical standard’ designed to make a probable-cause evaluation a more fluid analysis.”).

162. See *supra* notes 55–58 and accompanying text (discussing FRT's popularity in police departments); *Florida v. Jardines*, 569 U.S. 1, 16–17 (2013) (Alito, J., dissenting) (commenting that dogs “and their acute sense of smell ha[ve] been used in law enforcement for centuries”).

163. See Mary Nicol Bowman, *Truth or Consequences: Self-Incriminating Statements and Informant Veracity*, 40 N.M. L. REV. 225, 255 (2010) (considering “the incentives for an informant to provide a tip based on lies or guesses and hope the tip pans out when the informant does not actually know information that is useful for the police”).

164. See *infra* Part III.A.

165. *Florida v. Harris*, 568 U.S. 237, 247 (2013) (instructing trial courts to consider whether “the officer cued the dog”). For further examination of cueing and other avenues for misusing drug dogs, see *infra* Part III.A.

166. *Alabama v. White*, 496 U.S. 325, 328 (1990) (internal quotation marks removed).

relate to FRT, the factors that determine if a drug dog can provide probable cause hew more closely to FRT searches.¹⁶⁷

B. *Applying Drug Dog Case Law to FRT*

Florida v. Harris, the seminal case on drug dogs and probable cause, provides a baseline for judicial review in probable cause inquiries involving FRT. Probable cause inquiries require courts to consider the “totality of the circumstances.”¹⁶⁸ In drug dog cases, the totality of the circumstances includes factors such as a drug dog’s certification by “a bona fide organization” that “test[ed] his reliability in a controlled setting,” “if the dog has recently and successfully completed a training program that evaluated his proficiency in locating drugs,” or “evidence of the dog’s (or handler’s) history in the field.”¹⁶⁹ No one factor is dispositive,¹⁷⁰ but each informs a judge’s consideration of the totality of the circumstances.¹⁷¹

At probable cause hearings, a defendant “must have an opportunity to challenge . . . evidence of a dog’s reliability, whether by cross-examining the testifying officer or by introducing his own fact or expert witnesses.”¹⁷² At these hearings, courts consider issues like the adequacy of the dog’s training program, the dog and its handler’s performance in training exercises, whether the dog receives regular recertification, and the unique circumstances of the dog’s alert, including whether the handler cued the dog.¹⁷³

The *Harris* framework adapts well to FRT. Just as probable cause inquiries involving drug dogs must consider factors

167. See *Harris*, 568 U.S. at 245–46 (listing factors to consider in probable cause inquiries). For an analysis of these factors, see *infra* Part II.B.

168. *Harris*, 568 U.S. at 244.

169. *Id.* at 246–47.

170. See *id.* at 244 (rejecting “a strict evidentiary checklist” covering a dog’s field performance “whose every item the State must tick off” to establish probable cause).

171. *Id.* at 247–48.

172. *Id.* at 247.

173. *Id.* at 248; see *United States v. Green*, 740 F.3d 275, 283–84 (4th Cir. 2014) (viewing a drug dog’s annual recertification as a factor in favor of establishing the dog’s reliability in detecting drugs). For a more detailed discussion of cueing—when a dog responds to cues from its handler rather than the presence of drugs—see *infra* Part III.A.

affecting the dog's reliability, probable cause cases involving FRT must consider factors affecting FRT's reliability. In these FRT cases, the totality of the circumstances must include, at minimum, (1) the FRT's error rates and demographic biases, (2) the image(s) it used to identify an individual, (3) all potential "match" images the FRT identified, (4) an officer's history and training concerning FRT, and (5) the databases used to develop the FRT. All five of these factors measurably affect FRT's reliability.¹⁷⁴

No one factor is dispositive.¹⁷⁵ Instead, weighing each of these factors against each other will allow judges to "evaluate the proffered evidence [and] to decide what all the circumstances demonstrate."¹⁷⁶ Regarding error rates, the State need not meet rigid percentage thresholds that are "the antithesis of a totality-of-the-circumstances analysis."¹⁷⁷ The State should instead document how the FRT's error rates vary depending on the subject's race, gender, and age. Demographic variations in error rates affect the likelihood that an FRT correctly identified a particular defendant.¹⁷⁸ Beyond FRT, the totality of the circumstances should include any other evidence that police considered besides the FRT identification.¹⁷⁹

174. See NIST PART 3, *supra* note 40, at 15–16 (explaining how demographics and image quality affect FRT's error rates and reliability); WHITE ET AL., *supra* note 46, at 10–11 (demonstrating how FRT loses effectiveness based on human variables, including the drive to choose the "right" match from a list of potential matches); NIST PART 2, *supra* note 39, at 71 (noting that "more diverse, globally derived, training data" can reduce false-positive identifications).

175. Florida v. Harris, 568 U.S. 237, 244 (2013).

176. *Id.* at 247–48.

177. *Id.* at 245.

178. See BUOLAMWINI & GEBRU, *supra* note 41, at 1 ("The substantial disparities in the accuracy of classifying darker females, lighter females, darker males, and lighter males . . . require urgent attention . . ."); *supra* note 17 and accompanying text (highlighting the importance of particularized suspicion in probable cause).

179. See United States v. Bentley, 795 F.3d 630, 635 (7th Cir. 2015) (commenting that, in addition to a drug dog's alert, courts could consider the defendant's inconsistent narrative and other circumstances when determining whether an officer had probable cause to search the defendant's vehicle).

This judicial analysis should occur both before and after an arrest.¹⁸⁰ First, before a magistrate judge issues an arrest warrant,¹⁸¹ the police affidavit requesting the warrant should include the FRT's error rates and its demographic discrepancies, the image(s) it used to identify an individual, and any other potential matches the FRT returned.¹⁸² Ensuring judicial review of an FRT identification before an arrest occurs will serve as a check against wrongful arrests and better publicize FRT use in affidavits rather than disguising it behind vague phrases like "investigative means."¹⁸³

Second, after an arrest, defendants must be able to challenge an FRT-involved arrest as lacking probable cause. Beyond examining the FRT's error rates, demographic biases, the images it used, and the match(es) it produced, defendants at these probable cause hearings can challenge their FRT identification on several fronts. For instance, a defendant should "cross-examin[e] the testifying officer" who used the technology.¹⁸⁴ In the drug dog context, a handler's testimony can weaken a dog's probable cause credentials. The Seventh Circuit recently criticized an officer who admitted to rewarding his drug dog every time the dog alerted because the rewards encouraged false alerts and diminished the dog's accuracy.¹⁸⁵

An FRT defendant should also query how often their arresting officers use FRT and whether those officers have ever misused the technology.¹⁸⁶ Such questioning mirrors *Harris's*

180. Magistrate judges issue warrants upon a showing of probable cause before an arrest occurs. MCCABE, *supra* note 13, at 23–25. Trial courts assess whether probable cause existed to support the arrest after-the-fact. See *Ornelas v. United States*, 517 U.S. 690, 697, 699–70 (1996) (detailing the trial court's role in probable cause inquiries).

181. For a discussion of how magistrate judges issue warrants, see MCCABE, *supra* note 13, at 23–25.

182. See *supra* note 174 and accompanying text.

183. See *State v. Meyer*, 587 N.W.2d 719, 728 (S.D. 1998) ("An arrest warrant and a search warrant are safeguards of individual rights. These processes serve a gate keeping purpose. They protect individuals from unnecessary intrusions by the government.").

184. *Harris*, 568 U.S. at 247.

185. See *Bentley*, 795 F.3d at 636 (condemning the officer's practice of giving the dog "a rubber hose stuffed with a sock[] every time he alerts").

