The Face of Criminality: Regulating Facial Recognition Technology Through FRT Warrants

ALLISON JONES*

* Notes Editor, Volume 56, and Staff Member, Volume 55, *The University of Memphis Law Review*; Juris Doctor Candidate, 2026, The University of Memphis Cecil C. Humphreys School of Law, 2026. Thank you to Professor Jennifer Brobst for your unwavering support and guidance throughout the Note-writing process. Thank you to my peers, Shannon Crow, Meredith Ehemann, Jada Mitchell, Hailey Polisano, and Ruhiya Mithani, for the time and effort you spent reviewing and editing my Note. Thank you to my village, my parents, siblings, nieces, nephew, and late grandmother, for your presence, love, support, and encouragement.

I. INTRODUCTION

"No, this is not me."[1] In January of 2020, Robert Williams was hauled away from his home by Detroit, Michigan police officers in front of his family.[2] After being held in custody overnight, he was shown two images pulled from a boutique store's surveillance footage.[3] Police relied on facial recognition technology ("FRT") that misidentified Williams as the suspect.[4] They took few investigative steps to corroborate the match before obtaining an arrest warrant for Williams.[5]

Williams and the photographed suspect had only one thing in common: they were both "large-framed Black men."[6] When Williams held the images to his face to demonstrate that he was not the photographed individual, an officer replied, "[t]he computer must have gotten it wrong."[7] Williams only spent one night in police custody, but he and his family continued reliving the trauma long after his release.[8]

Michael Oliver, another African American male, was also wrongfully arrested due to an FRT misidentification.[9] The police officers failed to conduct an independent investigation, which would have revealed apparent corporeal distinctions between Oliver and the actual

---

1. Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; ACLU, *Wrongfully Arrested Because of Flawed Face Recognition Technology*, at 00:20 (YouTube, June 24, 2020), https://www.youtube.com/watch?v=Tfgi9A9PfLU&t=20s.

2. Hill, *supra* note 1.

3. *Id.*

4. *Id.*

5. Anderson Cooper, *Police Departments Adopting Facial Recognition Tech Amid Allegations of Wrongful Arrests*, CBS NEWS (May 16, 2021, at 19:08 ET), https://www.cbsnews.com/news/facial-recognition-60-minutes-2021-05-16/#.

6. Victoria Burton-Harris & Philip Mayor, *Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart*, ACLU (June 24, 2020), https://www.aclu.org/news/privacy-technology/wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart.

7. *Id.*

8. *See id.*

9. NAT'L ACADS. OF SCIS., ENG'G, AND MED., FACIAL RECOGNITION TECHNOLOGY: CURRENT CAPABILITIES, FUTURE PROSPECTS, AND GOVERNANCE 83–84 (2024) [hereinafter NAT'L ACADS.].

suspect.[10] Nevertheless, detectives obtained a warrant for Oliver's arrest based on results from an FRT system known for its alarming false-positive rate.[11] In fact, the police chief estimated that the system misidentified suspects in ninety-six percent of cases.[12] Police detained Oliver for a couple days.[13] Although the criminal charges were dropped, he struggled with economic loss, embarrassment, and difficulty securing employment in the aftermath.[14]

Despite Williams and Oliver spending short durations in police custody, their stories are noteworthy for several reasons. First, they uncover an unfortunate reality: that FRT "disproportionately harms the Black community."[15] Second, they demonstrate how an overreliance on flawed FRT systems can rob innocent individuals of their liberty.[16] Third, without clear guidelines, it is difficult to assert disparate impact,

---

10. *See id.* (revealing that Oliver had tattoos on his arms; the actual thief had none).

11. Elaisha Stokes, *Wrongful Arrest Exposes Racial Bias in Facial Recognition Technology*, CBS NEWS (Nov. 19, 2020, at 07:00 ET), https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/.

12. *Id.*

13. Natalie O'Neill, *Faulty Facial Recognition Led to His Arrest—Now He's Suing*, VICE (Sep. 4, 2020, at 09:39 CT), https://www.vice.com/en/article/faulty-facial-recognition-led-to-his-arrestnow-hes-suing/.

14. Stokes, *supra* note 11.

15. Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Jan. 6, 2021), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

16. *See* NAT'L ACADS., *supra* note 9 (describing other wrongful FRT arrests, each containing unique circumstances that made the inaccuracies of FRT results undeniable). Randal Reid spent six days in jail for a theft that occurred in Louisiana, but Reid had never been to Louisiana. Nijeer Parks spent eleven days in jail for crimes committed thirty miles away from his location. Porcha Woodruff spent eleven hours in jail for crimes committed by someone with clear, physical distinctions. Woodruff was eight months pregnant; the photographed suspect was not. *Id.*; *see also* Maria Cramer & Kashmir Hill, *How the N.Y.P.D.'s Facial Recognition Tool Landed the Wrong Man in Jail*, N.Y. TIMES (Aug. 26, 2025), https://www.nytimes.com/2025/08/26/nyregion/nypd-facial-recognition-dismissed-case.html?smid=url-share (describing a situation wherein Trevis Williams was arrested for publicly flashing a woman despite being eight inches taller than the actual perpetrator and twelve miles away from the location of the incident at the time it occurred).

offer remedies, and mitigate damaging effects. Thus, this Note recommends a warrant requirement for the use of FRT by law enforcement agencies ("LEAs") to balance an individual's Fourth Amendment rights and the government's duty to enhance public safety. This Note advocates for the use of FRT in limited circumstances—recognizing that complete abolition of FRT might maximize individual rights but would overlook considerable benefits associated with its use.[17]

Part II of this Note provides an overview of FRT's history and its current use in the criminal justice system. Part III considers FRT's constitutionality under the Fourth Amendment. Part IV analyzes current state statutes that regulate the use of FRT by LEAs and identifies procedural trends throughout. Part V proposes a warrant requirement for Congress and state legislatures to implement when FRT is used in criminal investigations.

II. FRT BIAS AND EFFICIENCY IN THE CRIMINAL JUSTICE SYSTEM

The origins and development of FRT shed light on its current capabilities and limitations. FRT is a biometric technology that uses images in a database to extract facial characteristics for automated identification.[18] FRT originated in the 1960s when Woody Bledsoe, a computer scientist, taught computers to read up to ten facial patterns, assign a "unique score" to each, and align database images with whichever facial pattern had the closest matching score.[19] Even at its

17. *See, e.g.*, *Biometrics—Identifying Friend or Foe*, NAT'L INST. OF STANDARDS AND TECH. (Aug. 12, 2025), https://www.nist.gov/congressional-and-legislative-affairs/fy07-biometrics-identifying-friend-or-foe [hereinafter *Biometrics*] (recognizing an ability to identify "known or suspected terrorists" as a potential benefit to FRT); *see also* UTAH CODE ANN. § 77-23e-103(2)(c) (West 2025) (allowing FRT use to identify deceased individuals and to assist incapacitated individuals who cannot identify themselves—a use recognized by several other jurisdictions).

18. NAT'L ACADS., *supra* note 9, at 1.

19. Shaun Raviv, *The Secret History of Facial Recognition*, WIRED (Jan. 21, 2020, at 06:00 CT), https://www.wired.com/story/secret-history-facial-recognition/. Today, FRT systems follow a similar process: extract facial characteristics from probe images, create an extraction template, and use the template to compute similarity scores between the probe and database images. NAT'L ACADS., *supra* note 9, at 1. The process of comparing the probe to a single reference image is known as one-to-one comparison, while the process of comparing the probe to the templates of multiple

inception, FRT was cryptic and unfamiliar because it empowered machines with a "dangerously powerful human capacity: the ability to recognize faces."[20] Earlier systems were less sophisticated and could not analyze pose variances or facial complexity.[21] Extensive research efforts led to more accurate and advanced computer algorithms.[22]

By 2000, FRT went from a "hit-or-miss tool" to "a profoundly impactful criminal justice resource."[23] FRT assists with investigations, suspect identification, and crime prevention.[24] Using ultrafast FRT processors, LEAs can process images hundreds of meters away with poor lighting and compare one face to millions of images in a database of known individuals to produce a list of potential matches.[25] Despite its improved performance, bias contributes to error rates that plague FRT and undercut arguments supporting its application to criminal justice.

The National Institute of Standards and Technology has identified three dominant categories of bias in AI systems: systemic bias, human bias, and statistical bias.[26] Each category undermines AI integrity and performance. First, systemic bias results from institutional practices that favor some social groups and devalue others.[27] For

---

individuals from a database is known as one-to-many comparison. *Id.* This Note focuses on the latter.

20. Raviv, *supra* note 19.

21. *Id.*

22. *See Face Recognition Grand Challenge (FRGC)*, NAT'L INST. OF STANDARDS AND TECH. (Mar. 26, 2025), https://www.nist.gov/programs-projects/face-recognition-grand-challenge-frgc (noting how newer algorithms, equipped for higher resolution, three-dimensional images, were ten times as accurate as those developed in the previous decade).

23. *History of NIJ Support for Face Recognition Technology*, NAT'L INST. OF JUST. (Mar. 5, 2020), https://nij.ojp.gov/topics/articles/history-nij-support-face-recognition-technology [hereinafter NIJ].

24. *See* G. Indumathi et al., *Facial Recognition for Criminal Identification*, 44 LIBR. PROGRESS INT'L 1700, 1700 (2024) (describing FRT as a powerful, emerging law enforcement tool).

25. NIJ, *supra* note 23.

26. REVA SCHWARTZ ET AL., TOWARDS A STANDARD FOR IDENTIFYING AND MANAGING BIAS IN ARTIFICIAL INTELLIGENCE, at ii (2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.

27. *Id.* at 6. *See generally* BRANDEIS HILL MARSHALL, DATA CONSCIENCE: ALGORITHMIC SIEGE ON OUR HUMANITY 5, 23 (2023) (noting that the oppression of certain groups via law and science is rooted in slave codes and white supremacy,

example, risk assessments identify an individual's potential risk of repeating an offense and inform a court's decision about which arrestees to set free, bond amounts, and sentence length.[28] The following example reveals how risk assessments perpetuate institutional practices that devalue Black individuals and are more favorable to White individuals. Brisha Borden—Black, eighteen, and female—was late to pick up her god-sister, so Borden and her friend swiped a bike and a scooter belonging to a stranger.[29] Right as Borden and her friend realized they were too big for the bike and scooter, a woman ran toward them and stated that the items belonged to her child; they immediately dropped the items, and walked away.[30] Despite never actually taking the items, Borden and her friend were later charged with burglary and petty theft for the bike and scooter, which were together valued at $80.[31] Vernon Prater—White, forty-one, male, and "the more seasoned criminal"—shoplifted $86 worth of product from a store.[32] The risk assessment classified Borden as a "high risk" future criminal, while Prater was classified as "low risk."[33] In reality, the assessments were incorrect.