186. See *Ferguson*, *supra* note 8, at 1203 (recognizing FRT's potential for "misuse against marginalized communities and dissenting voices").

recommended inquiry into a dog's handler.¹⁸⁷ For example, NYPD detectives misused FRT by using an image of Woody Harrelson to try to identify a suspect who allegedly resembled the actor.¹⁸⁸ Inquiries into an officer's FRT training or instruction are likewise relevant,¹⁸⁹ especially when police use FRT that produces a list of potential matches.¹⁹⁰ At least one study suggests that face identification training can mitigate human error in evaluating potential matches.¹⁹¹

Information on the FRT's training and development also merits consideration.¹⁹² The data sets of images used to train the FRT are particularly important.¹⁹³ The likelihood of misidentification is higher if the training data set lacks images sharing the defendant's race, age, or gender.¹⁹⁴ Courts should also examine the integrity of the FRT's image database. Some FRT databases include low-quality images that further diminish FRT accuracy.¹⁹⁵ Finally, like in drug dog cases, expert witnesses are another line of defense in FRT-based prosecutions.¹⁹⁶ Courts should assess these experts' testimony

187. See *Florida v. Harris*, 568 U.S. 237, 247 (2013) (“[T]he defendant may examine how the dog (or handler) performed in [training exercises] . . .”).

188. Garvie, *supra* note 47.

189. See *United States v. Green*, 740 F.3d 275, 283 (4th Cir. 2014) (crediting a state trooper's regular training with his drug-sniffing dog, Bono, in finding that Bono's alert provided the trooper with probable cause).

190. See *WHITE ET AL.*, *supra* note 46, at 10 (documenting how FRTs that present a list of potential matches open up opportunities for human error).

191. See *id.* at 11 (“[S]pecialist facial examiners performed far better on the candidate list task than untrained students and the non-specialist passport officers—making 20% fewer errors as a group.”).

192. See *Harris*, 568 U.S. at 246–47 (explaining how evidence of a drug dog's training influences the probable cause analysis).

193. See *NIST PART 3*, *supra* note 40, at 10 (recommending “refined training” and “more diverse training data” as means to increase FRT reliability).

194. See *id.* at 2, 63; *BUOLAMWINI & GEBRU*, *supra* note 41, at 10; *MERLER ET AL.*, *supra* note 45, at 4.

195. See *NIST PART 3*, *supra* note 40, at 15–16.

196. See *United States v. Diskin*, 364 F. Supp. 3d 1138, 1145 (D. Mont. 2019) (examining testimony from a defendant's drug dog expert), *aff'd*, No. 19-30218, 2021 WL 1549967 (9th Cir. Apr. 20, 2021); *United States v. Melchior*, 4:16CR3033, 2017 WL 9478421, at *7–8 (D. Neb. Jan. 17, 2017) (same).

as they would in any case.¹⁹⁷ A more active judicial role in probable cause cases involving FRT can empower judges to prevent wrongful arrests.

III. FRT MERITS MORE SCRUTINY THAN DRUG DOGS AND SHOULD NOT BE THE SOLE SOURCE OF PROBABLE CAUSE

Crucial differences between FRT and drug dogs demand that courts scrutinize FRT more skeptically. FRT harbors dangers that are either nominal or non-existent in drug dogs, namely (1) demographic biases stemming from flawed data, and (2) FRT's status as a technological policing tool. These factors justify increased judicial scrutiny of FRT in probable cause cases.¹⁹⁸ Applying that heightened scrutiny demonstrates why FRT, unlike drug dogs, should not provide the only basis of probable cause because of its potential reliance on bad data and its race, gender, and age biases.¹⁹⁹

A. *Differences Between FRT and Drug Dogs Call for Heightened Judicial Scrutiny*

1. Race, Gender, and Age Biases Hamper FRT Differently than Drug Dogs

FRT's reliability and bias problems come from poorly trained algorithms that rely on non-diverse datasets.²⁰⁰ Though both FRT and drug dogs can suffer from insufficient training that may lead to false-positive identifications,²⁰¹ a dog's misidentifications lack FRT's inherent racial, gender, and age biases that perpetuate injustices in the criminal justice system. A poorly trained dog may lead an officer to an empty car or get

197. See, e.g., *United States v. \$209,815 in U.S. Currency*, No. 3:14-cv-00780, 2015 WL 5970186, at *11 (N.D. Cal. Oct. 14, 2015) (applying the *Daubert* standard to competing drug dog experts).

198. See *infra* Part III.A.

199. See *infra* Part III.B.

200. BUOLAMWINI & GEBRU, *supra* note 41, at 10.

201. See Ken Lammers, *Canine Sniffs: The Search That Isn't*, 1 N.Y.U. J.L. & LIBERTY 845, 852 (2005) (“[A] dog’s accuracy depends on the quality of its training”); *id.* at 851 (showing the consequences of a drug dog’s false alert); NIST PART 3, *supra* note 40, at 10 (presenting FRT’s risk of false positives).

distracted by nearby animals.²⁰² It might alert its handler to money contaminated with drug residue, a surprisingly common occurrence,²⁰³ unbeknownst to an innocent person carrying a dirty dollar.²⁰⁴ A drug dog may also falsely alert due to “cueing” from its handler.²⁰⁵ Cueing occurs when a dog “recognize[s] and react[s] to [its handler’s] posture, facial expressions, tone of voice, and so on” such that the dog appears to “accomplish[] the job it is trained to perform, while in reality it is merely responding to cues from its handler.”²⁰⁶ For example, a dog may give a false positive alert when an officer leans into a car’s window because the dog associates alerting with seeing its handler lean into a car’s window.²⁰⁷

For all their flaws, drug dogs lack FRT’s built-in risk of false positives when dealing with people of color, women, and elderly and young people.²⁰⁸ Demographic biases may influence a dog’s handler, who subsequently cues the dog based on those biases.²⁰⁹

202. See Transcript of Oral Argument at 41, *Florida v. Harris*, 568 U.S. 237 (2013) (No. 11-817) (“[D]ogs make mistakes. Dogs err. Dogs get excited and will alert to things like tennis balls in trunks or animals, that sort of thing.”).

203. See Yuegang Zuo et al., *An Accurate and Nondestructive GC Method for Determination of Cocaine on US Paper Currency*, 31 J. SEPARATION SCI. 2444, 2444 (2008) (“Cocaine was detected in 67% of the circulated banknotes collected in Southeastern Massachusetts On average, \$5, 10, 20, and 50 denominations contain higher amounts of cocaine than \$1 and 100 denominations of US banknotes.”).

204. See *United States v. \$242,484.00*, 351 F.3d 499, 511 (11th Cir. 2003) (suggesting that contaminated currency makes drug dog alerts less reliable), *aff’d en banc*, 389 F.3d 1149 (11th Cir. 2004).

205. See Lammers, *supra* note 201, at 852 (detailing the risks of cueing in canine policing).

206. *Id.*

207. See *id.* (providing examples of cueing).

208. See Joseph Magrisso, *Protecting Apartment Dwellers from Warrantless Dog Sniffs*, 66 U. MIA. L. REV. 1133, 1148–49 (2012) (cataloging causes of dogs’ “high false alert rates” including poor temperament, smelling items associated with contraband, catching a whiff of a drug’s legal byproduct, and cueing from handlers).

209. See Carlee Beth Hawkins & Alexia Jo Vandiver, *Human Caregivers Perceive Racial Bias in Their Pet Dogs*, 22 GRP. PROCESSES & INTERGROUP RELS. 901, 912 (2019) (acknowledging that “[w]hite caretakers’ implicit personal pro-[w]hite preference could be ‘passed down the leash’ to their pet dogs through demonstrating negative nonverbal behaviors”).

But in that case the handler is the problem, not the dog.²¹⁰ Similarly, police may deploy drug dogs in a racially biased manner.²¹¹ There too, the biased action lies with the handler, not the dog.²¹² Demographic biases do not impede drug dogs in probable cause inquiries because drug dogs are not inherently less reliable when sniffing one group's vehicles versus another's.²¹³ Handler biases, not a dog's internal flaws, create discrepancies in drug dog accuracy across demographic groups.²¹⁴ In contrast, FRT's built-in demographic biases hamper its reliability in probable cause cases.²¹⁵ These technological biases call for more careful judicial scrutiny of FRT than drug dogs.

2. Digital Policing Tools Like FRT Deserve More Scrutiny than Analog Policing Tools Like Drug Dogs

Recent Supreme Court cases like *Riley*, *Carpenter*, and *Jones* differentiate digital policing tools from analog policing tools and reinforce why courts should treat FRT more stringently than drug dogs. These three cases demonstrate that

210. See Lisa Lit et al., *Handler Beliefs Affect Scent Detection Dog Outcomes*, 14 ANIMAL COGNITION 387, 387 (2011), <https://perma.cc/7YSA-9P92> (PDF) (“Handlers’ beliefs that scent was present potentiated handler identification of detection dog alerts. Human more than dog influences affected alert locations.”).