---

which reinforced a longstanding bias against African Americans that seeped into the tech industry). Although societal treatment is influenced by racial identity, race is a social construct that encourages division but is largely inconsistent with biological studies. *See* DOROTHY ROBERTS, FATAL INVENTION: HOW SCIENCE, POLITICS, AND BIG BUSINESS RE-CREATE RACE IN THE TWENTY-FIRST CENTURY, at x (2011) ("Human beings, regardless of race, are 99.9 percent the same," and "[b]iologically, there is one human race." (quotation omitted)). Thus, it is problematic to base criminality solely on a person's race.

28. Seena Fazel et al., *The Predictive Performance of Criminal Risk Assessment Tools Used at Sentencing: Systematic Review of Validation Studies*, 81 J. CRIM. JUST. 1, 1 (2022), [https://doi.org/10.1016/j.jcrimjus.2022.101902].

29. Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

30. *Id.*

31. *Id.*

32. *Id.*

33. *Id.* Faception is a company that equipped its FRT system with predictive screening capabilities to "forecast criminal events and public disorder without direct investigation or innocent people interrogations." *See* FACEPTION: FACIAL PERSONALITY ANALYTICS, https://www.faception.com/hls-and-public-safety (last visited Dec. 23, 2025). We cannot be certain that an FRT system is capable of predicting human behavior. This leaves people who committed past crimes without possibility

Borden did not commit subsequent crimes; Prater did.[34] The historical stereotype that African Americans are "irredeemable, dangerous criminals" devalues the African American race and makes the adoption of technology based on that stereotype inherently suspect.[35]

Second, human bias denotes error in human thought resulting from perception and gap-filling unknown information.[36] It reinforces the notion that the human mind sees what it wants and expects to see.[37] An example involves Michael Oliver, discussed above. Surveillance images demonstrated an individual without tattoos; Oliver had visible tattoos on his arms.[38] Nevertheless, officers made subjective decisions to gap-fill where the data was inconsistent with reality. Human bias is the equivalent of saying "close enough." But what appear to be harmless discrepancies could be indicia of innocence rather than guilt.

Third, statistical bias illuminates the effects of underinclusive population samples.[39] Algorithms based on data that lacks diversity struggle to interpret datasets outside their realm of familiarity.[40] Bledsoe's early facial recognition system successfully matched faces within a database of approximately 400 adult male Caucasians; the dataset, however, excluded women and people of color, underscoring the narrow scope of the technology's initial development rather than a comprehensive facial recognition model.[41] Thus, FRT started as a discriminatory tool because its underinclusive samples reinforced societal

---

of redemption and could lead to arrests based on a whim. It also seems impractical that an individual could defend against a machine's assertion that they *will* engage in criminal activity before it ever occurs.

34. Angwin et al., *supra* note 29.

35. MARSHALL, *supra* note 27, at 13 (indicating how slave codes, Black codes, and Jim Crow laws were born of the idea that "Black people's existence is seemingly a threat—a threat worth dedicating government personnel and resources to surveilling"); ROBERTS, *supra* note 27, at 69–70 (discussing how the "opposite race" ideology paints Black individuals as lazy, ignorant criminals).

36. SCHWARTZ ET AL., *supra* note 26, at 9.

37. Sandy L. Zabell, *Fingerprint Evidence*, 13 J.L. & POL'Y 143, 153 (2005).

38. Stokes, *supra* note 11.

39. SCHWARTZ ET AL., *supra* note 26, at 9.

40. *Id.* This limitation is present with human recognition. *See infra* note 69 and accompanying text (discussing own-race bias—the phenomenon that humans struggle to recognize faces belonging to a race outside their own).

41. MARK ANDREJEVIC & NEIL SELWYN, FACIAL RECOGNITION 7–8 (2022).

oppression, which devalued women and people of color.[42] Modern FRT datasets still struggle with inclusivity despite being used across the board to interpret facial patterns.[43]

These categories are intertwined and can lead to skewed results.[44] Effective systems target each, recognizing that biased technology can be "exploited and used as a weapon at scale, causing catastrophic harm."[45] Biased technology could be used by LEAs to criminalize minorities under the guise of public safety.[46] FRT inadequacies can have far-reaching effects when algorithms are used to determine the face of criminality.[47]

FRT is error prone and has resulted in numerous false arrests across the U.S., with a disproportionate effect on African Americans.[48] FRT's legitimacy has been called into question by statistics revealing alarming variances in accuracy based on gender and ethnicity.[49] In 2018, a research study uncovered the influence of bias on FRT

42. *See id.* at 8 ("Bledsoe's dream of an all-seeing 'computer friend' was already mired in the realities of 1960s US society and politics.").

43. *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROCS. MACHINE LEARNING RSCH. 1, 7–8 (2018), https://www.media.mit.edu/publications/gender-shades-intersectional-accuracy-disparities-in-commercial-gender-classification/ (revealing that two government-released benchmarks for judging progress of facial analysis, IJB-A and Adience, had datasets composed of 79.6% and 86.2% lighter-skinned subjects respectively).

44. SCHWARTZ ET AL., *supra* note 26, at 6.

45. *Id.* at 32.

46. *See* MARSHALL, *supra* note 27, at 12–14 (discussing how, during the Civil Rights Era, wiretapping and photo surveillance were used to restrict organizational movements and weaponize Black leaders under the guise of countering national security threats).

47. *See* Neil Selwyn et al., *Facial Recognition Technology: Key Issues and Emerging Concerns*, *in* THE CAMBRIDGE HANDBOOK OF FACIAL RECOGNITION IN THE MODERN STATE 11, 20 (Rita Matulionyte & Monika Zalnieriute eds., 2024) (noting that system inaccuracies have been linked to emotional distress, denial of social welfare benefits, and jeopardized job prospects).

48. NAT'L ACADS., *supra* note 9 (highlighting numerous FRT-related false arrests).

49. *See* Buolamwini & Gebru, *supra* note 43, at 3.

algorithms.[50] It identified a 34.7 percent error rate for darker-pigmented females and an error rate of 0.7 percent for lighter-pigmented males.[51] The widespread use of FRT necessitates improvement for better interpretation across intersections of identity.[52]

FRT image sources also speak to FRT's discriminatory nature. Many LEAs run images through mugshot and driver's license databases or use systems that search social media sites and the public internet.[53] Using mugshot databases as a repository perpetuates discrimination because minorities are often overrepresented.[54] African Americans are frequent victims of the criminal justice system and make up a substantial percentage of the nation's incarcerated population.[55] Mugshot

---

50. *Id.* at 7–11. This study (1,270 subjects) gauged the intersectional accuracy of FRT systems developed by leading technology companies: IBM, Face++, and Microsoft.

51. *Id.* at 9–11.

52. *See* Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. LAW (Oct. 18, 2016), https://www.perpetuallineup.org/ ("One in two American adults is in a law enforcement face recognition network."). FRT was suggested to "affect[] over 117 million American adults." Given FRT's growing prevalence, this number is likely to continue increasing. *Id.*

53. Paige Gross, *Facial Recognition in Policing is Getting State-By-State Guardrails*, STATELINE (Feb. 4, 2025, at 14:20 CT), https://stateline.org/2025/02/04/facial-recognition-in-policing-is-getting-state-by-state-guardrails/.

54. LENA GERAGHTY, FACIAL RECOGNITION REPORT 13 (2021), https://www.nlc.org/wp-content/uploads/2021/04/NLC-Facial-Recognition-Report.pdf; *see San Diego Association of Governments*, THE PERPETUAL LINE-UP (Sep. 2016), https://www.perpetuallineup.org/jurisdiction/san-diego-association-governments (indicating that San Diego, CA uses a database of over 1.4 million mugshots, and African Americans are "arrested at a rate 202% higher than their population share"). Using a mugshot database presupposes everyone in mugshot databases has committed a crime, and those who have, will again. *But see* Christopher Jones, *Law Enforcement Use of Facial Recognition: Bias, Disparate Impacts on People of Color, and the Need for Federal Legislation*, 22 N.C. J.L. & TECH. 777, 810 (2021) (noting that some people in the database could have been wrongfully accused or later had their charges dropped). Because FRT does not consider these factors, one wrong FRT match can have irreversible effects on an individual.

55. *Racial and Ethnic Disparities,* PRISON POL'Y INITIATIVE, https://www.prisonpolicy.org/research/race_and_ethnicity/ (noting that while only thirteen percent of the U.S. population is Black, Black inmates account for thirty-seven percent of the

databases personify statistical and systemic bias because they are underinclusive and give rise to an increased likelihood that African Americans will continue to be subjected to FRT searches, false positives, and wrongful arrests.[56]

Conversely, the use of social media and driver's license photos is overinclusive, subjecting more people to the criminal justice system where they otherwise might not have been.[57] Driver's license photos include more people without concentrating on subsections of the population, like mugshot databases, but leave every registered driver susceptible to FRT searches.[58] Also, image quality influences accuracy, and FRT algorithms perform at a lower error rate when higher-quality images are used.[59] Social media repositories can be problematic if

---

nation's incarcerated population). In the year 2020 alone, 1.99 million Black Americans were arrested. *Id.*

56. *See* Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, 34 CRIM. JUST. 9, 13 (2019) (noting how extensive use of FRT during Black Lives Matter ("BLM") protests raised fears due to overrepresentation of Black individuals in FRT repositories). Also, research shows that FRT is heavily concentrated in minority communities. NAT'L ACADS. *supra* note 9, at 82 (discussing how marginalized communities may be surveilled at higher rates than others, leading those communities to be "designated as high-crime areas" and creating a "feedback loop that can further justify use of FRT or other technologies that disproportionately affect marginalized communities").

57. *See* Selwyn et al., *supra* note 47; Gross, *supra* note 53.

58. GERAGHTY, *supra* note 54, at 33; Garvie, Bedoya & Frankle, *supra* note 52 (reporting that Nebraska's FRT repository includes around eight million driver's license photos).