211. See Anthony J. Ghiotto, *Traffic Stop Federalism: Protecting North Carolina Black Drivers from the United States Supreme Court*, 48 U. BALT. L. REV. 323, 366 (2019) (“[A] police officer who has a subjective belief that black drivers are more likely to carry drugs in their vehicles than white drivers may follow a black driver until the driver commits a traffic code violation and then immediately request a drug-sniffing dog to confirm the officer’s subjective hunch.” (footnote omitted)).

212. See *id.* at 365 (“The initial decision of whether to utilize a drug dog may provide for the most subjectivity on the part of the police officer.”); cf. Brandon Hasbrouck, *Abolishing Racist Policing with the Thirteenth Amendment*, 67 UCLA L. REV. DISCOURSE 1108, 1115 n.30 (2020) (“The use of police dogs is not inherently racist, but rather presents a violent and dehumanizing vehicle for officers’ own racial biases.”).

213. Magrisso, *supra* note 208, at 1448–49.

214. Cf. Lit et al., *supra* note 210, at 393 (“[H]andler beliefs affect working dog outcomes, and human indication of scent location affects distribution of alerts more than dog interest in a particular location.”).

215. NIST PART 3, *supra* note 40, at 2, 63; BUOLAMWINI & GEBRU, *supra* note 41, at 10.

traditional search and seizure doctrines do not always apply to technological policing.²¹⁶ Concerns over issues like privacy, the ease and convenience of digital versus analog policing, and heightened risks of arbitrary government intrusions into citizens' lives animate these opinions.²¹⁷

As discussed above, FRT is a digital policing tool that raises serious threats to personal privacy, such as tracking and surveilling citizens. In contrast, privacy concerns from drug dogs are shorter lived and less pervasive.²¹⁸ Regarding issues of ease and convenience, officers can run FRT searches from a police station and sort through thousands of photos at the click of a button.²¹⁹ But drug dogs require approaching vehicles or suspects in the field one at a time.²²⁰ Finally, the risk of arbitrary government intrusions from FRT is greater than for drug dogs. These higher risks stem from the frequency and ease of FRT searches vis-à-vis drug dogs, the likelihood of overreliance on FRT due to automation bias, and the potential for real-time public surveillance.²²¹ These differences between drug dogs and FRT illustrate the Supreme Court's concerns about the shift from traditional to digital policing.²²² Given these concerns, courts should treat FRT with a more protective constitutional analysis and refuse to recognize FRT as the sole basis of probable cause.²²³

216. See Ferguson, *supra* note 8, at 1129–40.

217. See *supra* Part I.C.

218. See *Illinois v. Caballes*, 543 U.S. 405, 406 (2005) (recounting that a search involving a drug dog lasted less than ten minutes).

219. Ferguson, *supra* note 8, at 1153.

220. See Lammers, *supra* note 201, at 285 (describing how drug dog sniffs occur).

221. See Ferguson, *supra* note 8, at 1115, 1139, 1153 (documenting FRT's risks of error and abuse).

222. See *id.* at 1134 (“[M]erely applying analog precedents to digital challenges does not maintain the status quo but significantly enhances police power at the expense of personal liberty.”).

223. The fact that FRT is a digital policing tool also distinguishes it from eyewitness identifications, a traditional analog policing tool that can provide the sole source of probable cause despite demographic biases. Eyewitness identifications typically occur using an in-person lineup or a group of photographs known as a photo array. Findley, *supra* note 88, at 442. Demographic bias can arise in eyewitness identifications from two sources: the eyewitness or the officers who present the lineup or photo array.

B. *An FRT Match Alone Cannot Provide Probable Cause*

A more searching constitutional analysis of FRT should focus on FRT's reliance on flawed data and the resulting demographic biases. These problems warrant precluding FRT from providing the sole source of probable cause. Robust public support for limiting FRT's role in law enforcement and probable cause inquiries bolsters this conclusion.

1. *Garbage in, Garbage out: Flawed Data, Police Databases, and Probable Cause*

Many FRTs rely on flawed inputs—faulty data sets and algorithms.²²⁴ These flawed inputs create flawed outputs—demographically biased error rates.²²⁵ “Garbage in, garbage out.”²²⁶ Recent cases about bad data in police databases

Eyewitnesses struggle with cross-racial identifications, which “are less accurate even if the witness harbors no significant biases and has had frequent interactions with persons of that race.” Sandra G. Thompson, *Judicial Blindness to Eyewitness Misidentification*, 93 MARQ. L. REV. 639, 665 (2009). But unlike FRT, an individual eyewitness's biases only affect the investigation the eyewitness participates in. Brandon Garrett, *Eyewitnesses and Exclusion*, 65 VAND. L. REV. 451, 458–60 (2012). FRT mechanically injects its biases into *every* investigation where police use it. See Ferguson, *supra* note 8, at 1120. Officer bias in identifications presents a more persistent problem—one biased officer can influence many eyewitnesses. See Richard A. Wise et al., *How to Analyze the Accuracy of Eyewitness Testimony in a Criminal Case*, 42 CONN. L. REV. 435, 461–63 (2009). Officers retain ample leeway in conducting lineups and photo arrays, with practices “traditionally passed on by senior officers through word of mouth.” Garrett, *supra*, at 459. Over time, demographic biases could seep into an entire department's eyewitness procedures. See Findley, *supra* note 88, at 280 (recognizing systemic problems related to identification errors). Despite this pervasive potential, officer bias lacks FRT's automated ease. See Ferguson, *supra* note 8, at 1200. Contacting eyewitnesses, compiling photo arrays, and fielding lineups take time and effort, whereas FRT merely requires a few clicks on a computer. See Garrett, *supra*, at 459. These digital differences merit added scrutiny.

224. NIST PART 3, *supra* note 40, at 2, 63; BUOLAMWINI & GEBRU, *supra* note 41, at 10; MERLER ET AL., *supra* note 45.

225. See NIST PART 3, *supra* note 40, at 7–8, 63; BUOLAMWINI & GEBRU, *supra* note 41, at 10.

226. See Garvie, *supra* note 47 (“Garbage in, garbage out’ is a phrase used to express the idea that inputting low-quality or nonsensical data into a system will produce low-quality or nonsensical results.”); *United States v. Esquivel-Rios*, 725 F.3d 1231, 1234 (10th Cir. 2013) (Gorsuch, J.) (“Garbage

can inform how courts should review FRT's faulty data inputs. These cases about flawed inputs, viewed in tandem with FRT's biased outputs, demonstrate why courts should preempt FRT from providing probable cause without further investigation.

a. Supreme Court Scrutiny of Police Databases

In *Herring v. United States*,²²⁷ the Supreme Court recognized that erroneous data inputs can disqualify technology from providing probable cause.²²⁸ Police wrongly arrested Herring after his name mistakenly appeared in a database of open warrants.²²⁹ Herring's "warrant had been recalled five months earlier," but the database showed an active warrant in his name.²³⁰ Because incorrect data populated the database, identifying Herring within it did not provide probable cause to arrest him.²³¹ *Herring's* acknowledgment that a technology's flawed inputs provide shaky grounding for probable cause is significant, even if the Court ultimately looked past the probable cause issue.²³²

Herring clarified that if "false information" in a database was "necessary to" reach a probable cause determination, then that false information could void the probable cause finding.²³³ The false information is essentially a bad input (garbage in) that negates probable cause premised on that input (garbage out).²³⁴

in, garbage out. Everyone knows that much about computers: you give them bad data, they give you bad results.").

227. 555 U.S. 135 (2009).

228. *Id.* at 137–39.

229. *Id.* at 138.

230. *Id.*

231. *Id.* at 137–39.

232. *See id.* at 146–47 (holding that even if police lacked probable cause to arrest, the good-faith exception to the exclusionary rule permitted admitting evidence obtained during the arrest).

233. *Id.* at 145.