59. *See* PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, FACE RECOGNITION VENDOR TEST (FRVT) PART 2: IDENTIFICATION 2 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf (reporting that FRT algorithms that were fed good-quality images of 12 million individuals indicated error rates of around 0.1%). These error rates differ drastically from those in footnote 40 because this study involved photos taken with ideal conditions, formalized photography, and cooperative subjects. With most one-to-many comparisons, these conditions do not apply, so accuracy sharply declines. NAT'L ACADS., *supra* note 9, at 1 (noting that "FRT accuracy is affected by image quality," and using images where "subjects may not even realize that their image is being captured, such as images taken from security cameras, generally result in lower-quality images"). Nevertheless, security footage remains one of the main sources that LEAs use when commencing investigations. *Id.* at 66.

filters and makeup obscure the face.[60] Most people are not aware that social media images may be used, yet when registering for accounts, they agree to their biometric data being used for various purposes.[61] An algorithm is only as good as the data it has been fed.[62] Therefore, inclusive datasets, quality images, and limited interference from bias help FRT perform more effectively.[63]

FRT can help LEAs achieve public safety.[64] For example, FRT can aid investigations when uncooperative individuals refuse to identify themselves.[65] One study indicated that machines surpass humans

60. Clare Garvie, *Garbage In, Garbage Out*, GEO. LAW (May 16, 2019), https://www.flawedfacedata.com/ (noting that LEAs may use low-quality, filtered images from social media and even composite sketches to conduct FRT searches). Maryland, Montana, and Washington take measures to ensure good-quality images are used; these states prohibit using manually-produced sketches with FRT. *See* MD. CODE ANN., CRIM. PROC. § 2-503(a)(1)(iii) (West 2025); MONT. CODE ANN. § 44-15-106(7) (West 2025); WASH. REV. CODE ANN. § 43.386.080(6) (West 2025).

61. *Compare* Patel v. Facebook, Inc., 932 F.3d 1264, 1267 (9th Cir. 2019) ("When a new user registers for a Facebook account, the user must . . . agree to Facebook's terms and conditions, which permit Facebook to collect and use data in accordance with [its] policies."), *with* Carpenter v. United States, 585 U.S. 296, 309–10 (2018) (offering *some* Fourth Amendment protection even when an individual's information is held by third parties). Georgia protects biometric data derived from the internet; it restricts using the internet to obtain personal identifying information, including biometrics, in a false representation context. *See* GA. CODE ANN. § 16-9-109.1 (West 2025).

62. *See* United States v. Esquivel-Rios, 725 F.3d 1231, 1234 (10th Cir. 2013) ("Garbage in, garbage out. Everyone knows that much about computers: you give them bad data, they give you bad results.").

63. NAT'L LEAGUE OF CITIES, FACIAL RECOGNITION GUIDE FOR CITIES, https://www.nlc.org/wp-content/uploads/2021/04/FacialRecognitionSummary_NLC.pdf [hereinafter NLC] ("The effectiveness of [FRT] is dependent on a good quality image of an unknown individual, an algorithm that has been trained on a wide variety of human faces and a strong definition of what the software should consider as a match between the unknown face and the database.").

64. GERAGHTY, *supra* note 54, at 11 (recognizing an ability to maintain effective investigations with fewer resources could be helpful to agencies struggling with reduced revenue, resources, and funding). *But see* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (suggesting that limited police resources serve as a check on police by constraining abusive techniques).

65. AUTOMATED REG'L JUST. INFO. SYS., TACIDS: TACTICAL IDENTIFICATION SYSTEM USING FACIAL RECOGNITION 6, https://voiceofsandiego.org/wp-content/uploads/2021/04/TACIDS-Final-Report-FINAL.pdf (acknowledging FRT's utility

when analyzing high-quality still images.[66] Nevertheless, humans are deemed "the most accurate face recognition systems" because we "recognize faces as part of social interactions . . . and under a wide variety of poses, expressions, and illuminations."[67] AI was designed to replace the human decision-making process but has not yet achieved that objective.[68] That deficiency undermines the immediacy to eliminate human involvement.[69]

Eyewitness testimony is a primary method for suspect identification.[70] However, eyewitness identification has been challenged as untrustworthy because of human bias and memory limitations.[71] Own-

when dealing with uncooperative, violent individuals who waste resources by providing false or unverifiable information); JOE PURSHOUSE & ANDREW ROBERTS, *Introduction: Criminal Justice, Technology, and the Future of Privacy*, *in* PRIVACY, TECHNOLOGY, AND THE CRIMINAL PROCESS 11 (Andrew Roberts, Joe Purshouse & Jason Bosland eds., 2024) (justifying the use of AI to achieve administrative objectives for criminal justice when systems operate with limited resources).

66. P. Jonathon Phillips & Alice J. O'Toole, *Comparison of Human and Computer Performance Across Face Recognition Experiments*, 32 IMAGE & VISION COMPUTING 74, 75 (2014).

67. *Id.* at 74. The study suggests that social interaction skills "allow[] the incorporation of motion and non-face identity cues into the recognition process." *Id.* at 78.

68. *See* J. E. Korteling et al., *Human- Versus Artificial Intelligence*, 4 FRONTIERS A.I. 1, 3 (2021), [https://doi.org/10.3389/frai.2021.622364] (highlighting AI limitations: inability to understand, make creative solutions, use context or intuition, or consider ethical implications). In other words, "machines don't have *common sense*." *Id.*

69. *See* Phillips & O'Toole, *supra* note 66, at 74 (suggesting that "accuracy equivalent to humans" is a difficult goal to ascertain and measure); *see also* Korteling et al., *supra* note 68, at 1–2 (establishing "the pursuit of human-like intelligence as the golden standard for [AI]" and analogizing the difference in cognitive ability between human intelligence and artificial intelligence to humans and animals).

70. *See* Brian L. Cutler & Gary L. Wells, *Expert Testimony Regarding Eyewitness Identification*, *in* PSYCHOLOGICAL SCIENCE IN THE COURTROOM: CONSENSUS AND CONTROVERSY 100, 100 (Jennifer L. Skeem, Kevin S. Douglas & Scott O. Lilienfeld eds., 2009).

71. *See, e.g.*, Noah Clements, *Flipping a Coin: A Solution for the Inherent Unreliability of Eyewitness Identification Testimony*, 40 IND. L. REV. 271, 271 (2007) (noting that the inherent unreliability of eyewitnesses makes mistaken eyewitness identification "the leading cause of wrongful convictions in the United States"); John C. Brigham, Adina W. Wasserman & Christian A. Meissner, *Disputed Eyewitness*

race bias—the idea that humans identify people of a different race than their own at a significantly lower rate of accuracy than other races—also presents constraints on human recognition.[72]

Machine recognition may eventually replace human informants, where "big data programs search through *all* available information for future or ongoing crimes."[73] This would ameliorate concerns about unreliable eyewitness testimony. Entrusting machines to do investigative work traditionally undertaken by humans raises additional privacy concerns, including an increased risk for technical glitches, criminal hacking, and data breaches.[74] Thus, human involvement can be a guardrail

---

Identification Evidence: Important Legal and Scientific Issues, 36 CT. REV., Summer 1999, at 12 ("[M]istaken identifications have been responsible for more miscarriages of justice than any other factor . . . ." (citation omitted)). Justice Frankfurter considered eyewitness identification "proverbially untrustworthy." United States v. Wade, 388 U.S. 218, 228 (1967).

72. *See* Cutler & Wells, *supra* note 70, at 102 ("[C]ross-race identifications were significantly less likely to be accurate than same-race identifications."); Bryan Scott Ryan, *Alleviating Own-Race Bias in Cross-Racial Identifications*, 8 WASH. U. JURIS. REV. 115, 115 (2015) ("Own-race bias in cross-racial identifications creates racial discrimination in the American judicial system, where a majority of defendants in criminal cases are minorities.").

73. Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 29 (2016) (emphasis added). However, humans lack the capacity of big data programs. Imagine how exhausting it would be to manually sift through large datasets to make identifications. *See* NAT'L ACADS., *supra* note 9, at 1 (observing that FRT "speeds up identification tasks that would otherwise need to be performed manually in a slower or more labor-intensive way and . . . makes identification tasks practical that would be entirely infeasible without the use of these tools"); Phillips & O'Toole, *supra* note 66, at 76 ("The main difference between measuring performance of humans and machines is the number of face pairs that can be compared."). Machines can compare millions of face pairs—an impossibility for humans, who can only rate a maximum of about 250. *Id.*; *see also* Korteling et al., *supra* note 68, at 5 (recognizing that humans have limited cognitive capacity in terms of attention span and memory while AI systems can operate and interpret data "with almost the speed of light"). *But see generally* SCHWARTZ ET AL., *supra* note 26 (exploring different categories of bias that cut against AI's effectiveness).

74. *Compare* Hafiz Sheikh Adnan Ahmed, *Facial Recognition Technology and Privacy Concerns*, ISACA (Dec. 21, 2022), https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-51/facial-recognition-technology-and-privacy-concerns ("Data breaches involving [FRT] data increase the potential for identity theft, stalking, and harassment because, unlike passwords and

in criminal investigations.[75] Humans are not perfect; neither are machines. The strengths and weaknesses of both humans and FRT suggest that neither should be used exclusively nor independently of the other in criminal investigations.[76] The struggle arises when attempting to fit the conflicting considerations within the existing Fourth Amendment framework.[77]

---

credit card information, faces cannot easily be changed."), *and* Edd Gent, *Hackers Compete to Confound Facial Recognition*, IEEE SPECTRUM (Aug. 29, 2022), https://spectrum.ieee.org/facial-recognition (suggesting that the main reason these systems are susceptible to attack is because they were "never built with security in mind," and security is treated as "an afterthought"), *with* Sarah Cwiek, *Detroit Police Commissioners Approve Facial Recognition Policy*, MICH. PUB. (Sep. 19, 2019, at 22:07 ET), https://www.michiganpublic.org/politics-government/2019-09-19/detroit-police-commissioners-approve-facial-recognition-policy (recounting the Detroit, Michigan police chief's statement that only negative aspects of FRT are accentuated: "[w]e never talk about the violent, predatory suspects who shoot and kill people. . . . We use the technology constitutionally, effectively, and it aids us in identifying that violent suspect."), *and* FACEPTION, *supra* note 33 (explaining that "[w]e live in a dangerous world," the vast majority of terrorists and criminals are unknown, and current methods of identifying criminals—including manual profiling—are insufficient to handle growing threats).

75. *See* SCHWARTZ ET AL., *supra* note 26, at i.

76. *See* University of Huddersfield, *Man Versus Machine: Who Wins When it Comes to Facial Recognition?*, NEUROSCIENCE NEWS (Dec. 3, 2018), https://neurosciencenews.com/man-machine-facial-recognition-120191/ (suggesting that accuracy levels drastically increase where AI and human intelligence are combined). *But see* NIJ, *supra* note 23 ("[FRT] is a tool that, if used properly, can greatly enhance law enforcement capabilities and improve public safety, but if used carelessly and improperly, may negatively impact privacy and civil liberties."). Also, polygraphs undercut this argument. *See* Lyudmila A. Spektor et al., *The Inadmissibility of the Use of the Polygraph in Criminal Proceedings*, 7 INT'L J. INNOVATION, CREATIVITY AND CHANGE 162, 169 (2019) (questioning the validity of polygraph tests as a science because the results depend on the examiner's qualifications and intuitive decisions).

77. *See* Terry v. Ohio, 392 U.S. 1, 9 (1968) ("'No right is held more sacred, or is more carefully guarded . . . than the right of every individual to the possession and control of his own person, free from all restraint or interference of others . . . .'" (quoting Union Pac. Ry. Co. v. Botsford, 141 U.S. 250, 251 (1891)). To justify an intrusion, "the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion." *Id.* at 21.