234. A critic might observe that *Herring* required "deliberate falsehoods" or "reckless disregard" rather than mere "innocent mistake[s]" or negligence to suppress evidence from an arrest based on faulty database. *Id.* This distinction does not determine FRT's role in probable cause. *Herring* distinguished reckless from innocent informational defects under the exclusionary rule and its purpose of "deter[ring] police misconduct." *Id.* at 143–44. FRT's flawed inputs are not the product of police misconduct, but the misconduct of private companies. *See Atlas of Surveillance, supra* note 55

Probable cause premised on FRT alone suffers from the same deficiency as the probable cause to arrest Herring: bad inputs. Like the database in *Herring*, FRT relies on questionable intake—non-diverse training data and biased algorithms.²³⁵ In both cases, these poor inputs led to poor outcomes: Herring’s wrongful arrest and FRT’s biased misidentifications. These similarities strengthen the conclusion that FRT cannot provide the sole source of probable cause.

Herring also suggested that relying on technology beset by recurring errors can preclude probable cause.²³⁶ Chief Justice Roberts reasoned that “[s]urely it would *not* be reasonable for the police to rely on a recordkeeping system that *routinely* leads to false arrests.”²³⁷ Because reasonableness guides probable cause inquiries,²³⁸ technology that police cannot reasonably rely

(cataloging dozens of private vendors from whom law enforcement agencies purchase FRT). The exclusionary rule does not apply to private parties. *See State v. Christensen*, 797 P.2d 893, 897 (Mont. 1990) (“Even though the exclusionary rule could be applied to evidence resulting from illegal private conduct, the courts have uniformly refused to do so because it would serve no purpose.”); *Commonwealth v. Corley*, 491 A.2d 829, 834 (Pa. 1985) (“Because the exclusionary rule . . . is aimed at ‘official misconduct’, it would be a wholly improper extension to apply it . . . as a remedy for private conduct.”). Accordingly, *Herring*’s exclusionary rule rationale does not affect whether privately-developed FRT can provide probable cause. *See Herring*, 555 U.S. at 139 (“[W]hether the error can be traced to a mistake by a *state actor* or *some other source* may bear on the analysis.” (emphasis added)). Because FRT’s private vendors are outside the exclusionary rule’s ambit, it is appropriate to curtail FRT’s errors by limiting FRT’s role in providing probable cause.

235. These algorithmic biases are more dangerous than *Herring*’s bookkeeping errors. *See Joy Buolamwini, Artificial Intelligence Has a Problem with Gender and Racial Bias. Here’s How to Solve It*, TIME (Feb. 7, 2019), <https://perma.cc/DW9G-5VLX> (highlighting that “failed machine learning systems” such as FRT “amplify, rather than rectify” failures in the criminal justice system).

236. *See Ferguson*, *supra* note 8, at 1194 (noting that, in *Herring*, “the Justices . . . acknowledged that recurring [technological] problems would impact Fourth Amendment decisions”).

237. *Herring v. United States*, 555 U.S. 135, 146 (2009); *see Arizona v. Evans*, 514 U.S. 1, 17 (1995) (O’Connor, J., concurring) (“[I]t would not be reasonable for the police to rely, say, on a recordkeeping system . . . that has no mechanism to ensure its accuracy over time and that routinely leads to false arrests . . .”).

238. *See Florida v. Jimeno*, 500 U.S. 248, 250 (1991) (“The touchstone of the Fourth Amendment is reasonableness.”).

on cannot provide probable cause.²³⁹ Moreover, the Court explained that “it might be reckless for officers to rely on” technology plagued by “systemic errors.”²⁴⁰

If police knowingly use FRT that routinely misidentifies suspects, *Herring* could prevent that FRT from establishing probable cause.²⁴¹ For instance, in Detroit, the Police Chief admitted that if his department used FRT alone to identify people, “96 percent of the time it would misidentify.”²⁴² Though probable cause evades fixed percentages,²⁴³ relying on FRT that misidentifies people *96 percent of the time* would “routinely lead[] to false arrests” and thus be reckless under *Herring* and prevent probable cause.²⁴⁴

The *Herring* Court ultimately admitted evidence seized without probable cause because of the officers’ “good-faith” belief that the faulty database was accurate.²⁴⁵ The defective database could not provide probable cause,²⁴⁶ but the officers could reasonably rely on it because they did not know about its flaws.²⁴⁷ Under *Herring*, the exclusionary rule, with its purpose of deterring police misconduct, only applies when officers deliberately or recklessly overlook their policing tools’ errors.²⁴⁸

239. See *Herring*, 555 U.S. at 145 (discussing how police reliance on false information from reckless or grossly negligent sources can void probable cause).

240. *Id.* at 146.

241. See Ferguson, *supra* note 8, at 1194–95 (commenting that “*Herring* turned on the lack of recurring errors in the arrest warrant database[, and] similarly, in *Utah v. Strieff*, both the majority and dissent recognized that proof of systemic violations would have impacted the analysis” (footnote omitted)).

242. Jason Koebler, *Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time*, VICE (June 29, 2020, 12:56 PM), <https://perma.cc/S4KW-4UHE>.

243. *United States v. Harris*, 568 U.S. 237, 244 (2013).

244. See Ferguson, *supra* note 8, at 1195 (“One would hope that intentionally choosing an 80% error rate in a facial recognition system . . . qualifies as recklessly promoting error.”).

245. *Herring*, 555 U.S. at 136–37, 143–45.

246. *Id.* at 136.

247. *Id.* at 143–45.

248. See *id.* at 144 (“[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.”).

FRT is one such policing tool hampered by erroneous data. By spotlighting FRT's error rates and biases, scholars and journalists aim to increase public knowledge about FRT, including calling on police to acknowledge FRT's flaws.²⁴⁹ When an officer knows of FRT's flaws but chooses to ignore them, that conduct may be "deliberate, reckless, or grossly negligent," and thus weaken the officer's good-faith reliance on FRT.²⁵⁰

Justice Ginsburg's dissent in *Herring* called for greater judicial scrutiny of technology beset by flawed data in probable cause cases.²⁵¹ She argued that judges should use the exclusionary rule to hold police accountable for their errant electronic databases.²⁵² Her opinion emphasized that "inaccuracies in expansive, interconnected collections of electronic information raise grave concerns for individual liberty."²⁵³ Furthermore, the "risk of error stemming from these databases is not slim" due to insufficient monitoring.²⁵⁴

Justice Ginsburg's concerns about police databases apply squarely to FRT. FRT often draws on vast national databases of photos.²⁵⁵ Some FRT databases utilize images obtained without the subject's consent.²⁵⁶ These FRT databases and the law enforcement agencies that use them typically receive little oversight or quality control.²⁵⁷ As Justice Ginsburg warned, these circumstances create a risk of error in FRT use that courts

249. See GARVIE, *supra* note 35, at 65–68 (providing twelve recommendations to law enforcement agencies regarding FRT usage).

250. See *Arizona v. Evans*, 514 U.S. 1, 17 (1995) (O'Connor, J., concurring) (noting that officers could not reasonably rely on technology they knew to be faulty); *supra* note 244 and accompanying text.

251. See *Herring v. United States*, 555 U.S. 135, 148–49 (2009) (Ginsburg, J., dissenting) ("[T]he most serious impact of the Court's holding will be on innocent persons wrongfully arrested based on erroneous information carelessly maintained in a computer data base." (internal quotation omitted)).

252. *Id.* at 157 ("Negligent recordkeeping errors by law enforcement threaten individual liberty, are susceptible to deterrence by the exclusionary rule, and cannot be remedied effectively through other means.").

253. *Id.* at 155.

254. *Id.*

255. Ferguson, *supra* note 8, at 1114–15.

256. Solon, *supra* note 29; Keyes et al., *supra* note 29.

257. See Garvie, *supra* note 47 ("[I]mprovements [to FRT] won't matter much if there are no standards governing what police departments can feed into these systems.").

cannot ignore. Courts can avoid the situations that the exclusionary rule exists to redress by taking a hard look at FRT and precluding it as the sole source of probable cause.