III. FRT AND THE FOURTH AMENDMENT

The U.S. Constitution is integral when determining how FRT should be regulated. FRT is an increasingly pervasive surveillance technology;[78] its widespread use implicates various constitutional rights. The Fourth Amendment is specifically implicated because it protects against unreasonable searches and seizures, assuring that warrants will only be issued if there is probable cause.[79] The Supreme Court has not yet evaluated the constitutionality of FRT but has held that the use of similar technologies constitutes an "unreasonable search," requiring a warrant supported by probable cause.

A. The Probable Cause Standard Applied to FRT

Government searches and seizures conducted without a warrant supported by probable cause are presumptively unconstitutional.[80] The Fourth Amendment protects an individual's personal security, and probable cause protects against baseless charges of crime.[81] The standard is a "fluid concept that is based on the totality of the circumstances."[82] A probable cause determination is based upon whether there is sufficient evidence that a criminal offense was committed and that the arrestee was the perpetrator.[83]

The Court has indicated a willingness to thwart the adoption of pervasive technologies to safeguard individual rights. In *Katz v. United States*, the Court articulated a test to determine when the government has disrupted an individual's reasonable expectation of privacy ("REP"): (1) whether an individual has exhibited an actual, subjective expectation of privacy; and (2) whether society deems the subjective expectation reasonable.[84] When both elements are met, a "search" has occurred.[85] Following that reasoning, some argue that "law

78. ANDREJEVIC & SELWYN, *supra* note 41, at ix.
79. U.S. CONST. amend. IV.
80. *See* Katz v. United States, 389 U.S. 347, 357 (1967).
81. Maryland v. Pringle, 540 U.S. 366, 370 (2003).
82. Moorer v. City of Chicago, 92 F.4th 715, 720 (7th Cir. 2024).
83. *See* Murray v. United States, 351 F.2d 330, 333 (10th Cir. 1965).
84. 389 U.S. at 361 (Harlan, J., concurring).
85. *Id.*

enforcement's observations of anything put on public display are not 'searches' at all" because there is no REP in a face—the most outward-facing aspect of our identity that is continuously exposed to the public.[86]

Traditionally, a person's face would likely not be considered protected by the Fourth Amendment.[87] The Court has stated, "[n]o person can . . . reasonably expect that his face will be a mystery to the world."[88] Yet, the Court has also made clear that "the Fourth Amendment protects *people*, not places."[89] While "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection[,] . . . what he seeks to preserve as private, even in an area accessible to the public, *may* be constitutionally protected."[90] Therefore, an individual's face is not disqualified from protection merely because of public exposure.[91] The Court's reasoning in *Katz* supports this argument.[92]

Whether an REP exists is also influenced by the specific use and the kind of information provided by FRT.[93] FRT reveals more

86. John Zens, Comment, *Face IT: Only Congress Can Preserve Privacy from the Pervasive Use of Facial Recognition Technology by Police*, 58 S.D. L. REV. 143, 184 (2021); *see also* Hamann & Smith, *supra* note 56 (stating there is no "automatic" REP for faces because they are exposed to the public).

87. The traditional approach defined "search" in terms of trespass or physical intrusions of a tangible object. Olmstead v. United States, 277 U.S. 438 (1928). In *Katz*, the Court ruled that a search was not limited to trespass and occurs whenever the government infringes upon a person's REP. 389 U.S. at 348.

88. United States v. Dionisio, 410 U.S. 1, 14 (1973).

89. *Katz*, 389 U.S. at 351 (1967) (emphasis added).

90. *Id.* (emphasis added).

91. *Cf.* Carpenter v. United States, 585 U.S. 296, 310 (2018) ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere.").

92. In *Katz*, the government placed an eavesdropping device on a *public* telephone booth to obtain evidence of illegal gambling. 389 U.S. at 348. The Court held that eavesdropping constituted a "search and seizure" because although Katz was in public, the device impinged upon the REP in the details of his conversation. *Id.* at 353.

93. *See* Lee Rainie et al., *Public More Likely to See Facial Recognition Use by Police as Good, Rather than Bad for Society*, PEW RSCH. CTR. (Mar. 17, 2022), https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/ (noting that about half of Americans favor its use in retail stores and apartment buildings but a majority oppose its use on social media platforms).

information than what is readily visible to the human eye.[94] People may consider it acceptable to be recorded for safety purposes but still expect to preserve privacy regarding the intricacies of their identity. Additionally, individuals may reasonably believe they should be protected from automatic identification upon entering a public space, and it is unreasonable to expect them to hide their faces to avoid such identification.[95]

In *Carpenter v. United States*, the Court required a warrant to access an individual's cell-site location information ("CSLI") records.[96] The Court emphasized the "unique" nature of CSLI records, which log extensive details of past movements, and described a cell phone as a "feature of human anatomy" that travels everywhere with its owner.[97] It also recognized a "legitimate expectation of privacy in the record of [Carpenter's] physical movements as captured through CSLI."[98] A person's face (also a feature of human anatomy) travels with them everywhere. FRT, like CSLI records, can reveal far more about a person than what the individual is willing to share with others.[99]

---

94. *See* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1110–11, 1119–20, 1122–25 (2021) (describing the extensive amounts of information available within a matter of seconds using FRT: facial characteristics such as the nose, eyes, and mouth; locational metadata revealing travel history and behavioral attributes or patterns; criminal history; and biographical data such as name, date of birth, race, employment history, and health issues); *see also* FACEPTION, *supra* note 33 (revealing that its FRT system can deduce details on personality type, ranging from extrovert, IQ level, and professional poker player, based on facial image alone). This level of detail is arguably unnecessary and irrelevant to criminal justice.

95. *See generally* Mailyn Fidler & Justin Hurwitz, *An Overview of Facial Recognition Technology Regulation in the United* States, *in* THE CAMBRIDGE HANDBOOK OF FACIAL RECOGNITION IN THE MODERN STATE 214, 215 (Rita Matulionyte & Monika Zalnieriute eds., 2024) (recognizing FRT makes it difficult for people to move anonymously in public: "[w]here before the advent of FRT there was 'anonymity in crowds,' today there is none.").

96. Prior to *Carpenter*, CSLI records were accessible via court order after demonstrating "'reasonable grounds' for believing that the records were 'relevant and material to an ongoing investigation'"—a far less stringent standard than that required for a warrant. 585 U.S. at 317 (quoting 18 U.S.C. § 2703(d)).

97. *Id.* at 311 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

98. *Id.* at 310.

99. NAT'L ACADS., *supra* note 9, at 25 (noting that unregulated use of FRT "allows repressive regimes to create detailed records of people's movements and

Further, an individual's identity is not readily accessible unless one knows them.[100]

In *United States v. Jones*, the government placed a GPS tracker on an individual's Jeep and obtained more than 2,000 pages of data.[101] The Court concluded that the GPS tracking constituted a "search."[102] The Court's fear that pervasive technologies are susceptible to abuse is more than idle speculation.[103] Today, it is easy to monitor and track individuals. "With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense" and increasingly creep into the "privacies of life" without invitation.[104]

---

activities, including political protests or organizing, and to block targeted individuals from participation in public life").

100. *Compare Carpenter*, 585 U.S. at 310 (holding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI"), *and* Olmstead v. United States, 277 U.S. 438, 478 (1928) (recognizing the right to be let alone, even as against the government, as the "most comprehensive of rights and the right most valued by civilized men"), *with* Sabrina A. Lochner, Note, *Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans*, 55 ARIZ. L. REV. 201, 211 (2013) (noting that people do not have a right to remain completely anonymous to police), *and* ARIZ. REV. STAT. ANN. § 13-2412(a) (2025) ("It is unlawful for a person, after being advised that the person's refusal to answer is unlawful, to fail or refuse to state the person's full name on request of a peace officer who has lawfully detained the person based on reasonable suspicion that the person has committed, is committing or is about to commit a crime.").

101. 565 U.S. 400, 402–03 (2012). Justice Alito questioned whether the use of a GPS tracker involved a level of "intrusion that a reasonable person would not have anticipated." *Id.* at 430 (Alito, J., concurring). *See also* Srivats Shankar, *Fourth Amendment Constraints on Automated Surveillance Technology in the Public to Safeguard the Right of an Individual to Be "Secure in their Person"*, 18 J. BUS. & TECH. L. 209, 226 (2023) (noting that the Court has often used "the amount of information collected" by different technologies to determine whether an individual's privacy interests have been infringed). The Court has closely scrutinized intrusive technologies, and FRT has a propensity to "provide encyclopedic levels of information about a particular individual" in a matter of seconds. *Id.* at 226–27.

102. *Jones*, 565 U.S. at 404–06.

103. *See id.* at 416–17 (Sotomayor, J., concurring) (referring to GPS monitoring as "a tool so amenable to misuse").

104. *Carpenter*, 585 U.S. at 311. *Compare Jones*, 565 U.S. at 429–30 (Alito, J., concurring) (noting how traditional surveillance tactics were difficult, time-consuming, and costly), *with* Kashmir Hill, *The Secretive Company That Might End Privacy*

These decisions exemplify the Court's hesitation to trust LEAs with indiscriminate authority over pervasive technology.[105] The Court is likely to scrutinize FRT as it has other similar technologies. If it does, it will likely conclude that using FRT constitutes a Fourth Amendment search requiring a warrant supported by probable cause because FRT can reveal vast amounts of personal information, individuals have an REP in that information, and avoiding public spaces to evade FRT is impractical. The following fingerprinting analysis provides additional insight into how FRT should be scrutinized as a biometric technology.

B. Judicial Scrutiny of Other Biometric Tech

Fingerprinting, like FRT, is a biometric technology that analyzes physical characteristics for automated recognition.[106] Fingerprinting has been recognized as "one of the most long-established biometrics modalities"[107] and revered as the "'gold standard' of human identification" because fingerprint curvatures are unique.[108] Litigants challenge its reliability—mainly debating whether "uniqueness" should be distinguished from accuracy and procedural validity.[109]

---

as We Know It, N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (noting how FRT's ability to "identify a suspect in a matter of seconds" makes identification quick, easy, and amenable to abuse).

105. *See Carpenter*, 585 U.S. at 312 ("Only the few without cell phones could escape this tireless and absolute surveillance."). Or, under *Jones*, those without vehicles. Consider how a person lacks the ability to evade such intrusiveness with FRT. All those with a face who venture out into public or have social media are susceptible to FRT detection.

106. *Biometrics*, U.S. DEPT. OF HOMELAND SEC. (Aug. 28, 2025), https://www.dhs.gov/biometrics; Sidney Perkowitz, *The Bias in the Machine: Facial Recognition Technology and Racial Disparities*, MIT CASE STUDIES IN SOCIAL AND ETHICAL RESPONSIBILITIES OF COMPUTING 1, 8–9 (2021).