Like *Herring's* warrant database populated by faulty entries, courts should restrict FRT driven by faulty data from providing probable cause. The Court's opinion in *Kansas v. Glover*²⁵⁸ bolsters this reasoning. In *Glover*, the Court discussed whether information from a police database can justify a traffic stop.²⁵⁹ There, a policeman ran a pickup truck's license plate number through a state database.²⁶⁰ The database indicated that Glover owned the truck and had a revoked driver's license.²⁶¹ The officer then matched the truck's plates, make, and model against the database information, and pulled Glover over.²⁶²

The Court found that the officer had reasonable suspicion to stop Glover because of what the officer learned from the database plus two "commonsense inference[s]" from that information.²⁶³ One, that the truck's owner was likely its driver,²⁶⁴ and, two, that "[d]rivers with revoked licenses frequently continue to drive and therefore to pose safety risks to other motorists and pedestrians."²⁶⁵

Glover's focus on the officer's inferences indicates the importance of establishing that the officer's reasonable suspicion did not solely rely on the police database.²⁶⁶ Justice Kagan's concurrence strengthens this notion, as she zeroed in on the fact that a revoked license is a strong indicator of a

258. 140 S. Ct. 1183 (2020).

259. *Id.* at 1190.

260. *Id.* at 1187.

261. *Id.*

262. *Id.* at 1188.

263. *See id.* ("From these . . . facts, Deputy Mehrer drew the commonsense inference that Glover was likely the driver of the vehicle, which provided more than reasonable suspicion to initiate the stop.")

264. *Id.*

265. *Id.*; *see id.* at 1192 (Kagan, J., concurring) (explaining that because "Kansas almost never revokes a license except for serious or repeated driving offenses . . . a person with a revoked license has already shown a willingness to flout driving restrictions.")

266. *See id.* at 1188 (majority opinion) ("[C]ombining database information and commonsense judgments in this context is fully consonant with this Court's Fourth Amendment precedents.")

“p penchant for ignoring driving laws.”²⁶⁷ She “would find this a different case if Kansas barred Glover from driving” on grounds separate from his history of breaking traffic laws.²⁶⁸ Justice Kagan’s reasoning signals that the database identification alone was not dispositive.²⁶⁹

Glover’s implication that database information, on its own, is insufficient to sustain reasonable suspicion bolsters the idea that an FRT identification alone cannot create probable cause.²⁷⁰ Reasonable suspicion is a “less demanding standard than probable cause”²⁷¹—if a database cannot provide reasonable suspicion, it cannot clear probable cause’s higher hurdle. The same goes for FRT, a digital policing tool that, unlike *Glover’s* database, also suffers from demographic biases.²⁷²

b. Federal Appellate Court Scrutiny of Police Databases

The Ninth and Tenth Circuits have also considered the relationship between probable cause and faulty data in databases. In *United States v. Esquivel-Rios*,²⁷³ then-Judge Neil Gorsuch opined on what happens when “the computer suggests you’ve broken the law only because of bad data.”²⁷⁴ In that case, a Kansas trooper performed a traffic stop “based *solely* on a database with apparent credibility problems.”²⁷⁵ The trooper noticed a minivan bearing a “Colorado temporary 30-day registration tag.”²⁷⁶ He then called a dispatcher to verify the tag

267. *Id.* at 1192 (Kagan, J., concurring).

268. *Id.*

269. *See id.* at 1194 (pointing out that “cases with more complete records” could come to a different conclusion on reasonable suspicion).

270. *See id.* at 1188 (majority opinion) (“Because it is a less demanding standard, reasonable suspicion can be established with information that is different in quantity or content than that required to establish probable cause.” (internal quotation marks omitted)).

271. *Illinois v. Wardlow*, 528 U.S. 119, 123 (2000).

272. *See* NIST PART 3, *supra* note 40, at 2, 63; BUOLAMWINI & GEBRU, *supra* note 41, at 10.

273. 725 F.3d 1231 (10th Cir. 2013) (Gorsuch, J.).

274. *Id.* at 1234.

275. *Id.* at 1237.

276. *Id.* at 1234.

in a Kansas police database.²⁷⁷ The dispatcher responded that the tag number did not show up in the database, but “*also* added that ‘*Colorado temp tags usually don’t return.*’”²⁷⁸ The trooper stopped the minivan and found methamphetamine inside.²⁷⁹

In finding that reasonable suspicion (a lower standard than probable cause)²⁸⁰ supported the trooper’s stop, “the district court overlooked one critical circumstance”—the dispatcher’s comment “casting doubt on [the database’s] reliability.”²⁸¹ On appeal, the Tenth Circuit admonished this failure to consider the database’s unreliability in finding reasonable suspicion.²⁸² Though Judge Gorsuch did not decide whether the database could provide reasonable suspicion,²⁸³ his opinion suggests that policing predicated on information from unreliable technology requires a hard look at that technology.²⁸⁴

Esquivel-Rios’s discussion of bad inputs in databases applies to FRT’s reliance on flawed data. Failing to use diverse datasets to train FRT creates racial, gender, and age biases.²⁸⁵ These biases create the danger that FRT will “suggest[] you’ve broken the law only because of bad data.”²⁸⁶ As *Esquivel-Rios* implies, courts should closely examine FRT’s flawed data in probable cause inquiries.

Building on *Esquivel-Rios*, the Ninth Circuit in *Gonzalez v. United States Immigration and Customs Enforcement*,²⁸⁷ expressly discussed whether flawed databases could provide

277. *Id.*

278. *Id.* at 1235.

279. *Id.* at 1234–35.

280. *Wardlow*, 528 U.S. at 123.

281. *Esquivel-Rios*, 725 F.3d at 1238.

282. *See id.* (“Simply put, the district court failed to engage with evidence seeming to call the database into question.”).

283. *See id.* at 1238–39 (remanding the case and ordering the trial court to consider the database’s unreliability).

284. *See* Andrew G. Ferguson, *The Exclusionary Rule in the Age of Blue Data*, 72 VAND. L. REV. 561, 593 (2019) (explaining that in *Esquivel-Rios*, the court “recognized that in order to decide the suppression issue, it needed to understand the type and magnitude of errors in the database”).

285. NIST PART 3, *supra* note 40, at 2, 63; BUOLAMWINI & GEBRU, *supra* note 41, at 10.

286. *United States v. Esquivel-Rios*, 725 F.3d 1231, 1234 (10th Cir. 2013); *see infra* Part III.B.2.

287. 975 F.3d 788 (9th Cir. 2020).

probable cause. Immigration and Customs Enforcement (ICE) mistakenly detained Gerardo Gonzalez, a U.S. citizen, because an ICE database “flagged Gonzalez’s birthplace as being in Mexico, and the agent could not find records showing that Gonzalez had lawfully entered the United States” in corresponding databases.²⁸⁸

Gonzalez sued ICE, challenging its practice of making probable cause determinations “based solely on searches of electronic databases.”²⁸⁹ The district court ruled in Gonzalez’s favor, finding that “ICE violates the Fourth Amendment by relying on an unreliable set of databases to make probable cause determinations.”²⁹⁰ On appeal, the Ninth Circuit discounted the conclusion that ICE’s database system was unreliable. After all, the district court only analyzed some databases, not the database system as a whole.²⁹¹ The Ninth Circuit remanded the case for more factfinding and clarified that “howsoever a database is unreliable, the ultimate inquiry is whether the database provides officers with reasonably trustworthy information for determining probable cause.”²⁹² A database’s unreliability can be measured by the “data it contains” and how many unlawful arrests the database causes.²⁹³

Gonzalez’s test for database reliability is akin to *Florida v. Harris’s* test for probable cause and can likewise apply to FRT. Both tests account for the flawed data that FRT relies on and the demographic biases that FRT manifests.²⁹⁴ This

288. *Id.* at 797.

289. *Id.* at 820.

290. *Gonzalez v. ICE*, 416 F. Supp. 3d 995, 1081 (C.D. Cal. 2019), *rev’d*, 975 F.3d 788 (9th Cir. 2020).

291. *See Gonzalez*, 975 F.3d at 821 (“[T]he district court did not make reliability findings for *all* the databases on which ICE relies.”); *id.* at 822 (concluding that the lower court failed to “explain how this *system* of databases results in unreliable probable cause determinations”).

292. *Id.* at 820; *see id.* at 823 (remanding the case to the district court “to reconsider the claim . . . by making additional findings of fact as are necessary to properly resolve it”).