107. U.S. DEP'T OF HOMELAND SEC., U.S. DEP'T OF JUST. & WHITE HOUSE OFFICE OF SCI. AND TECH. POL'Y, BIOMETRIC TECHNOLOGY REPORT 18 (2024) [hereinafter DHS REPORT].

108. Zabell, *supra* note 37, at 143.

109. *See* Simon A. Cole, *Grandfathering Evidence: Fingerprint Admissibility Rulings from* Jennings *to* Llera Plaza *and Back Again*, 41 AM. CRIM. L. REV. 1189, 1197–98, 1202 (2004) (dismissing the idea that uniqueness should be the basis of establishing accuracy—similar to how uniqueness of a human face cannot establish the

Nevertheless, courts still consider it admissible because of the established character and courts' longstanding acceptance of fingerprint reliability.[110]

The fingerprint identification process is similar to FRT: it "match[es] two fingerprints, one found in the crime scene and the other from a fingerprint register."[111] Latent prints—those taken from crime scenes—are often smudged or distorted, while the inked prints they are compared to are often taken under controlled conditions at booking stations.[112] Latent prints lack the detail, complexity, and particularity of ridge patterns, making them an "inevitable source of error in making comparisons."[113] Distinctions in quality necessarily lead to imperfect matches—a problem present when poor-quality images are used to conduct FRT searches.[114] Similar to FRT, fingerprinting involves human bias, requiring examiners to make subjective decisions to resolve inconsistencies.[115] Subjectivity cuts against accuracy because

---

"accuracy of eyewitness identification"); *see also* NAT'L RSCH. COUNCIL OF THE NAT'L ACADS., STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD 107–08 (2009), https://www.ojp.gov/pdffiles1/nij/grants/228091.pdf ("Much forensic evidence . . . is introduced in criminal trials without any meaningful scientific validation, determination of error rates, or reliability testing to explain the limits of the discipline.").

110. *See* JENNIFER A. BROBST, ADMISSIBILITY OF EVIDENCE IN NORTH CAROLINA § 12:40 (4th ed. 2025) (noting that this rationale has consistently been upheld by N.C. courts since 1951); State v. Graham, 882 S.E.2d 719, 730 (N.C. Ct. App. 2023) (holding that a fingerprint expert need not testify about error rates or scientific acceptance of the process); State v. Watlington, 759 S.E.2d 392, 394–95 (N.C. Ct. App. 2014) (concluding that evidence of the unreliability of fingerprinting evidence is not enough to challenge admissibility).

111. Virpi Mustonen et al., *Discrepancies in Expert Decision-Making in Forensic Fingerprint Examination*, 254 FORENSIC SCI. INT'L. 215, 215 (2015).

112. Zabell, *supra* note 37, at 144.

113. *Id.* (citation omitted); *see also id.* at 150 ("Latent prints of any type, digitized or not, almost always involve elements of distortion and a loss of information . . . .").

114. GROTHER, NGAN & HANAOKA, *supra* note 59, at 9 (discussing how image quality affects FRT performance).

115. *See supra* Part II (examining the effects human bias can have when FRT is used for criminal justice).

examiners make judgment calls on how best to fill gaps.[116] Accordingly, criminal processes that incorporate "large subjective component[s]" are rightfully subject to close scrutiny.[117] *Mayfield v. United States* is demonstrative of this point.[118]

Mayfield arose from the 2004 Madrid train-bombing incident.[119] The Spanish National Police ("SNP") recovered fingerprints from a bag of detonators near the explosion site and contacted the FBI to inquire whether the fingerprint produced a match in the FBI's database.[120] The FBI database produced twenty candidates, one of whom was Brandon Mayfield.[121] While the FBI declared a "100% positive identification" between Mayfield's prints and the latent from the scene, SNP disagreed and later matched the latent print to another person.[122]

Even long-established identification methods are susceptible to mistake.[123] The more differences there are between latent fingerprints

116. Zabell, *supra* note 37, at 178 (suggesting that the subjectivity of fingerprinting automatically rules out certainty); Spektor et al., *supra* note 76 (suggesting that the scientific validity of polygraphs is reasonably questioned because it is an art that depends on the qualifications, experience, and intuition of the examiner).

117. Zabell, *supra* note 37, at 178. Fingerprinting may be replaced by more credible forensic technologies because it contributes to a substantial amount of erroneous death penalty cases. DNA identification is preferred by LEAs and is based in science. *Id.* at 143–44, 169. The use of DNA evidence is a leading form of criminal justice reform. ROBERTS, *supra* note 27, at 284. However, even DNA identification is imperfect and can have devastating effects. *Id.* at 270, 274 ("DNA is *not* infallible. The genetic material in government databanks has to be retrieved, transferred, transported, identified, labeled, analyzed, and stored by human hands, and there is opportunity for error at every stage."). No criminal identification method—whether fingerprinting, DNA, eyewitness testimony, or FRT—will be without flaw; imperfection is inevitable.

118. 599 F.3d 964, 967 (9th Cir. 2010).

119. *Id.* at 966.

120. *Id.*

121. *Id.*

122. *Id.* at 967. An FBI official, later interviewed about what went wrong, stated: "[t]he determination by [the] examiner that the print was useable was hasty and erroneous," which "set the agency off in the wrong direction and corrupted the rest of the process." Zabell, *supra* note 37, at 149–50 (citation omitted). This reinforces the "garbage in, garbage out" phenomenon discussed in note 60.

123. Perkowitz, *supra* note 106, at 8.

and their purported match, the less probable the match.[124] The human mind sees what it wants, and "this ability flourishes in the absence of stringent safeguards."[125] *Mayfield* indicates that increased scrutiny can lead to reformation.[126] As with other technologies used for criminal justice, the stakes are high: a misidentification could be the "crucial evidence on the basis of which someone is sent to prison for a lifetime."[127] These limitations should inform FRT regulation.[128] Fingerprinting, albeit imperfect, exemplifies how FRT can be a resourceful tool if wielded correctly.

IV. STATE AND FEDERAL STATUTORY RESTRICTIONS ON FRT

Existing statutory limits on FRT lay the foundation for assessing how best to regulate FRT. The application of FRT to criminal justice unveils the inherent tension between public safety and the right to be free from unreasonable government interference. Statutes that afford greater flexibility to LEAs impose stricter limitations on individual liberties.[129] In contrast, statutes that maximize individual liberties place

---

124. Zabell, *supra* note 37, at 151. This relates to FRT because the more differences there are between a probe image and the database image, the less probable the match.

125. *Id.* at 151, 178.

126. Perkowitz, *supra* note 106, at 9 (suggesting *Mayfield* led to greater scrutiny being placed upon fingerprinting evidence).

127. Mustonen et al., *supra* note 111.

128. *See* SIMON A. COLE, SUSPECT IDENTITIES: A HISTORY OF FINGERPRINTING AND CRIMINAL IDENTIFICATION, 186, 194 (2001) (stating "[f]ingerprint evidence won acceptance without being subjected to the kind of organized skepticism and careful scrutiny that is supposed to be inflicted upon scientific and legal facts" and the absence of "rules for defining the boundary between certainty and conjecture nor an institutional mechanism for policing examiners" can invalidate the fingerprinting process, the examiners, and their conclusions). This should be avoided with FRT, which has the potential to be more reliable. *See also* Spektor et al., *supra* note 76, at 166 (discussing how polygraphs are inadmissible because they do not meet evidentiary requirements of reliability and violate the Constitution by invading a person's personal secrets).

129. *See e.g.*, ALA. CODE § 15-10-111 (2025) (addressing solely when LEAs may use FRT match results in establishing probable cause for arrests); N.H. REV. STAT. ANN. § 105-D:2 (2025) (prohibiting only the use of FRT to edit, alter, erase, delete, duplicate, copy, or otherwise subject body camera recordings to FRT). Before

greater restraint on LEAs' ability to use FRT to enhance public safety.[130] Some localities also stand at the far end of the spectrum by enforcing outright bans on FRT use, but those efforts are likely to be reconsidered or preempted by state law.[131] Thus, existing statutes serve as blueprints for Congress and states that have not yet regulated FRT's use in criminal investigations.

A. State Regulation of FRT

State and local jurisdictions impose various limitations on how LEAs can use FRT. Some are devoted to individual privacy.[132] Others govern the general use of AI by commercial entities.[133] Few, however, regulate FRT when used in criminal investigations. In 2015, Oregon

---

its statute expired, California also restricted the use of FRT only with regard to body cameras. *See infra* note 137 and accompanying text; Federal Police Camera and Accountability Act, H.R. 843, 118th Cong. (2023–2024), https://www.congress.gov/bill/118th-congress/house-bill/843/text (prohibiting the use of FRT in police body cameras and dashboard cameras—a federal bill introduced but not yet enacted).

130. *See e.g.*, Use of Facial Recognition Technology by Law Enforcement in Cases Involving Sexual Exploitation of Children, 2021 Vt. Laws No. 17 (West) (to be codified at VT. STAT. ANN. tit. 13, ch. 64) (prohibiting FRT in *all* contexts except in sexual exploitation of children cases); *see also* H.B. 195, Gen. Assemb. Reg. Sess. (Vt. 2021–2022), https://legislature.vermont.gov/Documents/2022/Docs/ACTS/ACT017/ACT017%20As%20Enacted.pdf.

131. *See* Oakland, Cal., Ordinance 13,563 (Sep. 17, 2019) https://oakland.legistar.com/View.ashx?M=F&ID=7743127&GUID=74F54F43-770A-4C7C-BE0B-B9CE7F351D36 [hereinafter Oakland Ordinance] ("[I]t shall be unlawful for the City or any City staff to obtain, retain, request, access, or use: (1) [FRT]; or (2) Information obtained from [FRT]."); City of Somerville, Mass., Ordinance 208,142 (Jun. 27, 2019), https://somervillecityma.iqm2.com/Citizens/Detail_LegiFile.aspx?ID=20991 (mirroring Oakland's statutory language). *But see* NAT'L ACADS., *supra* note 9, at 27 (revealing how some municipalities have reconsidered their bans after evaluating crime rates).

132. *See, e.g.*, 740 ILL. COMP. STAT. ANN. 14/1–14/99 (West 2025) (establishing Illinois' Biometric Information Privacy Act—the first jurisdiction to extensively regulate the acquisition, use, and distribution of biometric data).

133. For a comprehensive outline of generally-enacted legislation across the U.S. surrounding AI, see *Artificial Intelligence 2023 Legislation*, NAT'L CONF. OF STATE LEGISLATURES (Jan. 12, 2024), https://www.ncsl.org/technology-and-communication/artificial-intelligence-2023-legislation.

banned the use of body cameras equipped with FRT.[134] At the time, Oregon was the only state restricting FRT, but its scope was limited to body cameras.[135] Jurisdictions were motivated to restrict FRT use following the 2020 social protests.[136] By 2022, New Hampshire, Vermont, Maine, and California followed Oregon's lead.[137] FRT remains unregulated in a great number of states, allowing LEAs to use FRT in their investigations without restriction.[138]

---

134. OR. REV. STAT. ANN. § 133.741 (West 2025) (imposing a "prohibition on the use of facial recognition or other biometric matching technology to analyze recordings obtained through the use of the camera"). By establishing statewide procedures for body cameras, Oregon sought to build a credible, trustworthy criminal justice system. Press Release, Or. State Legislature, Bills Aim to Bolster Trust in the Criminal Justice System (May 5, 2015), https://www.oregonlegislature.gov/housedemocrats/Documents/CriminalJusticeTransparencyPressRelease.pdf.

135. Joh, *supra* note 73, at 15 (highlighting FRT's ability to make real-time identifications if combined with body cameras: "the feed is sent in real time back to the department where facial recognition and movement analysis software alerts the patrol officer as to whether furtive movements or people on watch lists have been identified. Police follow up on these alerts to identify people who should be immediately investigated. Other people are dismissed as not posing an immediate threat but are logged on watch lists for future reference.").

136. Anushka Jain, *Facial Recognition Laws in the United States #Project-Panoptic*, INTERNET FREEDOM FOUND. (May 3, 2021), https://internetfreedom.in/facial-recognition-laws-in-the-united-states-projectpanoptic/ (noting that George Floyd's death and the BLM movement increased police surveillance of protestors, thwarting First Amendment rights). In 2020, nearly twelve localities passed ordinances to restrict FRT. For an interactive map detailing where FRT has been banned, see BAN FACIAL RECOGNITION, https://www.banfacialrecognition.com/map/?ref=static.internetfreedom.in (last visited Oct. 15, 2025).

137. New Hampshire enacted similar body camera restrictions. N.H. REV. STAT. ANN. § 105-D:2 (2025). Vermont's statute was different in scope and substance. *See infra* note 162 and accompanying text. Maine prohibited the use, retention, and possession of FRT and information derived from it. ME. REV. STAT. ANN. tit. 25, § 6001 (2025). California's statute, which banned the use of FRT in combination with body cameras, was enacted as a three-year moratorium that expired in January of 2023. *See* Assemb. B. 1215, ch. 579 (Cal. 2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215. California no longer regulates FRT, but many of its localities have stepped in. *See, e.g.*, Oakland Ordinance, *supra* note 131.

138. *See* Garvie, Bedoya & Frankle, *supra* note 52 (suggesting that one in every four LEAs use FRT). This is inconsistent with the Framers' vision that the Fourth Amendment curb "arbitrary exercises of police power." United States v. Jones, 565

To date, thirteen states govern the use of FRT by LEAs: Alabama, Colorado, Kentucky, Maine, Maryland, Massachusetts, Montana, New Hampshire, Oregon, Utah, Vermont, Virginia, and Washington.[139] Current legislation in these states draws broadly on three requirements: probable cause, serious or violent crime limits, and meaningful human review.

1. Probable Cause Requirement

State legislatures adopt different methods to situate FRT into the existing probable cause standard. Alabama, Colorado, Kentucky, Maine, Maryland, Massachusetts, Montana, Oregon, Virginia, and Washington have each articulated that FRT results cannot be the sole basis for establishing probable cause.[140] Instead, FRT results may only

---

U.S. 400, 416 (2012) (Sotomayor, J., concurring). To track LEAs' use of various surveillance technology, including FRT, see *Atlas of Surveillance: Documenting Police Tech in our Communities with Open Source Research*, ELEC. FRONTIER FOUND., https://www.atlasofsurveillance.org/search (last visited Dec. 12, 2025).

139. ALA. CODE § 15-10-111 (2025); COLO. REV. STAT. ANN. § 24-18-307 (West 2025); KY. REV. STAT. ANN. § 61.9305 (West 2025); ME. REV. STAT. ANN. tit. 25, § 6001 (2025); MD. CODE ANN., CRIM. PROC. §§ 2-502 to -503 (West 2025); MASS. GEN. LAWS ANN. ch. 6, § 220 (West 2021), *amended by* H.B. 4359, 193rd Gen. Ct. (Mass. 2023–2024); MONT. CODE ANN. §§ 44-15-105 to -106 (West 2025); N.H. REV. STAT. ANN. § 105-D:2 (2025); OR. REV. STAT. ANN. § 133.741 (West 2025); UTAH CODE ANN. § 77-23e-103 (West 2025); Use of Facial Recognition Technology by Law Enforcement in Cases Involving Sexual Exploitation of Children, 2021 Vt. Laws No. 17 (West) (to be codified at VT. STAT. ANN. tit. 13, ch. 64); VA. CODE ANN. §§ 15.2-1723.1 to 1723.2 (West 2025); WASH. REV. CODE ANN. § 43.386.080 (West 2025).

140. *See, e.g.*, ALA. CODE § 15-10-111 (2025) ("(a) A state or local [LEA] may not use [FRT] match results as the sole basis to establish probable cause in a criminal investigation or to make an arrest. (b) To establish probable cause in a criminal investigation or to make an arrest, a state or local [LEA] may use [FRT] match results only in conjunction with other lawfully obtained information and evidence."). The language of other statutes is largely consistent with Alabama's language. COLO. REV. STAT. ANN. § 24-18-307(1)(c) (West 2025); KY. REV. STAT. ANN. § 61.9305(3)(a)(1) (West 2025); ME. REV. STAT. ANN. tit. 25, § 6001(2)(E) (2025); MD. CODE ANN., CRIM. PROC. § 2-502(b) (West 2025); H.B. 4359, 193rd Gen. Ct. (Mass. 2023–2024); MONT. CODE ANN. § 44-15-106(2)(a) (West 2025); OR. REV. STAT. ANN. § 133.741(1)(b) (West 2025); VA. CODE ANN. § 15.2-1723.2(C) (West 2025); WASH. REV. CODE ANN. § 43.386.080(5) (West 2025).

be used in conjunction with other lawfully obtained evidence.[141] The purpose of this requirement is to ground the use of FRT in existing criminal procedure standards that establish privacy rights and civil liberties.[142] Requiring LEAs to supplement FRT results with other evidence reduces the risk of error by showing that it is more probable than not that an arrestee is the one who committed the crime. Determining the point at which LEAs need probable cause can have a significant impact on the investigatory tactics LEAs choose to employ and on the suspected individual whose rights are implicated.[143] Essentially, the question is at what point can LEAs rely solely on FRT results?

FRT is often used before an arrest when identifying a suspect. Kentucky prohibits LEAs from relying solely on FRT results when making an arrest.[144] Kentucky's focus on the arrest aspect of the

141. This requirement aligns with the Fourth Amendment requirement that police "have probable cause or a warrant before making an arrest." Herring v. United States, 555 U.S. 135, 136 (2009).

142. *See, e.g.*, ALA. ADMIN. CODE r. 265-X-5-.01 (2025); S.B. 56, 2022 Leg., Reg. Sess. (Ala. 2022) (indicating the legislative purpose behind the probable cause requirement is to ensure AI is not the sole basis for arrests). *See also* Maryland v. Pringle, 540 U.S. 366, 370 (2003) (stating that the probable cause standard "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'" (citation omitted)); WASH. REV. CODE ANN. § 43.386.900(1) (West 2025) ("Unconstrained use of [FRT] by state and local government agencies poses broad social ramifications that should be considered and addressed. Accordingly, legislation is required to establish safeguards that will allow state and local government agencies to use [FRT] in a manner that benefits society while prohibiting uses that threaten our democratic freedoms and put our civil liberties at risk.").

143. Localities are demonstrative of this point. *See, e.g.*, N.Y. STATE DIV. OF CRIM. JUST. SERVS., FACIAL RECOGNITION MODEL POLICY (2019), https://www.criminaljustice.ny.gov/crimnet/ojsa/standards/MPTC%20Model%20Policy-Facial%20Recognition%20December%202019.pdf (allowing FRT results to be used as a *lead* in an investigation, but not as the sole basis for probable cause to make *arrests*); Garvie, Bedoya & Frankle, *supra* note 52 (requiring only a reasonable suspicion to run FRT searches in San Diego, California); *Nebraska*, THE PERPETUAL LINE-UP, https://www.perpetuallineup.org/jurisdiction/nebraska (last visited Dec. 18, 2025) (imposing no evidentiary requirement to conduct FRT searches). Lincoln, Nebraska's approach is most favorable to LEAs; no standard restricts the way in which FRT is used. However, that assures no safeguards for individual rights.

144. *See* KY. REV. STAT. ANN. § 61.9305(3)(a)(2) (West 2025).

investigation addresses the risk that an arrestee is not the actual suspect.[145] Under that framework, LEAs are expected to provide more to support the assertion that *this* person committed *this* crime. Nevertheless, a criminal investigation extends beyond an arrest. Washington, Montana, and Maryland provide that FRT cannot be the sole basis "in a criminal investigation" without targeting a specific point in the investigation.[146] Moreover, it leaves open the possibility of using FRT for more than simply identifying suspects.[147]

States should provide clearer restrictions on how FRT results can be used. Alabama addresses this ambiguity by prohibiting FRT results from serving as the sole basis for establishing probable cause in criminal investigations or making an arrest.[148] This language is equivalent to stating, "at any time during the criminal investigation, including making arrests." Virginia provides: "[a] match made through [FRT] shall not be included in an affidavit to establish probable cause for purposes of issuance of a search warrant or an arrest warrant but shall be admissible as exculpatory evidence."[149] This approach strongly protects criminal defendants by admitting the evidence only to absolve defendants, not to establish their guilt. This is unduly restrictive on LEAs' ability to ferret out crime and impedes the prosecution's evidentiary case.

Four states require warrants in this context: Washington, Colorado, Montana, and Utah.[150] Washington and Colorado provide that LEAs cannot use FRT for surveillance or identification purposes

145. Maine's statute might yield a similar analysis. It states that "[FRT] data does not, without other evidence, establish probable cause justifying arrest, search or seizure." ME. REV. STAT. ANN. tit. 25, § 6001(2)(E) (2025).

146. WASH. REV. CODE ANN. § 43.386.080(5) (West 2025); MONT. CODE ANN. § 44-15-106(2)(a) (West 2025); MD. CODE ANN., CRIM. PROC. § 2-503(a)(1) (West 2025).

147. *See, e.g.*, MONT. CODE ANN. § 44-15-106(2)(a) (West 2025) (allowing FRT searches to identify individuals believed to be either perpetrators, victims, or witnesses of serious crimes); VA. CODE ANN. §§ 15.2-1723.2(A)(ii)–(iii) (West 2025) (authorizing FRT use to help identify crime victims or witness).