293. *Id.* at 820, 822–23.

294. *Compare id.* (instructing the district court to look at the data in a database and the outcomes that the database perpetuates), *with Florida v. Harris*, 568 U.S. 237, 247 (2013) (clarifying that a dog’s training and its field performance are relevant to whether that dog’s drug-sniffing alert can provide probable cause).

combination of faulty data and biases prevents an FRT match, on its own, from providing reasonably trustworthy information to create probable cause.²⁹⁵

2. Race, Gender, and Age Biases

FRT's racial, gender, and age biases strengthen the case for barring FRT as a sole source of probable cause. FRT's demographic-based misidentifications impermissibly inject race, gender, and age discrimination into probable cause inquiries—repackaging human biases under the guise of cold, technological objectivity.²⁹⁶ Precluding probable cause based solely on FRT comports with probable cause case law and the noted importance of “combating racial discrimination in the administration of justice.”²⁹⁷ Though the most relevant precedents focus on racial discrimination,²⁹⁸ this analysis of race in probable cause applies equally to gender, age, and the intersection of two or all three of these characteristics.

In *United States v. Brignoni-Ponce*,²⁹⁹ the Supreme Court decided that race alone cannot justify a traffic stop.³⁰⁰ U.S. Border Patrol officers in southern California stopped a car to question its occupants about their citizenship and immigration

295. An FRT identification alone may suffice to create reasonable suspicion, which is a lower standard than probable cause. *See Alabama v. White*, 496 U.S. 325, 330 (1990) (“[R]easonable suspicion can be established with information that is different in quantity or content than that required to establish probable cause . . . [and] can arise from information that is less reliable than that required to show probable cause.”).

296. *See* Barrett, *Ban Facial Recognition*, *supra* note 25, at 245 (discussing the human tendency “to trust the judgment of computers over their own without a rational basis to do so”); Joy Buolamwini, Opinion, *When the Robot Doesn't See Dark Skin*, N.Y. TIMES (June 21, 2018), <https://perma.cc/27AM-ZQVA> (“[A]rtificial intelligence, often heralded for its potential to change the world, can actually reinforce bias and exclusion, even when it's used in the most well-intended ways.”).

297. *Rose v. Mitchell*, 443 U.S. 545, 558 (1979).

298. *See, e.g., United States v. Brignoni-Ponce*, 422 U.S. 873, 886–87 (1975) (stating that race alone cannot justify a traffic stop, let alone establish probable cause).

299. 422 U.S. 873 (1975).

300. *Id.* at 886–87; *see Gonzales-Rivera v. INS*, 22 F.3d 1441, 1449 (9th Cir. 1994) (noting that a “stop based solely on race” is “proscribed by *Brignoni-Ponce*”).

status.³⁰¹ The officers gave only one reason for the stop: because the vehicle’s “three occupants appeared to be of Mexican descent.”³⁰² In a 9–0 decision, the Court declared that the occupants’ apparent Mexican ancestry alone could not provide reasonable suspicion to justify the stop.³⁰³ “The likelihood that any given person of Mexican ancestry is an alien . . . does not justify stopping all Mexican-Americans to ask if they are aliens.”³⁰⁴

Probable cause is a more demanding standard than *Brignoni-Ponce*’s reasonable suspicion.³⁰⁵ Race alone cannot create reasonable suspicion, so race alone cannot satisfy probable cause’s higher standard.³⁰⁶ An individual’s race cannot provide a reasonable belief that the individual “had committed or was committing an offense.”³⁰⁷ A suspect’s racial identity does not allow officers to infer that anyone sharing that identity might be the suspect and should be arrested.³⁰⁸

The same is true for gender, age, and combinations of race, gender, and age. For example, in *Davis v. Mississippi*,³⁰⁹ the Supreme Court noted, and the State conceded, that probable

301. *Brignoni-Ponce*, 422 U.S. at 874–75.

302. *Id.* at 875.

303. *Id.* at 886–87.

304. *Id.* at 876–77.

305. See *Illinois v. Wardlow*, 528 U.S. 119, 123 (2000).

306. See *Coleman v. State*, 562 A.2d 1171, 1175 (Del. 1989) (“The majority of Courts have held that race, as a single criteria, provides an insufficient basis for the detention or arrest of a suspect.”); *Brown v. City of Oneota*, 235 F.3d 769, 776 (2d Cir. 2000) (Walker, C.J., concurring) (“[S]tops based on racial considerations alone . . . would almost never rest on the constitutionally required reasonable articulable suspicion of criminal activity . . . and *a fortiori* would never rise to the level of probable cause . . .” (internal citation and quotation omitted)).

307. *Gerstein v. Pugh*, 420 U.S. 103, 111 (1975) (providing the probable cause standard); *cf.* *United States v. Montero-Camargo*, 208 F.3d 1122, 1134 (9th Cir. 2000) (declaring that an individual’s Hispanic appearance “casts too wide a net to play any part in a particularized reasonable suspicion determination”).

308. See *United States v. Sokolow*, 490 U.S. 1, 12 (1989) (Marshall, J., dissenting) (“[T]he Fourth Amendment protects innocent persons from being subjected to overbearing or harassing police conduct carried out solely on the basis of imprecise stereotypes of what criminals look like, or on the basis of irrelevant personal characteristics such as race.” (internal quotations and citations omitted)).

309. 394 U.S. 721 (1969).

cause could not exist where the alleged victim only identified her attacker's race, gender, and age.³¹⁰ Relying on *Davis*, the Third Circuit recognized that identifying suspects by their race and gender alone, or by their race and age alone, does not support probable cause.³¹¹ The Fourth and Ninth Circuits have also recognized that probable cause cannot arise from race and gender combined,³¹² as have lower courts at the state and federal levels.³¹³

Likewise, in *Brown v. City of Oneota*,³¹⁴ the Second Circuit realized the futility of basing reasonable suspicion, a lower standard than probable cause, on an individual's race, gender, and age. Though the court's Fourth Amendment discussion focused on whether a seizure occurred,³¹⁵ the court commented that law enforcement would have "difficulty demonstrating

310. See *id.* at 726 ("The State's brief also candidly admits that 'all that the Meridian Police could possibly have known about [the defendant] at the time . . . would not amount to probable cause for his arrest . . .'" (omissions in original)).

311. See *Edwards v. City of Philadelphia*, 860 F.2d 568, 571 n.2 (3d Cir. 1988) (explaining that a description of suspects as "two 'black males,'" without more, "would not have been sufficient to provide probable cause"); *United States ex rel. Wright v. Cuyler*, 563 F.2d 627, 630 (3d Cir. 1977) ("It is obvious that race and age alone . . . do not furnish probable cause.").

312. See *Smith v. Munday*, 848 F.3d 248, 252 (4th Cir. 2017) ("[A] criminal history, common race, common gender, and unfortunately common name is not enough to establish probable cause."); *Washington v. Lambert*, 98 F.3d 1181, 1192 (9th Cir. 1996) (finding no probable cause where "[a]t most there were two African-American men, one short and one tall . . . at night, who appeared to a police officer to be both nervous and casual").

313. See *State v. Hill*, 465 N.W.2d 309, 311 (Iowa Ct. App. 1990) ("We note the 'M/B [black male]' description by itself would not be specific enough for a search warrant." (alteration in original)); *Lawson v. City of Coatesville*, No. 12-6100, 2013 WL 4596129, at *5 (E.D. Pa. Aug. 29, 2013) (recognizing that if the defendant was "arrested simply because he was a black man in the vicinity of the robbery, the officers would not have had probable cause to arrest him").

314. 221 F.3d 329 (2d Cir. 2000).

315. See *id.* at 340 (evaluating the law enforcement officers' argument that "no seizure . . . occurred in this case"). The Second Circuit also found that absent evidence of discriminatory animus, law enforcement did not violate the Fourteenth Amendment's Equal Protection Clause when officers stopped over 200 Black men in a small town because the suspect was a young Black man. *Id.* at 333-34. *Brown's* Fourteenth Amendment analysis sparked intense debate. See generally Peter A. Lyle, *Racial Profiling and the Fourth Amendment: Applying the Minority Victim Perspective to Ensure Equal Protection Under the Law*, 21 B.C. THIRD WORLD L.J. 243 (2001).

reasonable suspicion” when officers only knew a suspect’s race, gender, and age.³¹⁶ The State did not even attempt such an argument.³¹⁷ In *Brown*, the Second Circuit alluded to what its sister circuits and the Supreme Court in *Davis* more readily recognized: an individual’s race, gender, and age, alone or in tandem, cannot, without more, sustain reasonable suspicion, let alone meet the higher bar of probable cause.