148. ALA. CODE § 15-10-111(a) (2025).

149. VA. CODE ANN. § 15.2-1723.2(C) (West 2025).

150. WASH. REV. CODE ANN. § 43.386.080(1)(a) (West 2025); COLO. REV. STAT. ANN. § 24-18-307(1)(a) (West 2025); MONT. CODE ANN. § 44-15-106(3) (West 2025); UTAH CODE ANN. § 77-23d-106 (West 2025).

without a warrant authorizing use.[151] Montana prohibits LEAs from obtaining, retaining, possessing, accessing, or using FRT to investigate serious crime without a warrant.[152] Lastly, Utah recently updated its provision, requiring a warrant to operate imaging surveillance devices and obtain biometric surveillance information.[153]

The difference between an FRT warrant requirement and a rule prohibiting FRT as the sole basis for probable cause is that the "sole basis" approach still allows LEAs to rely heavily on FRT results.[154] The warrant requirement forces LEAs to articulate their need for such use without relying on a "match" produced by FRT. Colorado further requires judges who issue or deny warrants to report the following to state court administrators: the fact that a warrant was applied for, whether it was approved or denied, the scope of authorized surveillance, and the identity of the officer or agency who made the request.[155] In short, the probable cause requirement is a barrier against unsupported assertions

151. WASH. REV. CODE ANN. § 43.386.080(1)(a) (West 2025); COLO. REV. STAT. ANN. § 24-18-307(1)(a) (West 2025). However, LEAs can use § 24-18-307(1)(b) to surpass the warrant requirement or judicial authorization if deemed "necessary to develop leads in an investigation."

152. MONT. CODE ANN. § 44-15-106(2)(a), (3) (West 2025).

153. The provisions on biometric surveillance information and facial recognition comparisons are inconsistent. "Biometric surveillance information" is defined as "the analysis of surveillance information using biometric software to identify an individual's identity or location using the individual's physical attributes or manner." UTAH CODE ANN. § 77-23d-102(3) (West 2025). "Facial recognition comparison" is defined as "the process of comparing an image or facial biometric data to an image database" and "'[f]acial recognition comparison' does not include biometric surveillance information." *Id.* § 77-23e-102(3). Both processes involve analyzing biometric data for identification but yield different procedural requirements. *Compare* UTAH CODE ANN. § 77-23d-106(1) (West 2025) (requiring a *warrant* to obtain the biometric surveillance information) *with* UTAH CODE ANN. § 77-23e-103(2)(b)(iii) (West 2025) (requiring a statement of the specific crime and a factual narrative supporting a *fair probability* that the individual is connected to the crime).

154. Jake Laperruque, *Status of State Laws on Facial Recognition Surveillance: Continued Progress and Smart Innovations*, TECH POL'Y PRESS (Jan. 6, 2025), https://www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations/ ("Under a sole basis rule, [an FRT] match could serve as the primary, even overwhelming basis for an arrest."). This does not effectively address issues of overreliance and subsequent wrongful arrests.

155. COLO. REV. STAT. ANN. § 24-18-308(2) (West 2025).

that a particular individual is a perpetrator and, at a minimum, requires corroborating evidence.

2. Serious or Violent Crime Limit

Limiting the scope of authorized FRT use can minimize its discriminatory effects while also enhancing public safety.[156] This is based on the idea that FRT can be very invasive and should only be used in a narrow set of scenarios.[157] In 2021, nearly seventy million Americans had a criminal record. Only twenty million reflected felony convictions; the rest were misdemeanors, arrests that did not lead to conviction, or dismissed charges.[158] Permitting use of FRT related to misdemeanors or minor offenses is most problematic for racial discrimination because Black men are eight times more likely to be imprisoned than White men.[159]

---

156. *See generally* NLC, *supra* note 63 (advocating for limiting the scope of FRT use to violent crimes to reduce misidentification rate).

157. *See* Jake Laperruque, *Limiting Face Recognition Surveillance: Progress and Paths Forward*, CTR. FOR DEMOCRACY & TECH. (Aug. 23, 2022), https://cdt.org/insights/limiting-face-recognition-surveillance-progress-and-paths-forward/ (suggesting it is more reasonable for FRT to be used for serious crimes like homicide versus nonviolent offenses or misdemeanors).

158. Jones, *supra* note 54 ("'Even the briefest minor interaction with the justice system can leave someone with a criminal record' and consequently, included in police records for life." (quoting Tina Rosenburg, *Have You Ever Been Arrested? Check Here*, N.Y. TIMES (May 24, 2016), https://www.nytimes.com/2016/05/24/opinion/have-you-ever-been-arrested-check-here.html)).

159. *See* Alexandra Natapoff, *Misdemeanors*, 85 S. CAL. L. REV. 1313, 1313 (2012) ("Misdemeanor convictions are typically dismissed as low-level events that do not deserve the attention or due process accorded to felonies. And yet, ten million petty cases are filed every year . . . ."); ROBERTS, *supra* note 27, at 277 (noting that the imprisonment rate gap between Black and White individuals continues to increase); Kade Crockford, *How is Face Recognition Surveillance Technology Racist?*, ACLU (June 16, 2020), www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist (noting that despite similar rates of cannabis use between Black and White people, Black people are four times more likely to be arrested for minor crimes like cannabis possession). Thus, investigating minor crimes with FRT disproportionately affects Black individuals. *See also* ROBERTS, *supra* note 27, at 279, 283 (discussing how police make drug arrests in a racially discriminatory manner, and Black people are "disproportionately stopped for traffic infractions, arrested for drug offenses, swept off the streets for 'gang loitering,' and sent to prison").

Most states limit FRT use to serious or violent crimes.[160] Maryland's statute has great breadth because, while it limits use to certain offenses, its exception includes twelve crimes ranging from weapon crimes to hate crimes.[161] There are advantages and disadvantages to having such an overbroad statute. It is clear to defendants that their rights will only be limited if charged with an enumerated offense. LEAs, however, may not want permitted uses confined to an enumerated list. Vermont, for example, only allows use of FRT to investigate the sexual exploitation of children where LEAs believe an individual is either a victim or an unidentified suspect.[162] Vermont specifies that its provision only applies in the context of a particular offense and purpose; it does not permit use beyond that.

Maine, Massachusetts, Utah, Maryland, Virginia, Montana, Washington, and Colorado each permit using FRT to identify deceased or incapacitated individuals.[163] These situations are clearer to ascertain:

Even if wrongfully convicted, minorities have fewer resources to challenge police misconduct, and the wrongful arrest has far-reaching effects, including lifelong police surveillance. *Id.* at 280, 283.

160. *See, e.g.*, ME. REV. STAT. ANN. tit. 25, § 6001(1)(I) (2025) (defining "serious crime" as crimes punishable for at least a year, crimes involving a dangerous weapon, or Class D and Class E crimes); MONT. CODE ANN. § 44-15-103(17) (West 2025) (defining "serious crime" as a variety of offenses including negligent homicide, vehicular homicide while under the influence, aggravated assault, assaulting a peace officer or judicial officer, assaulting a minor, stalking, kidnapping, aggravated kidnapping, robbery, sexual intercourse without consent, endangering welfare of children, sexual abuse of children, sex trafficking, labor trafficking, and patronizing victim of sex trafficking); UTAH CODE ANN. § 77-23e-103(c)(i) (West 2025) (allowing the use of FRT to investigate a felony, violent crime, or threat to human life).

161. MD. CODE ANN., CRIM. PROC. § 2-503(a)(1)(i) (West 2025) (authorizing LEAs to use FRT to investigate crimes of violence, human trafficking, first and second-degree child abuse, child pornography, hate crimes, weapon crimes, aggravated cruelty, importation of fentanyl, and criminal acts presenting a substantial threat to public safety and national security).

162. Use of Facial Recognition Technology by Law Enforcement in Cases Involving Sexual Exploitation of Children, 2021 Vt. Laws No. 17 (West) (to be codified at VT. STAT. ANN. tit. 13, ch. 64).

163. *See* ME. REV. STAT. ANN. tit. 25, § 6001(2)(B)(2) (2025); H.B. 4359, 193rd Gen. Ct. (Mass. 2023–2024) (permitting the use of FRT to "identify a deceased person"); UTAH CODE ANN. § 77-23e-103(2)(c)(ii) (West 2025) (permitting the use of FRT to identify "an individual who is . . . deceased . . . [or] incapacitated"); MD. CODE ANN., CRIM. PROC. § 2-507 (West 2025) (authorizing the use of FRT "for the purpose

either a person is or is not deceased or incapacitated. Furthermore, it is less likely that LEAs would encounter uncooperative subjects in either circumstance. That determination is more problematic if FRT is used for emergencies, imminent threats, substantial risks to public safety, or exigencies.[164] If the jurisdiction fails to clarify, it leaves room for officers to make subjective decisions about what constitutes those circumstances.

Determining what should fall within the scope of authorized use gets at the heart of the tension between individual rights and public safety.[165] In states where FRT is unregulated, FRT could be used by

---

of . . . identifying a missing or deceased person or a person who is incapacitated and unable to otherwise provide the person's own identity"); VA. CODE ANN. § 15.2-1723.2(A) (West 2025) (authorizing the use of FRT to "identify a deceased person" and "help identify a person who is incapacitated"); MONT. CODE ANN. § 44-15-106(2)(c) (West 2025) (authorizing the use of FRT to assist in identifying "a person who is deceased"); WASH. REV. CODE ANN. § 43.386.080(1)(c) (West 2025) (authorizing the use of FRT to identify a deceased person); COLO. REV. STAT. ANN. § 24-18-307(1)(d) (West 2025) (authorizing the use of FRT to locate or identify a deceased person).

164. Massachusetts allows use where a reasonable belief of "emergency involving immediate danger of death or serious physical injury to an individual or group," requires FRT use without delay. H.B. 4359 § 220(d)(3), 193rd Gen. Ct. (Mass. 2023–2024). Utah has a similar provision for threats to human life. *See* UTAH CODE ANN. § 77-23e-103(2)(c)(i) (West 2025) (authorizing the use of FRT for the purpose of "investigating a felony, a violent crime, or a threat to human life"). Washington requires a warrant for FRT use except where "[e]xigent circumstances exist" but provides no further guidance as to what constitutes those circumstances. WASH. REV. CODE ANN. § 43.386.080(1)(b) (West 2025). *See also* MD. CODE ANN., CRIM. PROC. § 2-503(a)(1)(i)(11) (West 2025) (allowing use if the "criminal act involv[es] circumstances presenting a substantial and ongoing threat to public safety or national security"). In Montana, "[an LEA] may perform a search . . . prior to the issuance of a warrant if there is an emergency posing imminent threat to a person." MONT. CODE ANN. § 44-15-106(5)(a) (West 2025). However, the LEA must obtain the warrant within twenty-four hours following the search. *Id.*

165. *See* PURSHOUSE & ROBERTS, *supra* note 65, at 12 (questioning whether we should rely on AI when answering constitutional questions: "AI systems intended for the administration of justice should, because of their 'potentially significant impact on democracy, rule of law, individual freedoms, as well as the right to effective remedy' be considered 'high risk'" because of the risk of bias, opacity, and error). The book acknowledges, however, that those concerns also arise with human decision-making and subjective bias.