Probable cause premised solely on FRT raises the same problems as probable cause based solely on race, gender, and age. FRT carries the risk of race, gender, or age-based misidentifications.³¹⁸ As such, relying solely on FRT for probable cause places undue weight on race, gender, and age.³¹⁹ Giving such weight to these demographic factors opens the door to impermissible race, gender, or age-based probable cause findings.³²⁰ Such findings “based on race send the underlying message to all our citizens that those who are not white are judged by the color of their skin alone.”³²¹ Using FRT as the sole basis of probable cause broadcasts the same discriminatory message to women, older people, and young people.³²² Where these discriminatory messages intersect, such as for young Black women, their pernicious effects multiply.³²³

316. *Brown*, 221 F.3d at 340.

317. *Id.*

318. NIST PART 3, *supra* note 40, at 2, 63; BUOLAMWINI & GEBRU, *supra* note 41, at 10.

319. *See* NIST PART 3, *supra* note 40, at 18 (reporting a “large false positive differential across sex, age and race”); BUOLAMWINI & GEBRU, *supra* note 40, at 11 (explaining how race and gender can cause large variations in error rates).

320. *See* *United States v. Martinez-Fuerte*, 428 U.S. 543, 571 n.1 (1976) (Brennan, J., dissenting) (“That law in this country should tolerate use of one’s ancestry as probative of possible criminal conduct is repugnant under any circumstances.”).

321. *United States v. Montero-Camargo*, 208 F.3d 1122, 1135 (9th Cir. 2000).

322. *See supra* Part I.B.

323. *See* Kimberlé Crenshaw, *Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics*, 1989 U. CHI. LEGAL F. 139, 140 (1989) (“Because the intersectional experience is greater than the sum of racism and sexism, any analysis that does not take intersectionality into account cannot sufficiently address the particular manner in which Black women are subordinated.”).

Discrimination in the criminal justice system “undermines public confidence in the fairness of our system of justice.”³²⁴ The Supreme Court has been emphatic in its desire to stamp out such discrimination,³²⁵ but relying solely on FRT for probable cause enmeshes race, gender, and age biases into probable cause findings.³²⁶ Curtailing and clarifying FRT’s role in probable cause cases can lessen discrimination, especially racial discrimination,³²⁷ in the criminal justice system.³²⁸

A critic might argue that this Note’s probable cause analysis is incompatible with *Whren v. United States*.³²⁹ There, the Supreme Court observed that “the constitutional basis for objecting to intentionally discriminatory application of laws is the Equal Protection Clause, not the Fourth Amendment.”³³⁰ In *Whren*, police stopped a car after watching its young Black driver commit a traffic infraction.³³¹ Observing the traffic violation established probable cause to make the stop.³³² The defendant argued that the officer’s ulterior motives invalidated an otherwise “objectively justifiable” stop.³³³ The Court responded that the officer’s “subjective intent alone” could not “make otherwise lawful conduct illegal or unconstitutional.”³³⁴

324. *Batson v. Kentucky*, 476 U.S. 79, 87 (1986).

325. *See Rose v. Mitchell*, 443 U.S. 545, 555 (1979) (“Discrimination on the basis of race, odious in all aspects, is especially pernicious in the administration of justice.”); *Batson*, 476 U.S. at 87–88 (“Discrimination within the judicial system is most pernicious because it is a stimulant to that race prejudice which is an impediment to securing to black citizens that equal justice which the law aims to secure to all others.” (internal quotation omitted)).

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

327. *See Jain, supra* note 22, at 1232–33 (spotlighting entrenched racial biases in the criminal justice system).

328. *See Barrett, Ban Facial Recognition, supra* note 25, at 249 (“The opaque use of facial recognition systems that misidentify people of color exacerbates other forms of structural racism in the criminal justice system.”).

329. 517 U.S. 806 (1996).

330. *Id.* at 813.

331. *Id.* at 808–10.

332. *Id.* at 806.

333. *Id.* at 811–12.

334. *Id.* at 813.

Thus, “[s]ubjective intentions play no role in ordinary, probable-cause Fourth Amendment analysis.”³³⁵

When law enforcement officers rely on FRT alone to establish probable cause, those officers’ intentions, subjective or otherwise, are immaterial to the FRT’s biases and error rates.³³⁶ FRT produces the same outputs no matter who uses it.³³⁷ Though FRT is purportedly neutral, it relies on biased data that generates biased misidentifications.³³⁸ FRT does not intentionally discriminate, it simply follows its algorithms.³³⁹ Precluding FRT from being the sole source of probable cause curtails FRT and its biases, not those of an officer. *Whren’s* pronouncements about human intentions are inapplicable to FRT’s algorithmic biases.

3. Public Support for Curtailing FRT in Probable Cause Cases

Prohibiting FRT from being the sole source of probable cause finds support among law enforcement, lawmakers, and FRT developers. The NYPD, who used FRT in over 7,000 searches in 2018,³⁴⁰ adopted this policy.³⁴¹ Among law enforcement agencies with published FRT policies, agencies at both the local and federal levels agree that an FRT identification does not establish probable cause.³⁴² Likewise, many FRT

335. *Id.*

336. See NIST PART 2, *supra* note 39, at 3 (commenting that individual FRT’s users should be aware of accuracy differences between different FRT).

337. See WHITE ET AL., *supra* note 46, at 10 (discussing how different human operators respond to the same FRT outputs). Individual human error can exacerbate FRT error rates. See *id.* at 42 (“These results have clear implications for the reliability of identity verification systems that employ human operators to monitor the output of FR software.”).

338. NIST PART 3, *supra* note 40, at 2, 63; BUOLAMWINI & GEBRU, *supra* note 41, at 10.

339. See BUOLAMWINI & GEBRU, *supra* note 40, at 1 (“[F]ace recognition tools[] rely on machine learning algorithms that are trained with labeled data.”).

340. O’Neill, *supra* note 47.

341. NYPD, *supra* note 122, at 1.

342. See Jon Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC NEWS (May 11, 2019, 4:19 AM), <https://perma.cc/6DM7-EVCV> (quoting a Colorado investigator who stated that FRT cannot establish probable cause); Valentino-DeVries, *supra* note 60 (“Law enforcement officials

companies maintain that their technology only creates leads, not probable cause.³⁴³

Advocates in multiple states are gathering momentum against FRT as the sole basis of probable cause. As part of a broader FRT law,³⁴⁴ Washington State bans “state or local law enforcement agenc[ies from] . . . us[ing] the results of a facial recognition service as the sole basis to establish probable cause in a criminal investigation.”³⁴⁵ Likewise in Alabama, “[a] state or local law enforcement agency may not use facial recognition technology match results as the sole basis to establish probable cause in a criminal investigation or to make an arrest.”³⁴⁶ State legislatures in Colorado,³⁴⁷ Hawaii,³⁴⁸ Maryland,³⁴⁹ New York,³⁵⁰ and Virginia³⁵¹ are trying to pass similar bills.³⁵² This broad support for barring FRT as the only basis of probable cause

in Florida and elsewhere emphasized that facial recognition should not be relied on to put anyone in jail.”); DEP’T OF HOMELAND SEC., *supra* note 122 (stating ICE’s policy that FRT cannot create probable cause).

343. See Shira Ovide, *When the Police Treat Software Like Magic*, N.Y. TIMES (June 25, 2020), <https://perma.cc/J4SL-H2W4> (“The technology companies say none of [FRT’s identifications are] probable cause for arrest.”); *Facial Recognition Code of Ethics*, RANK ONE COMPUTING (Nov. 22, 2019), <https://perma.cc/2XGQ-6LPV> (“Facial recognition should not support probable cause for arrest, search or seizure.”); Memorandum from Paul D. Clement, Esq. to Clearview AI, Inc. 2 (Aug. 14, 2019), <https://perma.cc/33KT-9HJ7> (PDF) (“The results from a Clearview search are not intended or designed to . . . demonstrat[e] probable cause to obtain a warrant or otherwise.”).

344. See Ryan Tracy, *Washington State OKs Facial Recognition Law Seen as National Model*, WALL ST. J. (Mar. 31, 2020, 4:34 PM), <https://perma.cc/4937-JL57> (reporting on “the most detailed regulations of facial recognition in the U.S.”).

345. WASH. REV. CODE § 43.386.080(5) (2021).

346. 2022 Ala. Acts 420, <https://perma.cc/SRQ2-GEQY>.

347. S.B. 113, 73d Gen. Assemb., 2d Reg. Sess. (Colo. 2022).

348. S.B. 2005, 31st Leg. (Haw. 2022); S.B. 2293, 31st Leg. (Haw. 2022).

349. S.B. 762, 442d Gen. Assemb., Reg. Sess. (Md. 2022); H.B. 1046, 442d Gen. Assemb., Reg. Sess. (Md. 2022).

350. A.B. 768, 2021 Assemb., 244th Sess. (N.Y. 2021).

351. H.B. 1339, 2022 Leg., 2022 Sess. (Va. 2022). A bill in Virginia’s Senate goes further, barring the use of FRT matches in affidavits to establish probable cause. S.B. 741, 2022 Leg., 2022 Sess. (Va. 2022).

352. On April 8, 2022, Kentucky adopted a law establishing a working group that will create a model policy for law enforcement. 2022 Ky. Acts 147. The policy will address, among other things, “[h]ow search results using facial recognition technology relate to establishing probable cause for arrests.” *Id.*

strengthens the argument that FRT can be a factor but not *the* factor in establishing probable cause.

Growing scholarly critiques of FRT on other constitutional grounds further support limiting FRT in probable cause cases. Professor Andrew Guthrie Ferguson dedicated a recent law review article to identifying additional Fourth Amendment issues, including whether FRT surveillance violates reasonable expectations of privacy.³⁵³ Professor Samuel Hodge and Georgetown Law's Clare Garvie are among those who argue that using FRT at political protests chills speech protected by the First Amendment.³⁵⁴ Finally, Professor Sonia Gipson Rankin argues that the absence of "evidentiary mechanisms to question algorithmic accusers [like FRT] violates the intent of the Sixth Amendment's Confrontation Clause."³⁵⁵ Barring FRT as the sole basis of probable cause is a small price to pay for protecting the innocent from misidentification and wrongful arrest.³⁵⁶

CONCLUSION

Greater judicial oversight of FRT in probable cause inquiries and curbing FRT from providing the sole source of probable cause will help prevent wrongful arrests and combat injustices like those that Robert Julian-Borchak Williams, Michael Oliver, and Nijeer Parks faced. Publicly airing FRT's error rates and biases will better inform judges and defense attorneys of how, when, and why law enforcement use FRT. Police rarely publicize FRT use,³⁵⁷ and recognizing when FRT leads to an arrest is difficult.³⁵⁸ Thus, FRT-based policing often

353. See Ferguson, *supra* note 8, at 1140–47.

354. Hodge, *supra* note 37, at 73–74; Clare Garvie, *Public Protest, Face Recognition, and the Shield of Anonymity*, CTR. ON PRIV. & TECH. AT GEO. L. (June 9, 2020), <https://perma.cc/XC9A-K8PB>.

355. Gipson Rankin, *supra* note 114, at 707 (discussing Sixth Amendment concerns).

356. See 2 WILLIAM BLACKSTONE, COMMENTARIES *358 (“[I]t is better that ten guilty persons escape than that one innocent suffer.”).

357. Jackson, *supra* note 59; Valentino-DeVries, *supra* note 60.

358. See Jackson, *supra* note 59, at 15–16 (describing the challenges of “recogniz[ing] cases where facial recognition was used”).

occurs behind the scenes and without oversight.³⁵⁹ Requiring judicial review of FRT's flaws in probable cause cases encourages transparency by generating discussions in the courtroom about FRT's faults.³⁶⁰ Publicizing FRT's shortcomings can also assist defense attorneys in challenging FRT outside of the probable cause context.³⁶¹

Better judicial oversight of FRT can also increase police accountability and encourage police to learn about the FRT they use. Creating a written record of FRT use in affidavits and probable cause hearings can "allow[] for a measure of transparency, accountability, and avoidance of abuse."³⁶² Increased judicial focus on FRT's flaws can also serve as a de facto audit on a particular law enforcement agency's FRT,³⁶³ incentivizing officers to comprehend and mitigate FRT's flaws when establishing probable cause.³⁶⁴ For instance, if one FRT struggles to identify Black women, officers could mitigate that flaw by using extra investigatory means to assess whether a Black woman that FRT identified is the correct suspect. Though officers may not exercise such diligence in every case,³⁶⁵ encouraging police to better understand FRT's flaws is a positive goal. Judicial ventilation of FRT's role in probable cause inquiries adds an extra layer of protection, transparency, and

359. See Valentino-DeVries, *supra* note 60 (documenting the lack of record-keeping for FRT usage); Garvie, *supra* note 47 (reporting on inconsistent or non-existent FRT training in police departments).

360. See Ferguson, *supra* note 8, at 1201–02 (arguing that requiring courts to document how and when police use FRT will increase transparency surrounding FRT use).

361. See Jackson, *supra* note 59, at 17 (identifying the difficulties of challenging FRT in court).

362. Ferguson, *supra* note 8, at 1201.

363. See *id.* at 1207 (advocating auditing law enforcement FRT use to "both offer a measure of practical accountability to prevent misuse, [and] also ensure that the technology is improving in accuracy and precision and not harming particular communities").

364. Cf. *Florida v. Harris*, 568 U.S. 237, 247 (2013) (recognizing that "law enforcement units have their own strong incentive" to ensure proper training of their drug dogs so that those units can use their drug dogs to establish probable cause).

365. See, e.g., Anderson, *supra* note 51 (recalling that police trusted FRT to make an arrest, despite obvious physical differences between the suspect and man the FRT identified).

accountability that will hopefully decrease needless police action premised on FRT.

Restricting probable cause based solely on an FRT match likewise lowers the risk of wrongful arrests based on FRT's biased algorithms. This restriction finds support in precedent, police stations, and state legislatures. It also advances the purpose of requiring probable cause to arrest—to “protect[] citizens from rash and unreasonable interferences with privacy and from unfounded charges of crime.”³⁶⁶

Admittedly, advances in FRT could change this Note's analysis, particularly concerning FRT as the sole source of probable cause. FRT vendors can better train their technologies with more diverse data sets to address demographic biases and error rates.³⁶⁷ But improving FRT is only half the battle. Better technology will only make a difference if police widely adopt it.³⁶⁸ Widespread adoption requires hundreds of law enforcement agencies to have the means and motivation to upgrade their FRT.³⁶⁹

If police widely adopt accurate and unbiased FRT, courts *could* consider lifting a bar on probable cause based solely on FRT. But any such decision must seriously contemplate the myriad of other problems such powerful technology creates.³⁷⁰ After all, police can “enjoy the substantial advantages [that] technology confers. They may not, however, rely on it blindly. With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities.”³⁷¹

366. *Maryland v. Pringle*, 540 U.S. 366, 370 (2003) (citation omitted).

367. See NIST PART 3, *supra* note 40, at 10 (suggesting that “refined training” and “more diverse training data” could “mitigate[e] demographic differentials with respect to false positives”).

368. See Hill, *Wrongfully Accused*, *supra* note 1 (quoting Clare Garvie, who stated that “[t]here are mediocre algorithms and there are good ones, and law enforcement should only buy the good ones”).

369. See GARVIE, *supra* note 35, at 67–68 (exploring how law enforcement can improve their FRT practices through smarter purchases and federal funding).

370. See generally Ferguson, *supra* note 8; Barrett, *Ban Facial Recognition*, *supra* note 25.

371. *Arizona v. Evans*, 514 U.S. 1, 17–18 (1995) (O'Connor, J., concurring).