LEAs to do more than identify criminals.[166] FRT is already used in aimless ways; and, in many contexts, people are not even aware. Even where notice is provided, the specified use is often exceeded.[167] Research indicates that the more common and less threatening the activity, the more likely that FRT use in that context is to be frowned upon.[168] FRT is especially frowned upon where it infringes upon the exercise of constitutionally protected activities.[169] Thus, a serious or violent crime limit, if narrowly tailored enough, mitigates concerns about FRT being abused.[170] If permitted in the context of *all* crimes or

166. *See generally* Rainie et al., *supra* note 93 (reporting that FRT is used to monitor crowds at sports venues, concerts, protests, and to scan people as they walk down the street).

167. NAT'L ACADS., *supra* note 9, at 25 (noting how public housing residents are subjected to widespread FRT use that was intended to address "public safety concerns"); Douglas MacMillan, *Eyes on the Poor: Cameras, Facial Recognition Watch over Public Housing*, WASH. POST (May 16, 2023, at 06:03 ET), https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/ (revealing that Ohio officials said they were surveilling apartment complexes to crack down on a gang war but were instead using FRT cameras to record activities like "removing a cart from a communal laundry room" or "spitting in a hallway"). Most Americans are unaware about how LEAs are using FRT. Some provisions aim to keep the public involved, cutting against FRT's cryptic, unfamiliar nature. *See, e.g.*, COLO. REV. STAT. ANN. § 24-18-302 (West 2025) (requiring public accountability reports with: FRT system and vendor, system capabilities and limitations, type of data inputs used, what the system is being used for, how the decision of whether to use FRT will be reached, and how, when, and by whom the system will be used).

168. *See* Rainie et al., *supra* note 93 (indicating that 68% of Americans do not think it is acceptable to use FRT as people walk down the street; but only 36% think use is unacceptable to monitor concert crowds, and 38% think use is unacceptable at protests); Laperruque, *supra* note 157 (noting China's more pervasive application to investigate minor offenses and Baltimore's use of FRT as a punitive measure for protesting).

169. *See, e.g.*, KY. REV. STAT. ANN. § 61.9305(3)(a)(2) (West 2025) (prohibiting use "to identify a person participating in constitutionally protected activities in public spaces unless there is probable cause to believe that an offense has been committed"); MD. CODE ANN., CRIM. PROC. § 2-503(a)(1)(ii)(1) (West 2025) (imposing a similar provision but only requiring that there be a "reasonable suspicion" of crime).

170. *See supra* Section II (discussing how all sources of images for FRT databases are problematic), but comparative images have to come from somewhere. *See also* Garvie, Bedoya & Frankle, *supra* note 52 ("One in two American adults is in a law enforcement face recognition network."). Limiting use to certain circumstances softens that blow.

even *minor* crimes, FRT would be used more frequently, putting more people at risk. Furthermore, where an offense requires little investigative work, it can be argued that traditional methods should be used instead of FRT.[171]

3. Meaningful Human Review

Meaningful human review explores the fundamental constraints of humans and machines. FRT is a relatively novel technology with an alarming error rate; its output should not be automatically trusted.[172] Existing statutes use meaningful human review to double-check FRT results and catch obvious discrepancies.[173]

Kentucky's statute requires initial findings to be confirmed by a secondary examiner, but it does not define that process or establish who can qualify as a secondary examiner.[174] Colorado only requires meaningful human review where FRT is used to make decisions that could generate legal effects on an individual.[175] Colorado further defines "meaningful human review" as another trained individual or someone with the authority to change the decision being reviewed.[176] Maryland simply requires "independent[] verifi[cation]" by trained individuals and limits that requirement to FRT used for criminal investigations.[177] Montana, interestingly, requires "meaningful human review prior to making . . . adverse final decision[s]," but fails to provide clarity on

171. *But see* Paresh Dave, *Focus: U.S. Cities Are Backing Off Banning Facial Recognition as Crime Rises*, REUTERS (Mar. 12, 2022, at 12:35 CT), https://www.reuters.com/world/us/us-cities-are-backing-off-banning-facial-recognition-crime-rises-2022-05-12/ (acknowledging FRT as a possible way to curtail and mitigate crime rates, so FRT should not be limited only to specific criminal offenses).

172. *See* COLE, *supra* note 128, at 194 (revealing other biometric technologies, like fingerprinting, that have been trusted without a determination of the process' reliability and accuracy).

173. *See supra* Part I (discussing Robert Williams and Michael Oliver). In both situations, the photographed subjects only vaguely resembled the arrestees. *Id.* With meaningful human review, minimal similarities cast doubt on the "match" produced by FRT. *Id.*

174. KY. REV. STAT. ANN. § 61.9305(3)(d) (West 2025).

175. COLO. REV. STAT. ANN. § 24-18-303 (West 2025).

176. *Id.* § 24-18-301(9).

177. MD. CODE ANN., CRIM. PROC. § 2-503(a)(3) (West 2025).

that phrase.[178] Whenever FRT is used to identify an individual, that determination should be thoroughly reviewed. Furthermore, it can be difficult to anticipate whether a decision will be adverse to an individual. Criminal investigations and trials cannot be predicted and often involve uncertainty.

Utah provides that where an FRT system indicates a "possible match," an independent visual comparison is required to ensure that the "possible match" is actually a "probable match."[179] Utah also requires a supervisor or another trained employee to agree that the match is probable.[180] If there is disagreement about a probable match, then the results are not reported.[181] This approach appears objective, but the language could be misconstrued. Is the second employee making their determination independently, or are they merely verifying the results from the first employee? What if secondary decisions are influenced by the prior decisions?

Requiring meaningful human review ensures that an individual is not unnecessarily deprived of individual rights. Judicial oversight is also baked into each statute that has a warrant requirement because a neutral, detached magistrate authorizes the warrant and ameliorates concerns that a fellow officer might be influenced by their mutual stake in the case.

If evidence is obtained in violation of FRT restrictions, the Fourth Amendment allows exclusion of that evidence where certain circumstances are met.[182] Maine similarly provides a suppression mechanism where any data collected or obtained as a violation is unlawfully obtained, must be deleted upon discovery, and is inadmissible in any proceeding.[183] The incentive for LEAs to violate FRT restrictions is removed if the unlawfully obtained information has little

178. MONT. CODE ANN. § 44-15-106(9) (West 2025).

179. UTAH CODE ANN. § 77-23e-103(4)(b) (West 2025).

180. *Id.* § 77-23e-103(4)(c).

181. *Id.* § 77-23e-103(4)(d)(ii).

182. *See* United States v. Leon, 468 U.S. 897, 910 (1984) (explaining that the exclusionary rule suppresses evidence obtained by Fourth Amendment violations and police misconduct).

183. ME. REV. STAT. ANN. tit. 25, § 6001(3)(A)(2) (2025); MONT. CODE ANN. § 44-15-107(3)(b) (West 2025).

to no practical use. This Note suggests a warrant requirement that combines existing restrictions.

B. Proposed Federal Regulation of FRT

While states and localities have been proactive in FRT regulation, Congress has not regulated the use of FRT in federal investigations.[184] Congress, however, has proposed some relevant legislation.[185] Congress' consideration indicates a general consensus that FRT should be regulated to some degree.

The Facial Recognition and Biometric Technology Moratorium Act of 2020 ("the Moratorium") is an attempt at reconciling competing interests. Though proposed multiple times since 2020, the Moratorium has stalled in legislation.[186] It prohibits the government from using,

184. To date, nearly twenty-eight localities have ordinances that restrict FRT use. *See* DHS REPORT, *supra* note 107, at 114; *see also* NLC, *supra* note 63 (noting that "[f]ederal or state legislation may eventually preempt or nullify local legislation," but in the meantime, "cities are taking the lead in shaping [FRT] policy," often with the most thorough regulation occurring at the local level). *See generally* Fidler & Hurwitz, *supra* note 95, at 224 (noting that state and local jurisdictions have an advantage because their governments "can regulate [FRT] in ways and at speeds that the federal government cannot" and experiment as "laboratories of democracy").

185. For examples, see the Facial Recognition and Biometric Technology Moratorium Act of 2023, S. 681, 118th Cong. (2023–2024), https://www.congress.gov/bill/118th-congress/senate-bill/681 (indicating one of its primary purposes as "prohibit[ing] biometric surveillance by the Federal Government without explicit statutory authorization"); the George Floyd Justice in Policing Act of 2021, H.R. 1280, 117th Cong. (2021–2022), https://www.congress.gov/bill/117th-congress/house-bill/1280 (passed House) (prohibiting body cameras from being equipped with FRT); and the Advancing Facial Recognition Technology Act, H.R. 4039, 117th Cong. (2021–2022), https://www.govinfo.gov/content/pkg/BILLS-117hr4039ih/pdf/BILLS-117hr4039ih.pdf (requiring the Secretary of Commerce and the Federal Trade Commission to conduct studies on risks and trends in the marketplace of FRT and to report back to Congress with recommendations for continued development). This Note focuses primarily on the Moratorium Act.

186. Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084, 116th Cong. (2019–2020), https://www.congress.gov/bill/116th-congress/senate-bill/4084/text?ref=static.internetfreedom.in; Facial Recognition and Biometric Technology Moratorium Act of 2021, S. 2052, 117th Cong. (2021–2022), https://www.congress.gov/bill/117th-congress/senate-bill/2052; Facial Recognition

possessing, acquiring, or accessing biometric surveillance unless authorized by statute and provides a remedy for those injured by violations.[187] It incentivizes the adoption of the Moratorium or substantially similar legislation through financial means. Once enacted, state and local governments will be ineligible to receive federal funding under the Edward Byrne Memorial Justice Assistance Grant program ("Byrne program") if noncompliant.[188] The Byrne program provides substantial financial assistance to states and localities, targeted toward enhancing major criminal justice initiatives.[189]

The Moratorium would be a temporary means of addressing FRT imperfections.[190] A moratorium, by nature, is temporary and merely postpones an issue for later.[191] To address high-stakes issues, like disproportionate, wrongful arrests stemming from FRT, permanent congressional action is warranted.[192] Much has occurred politically, socially, and technologically, such that Congress should reconsider the elements of the Act.[193] States and localities have spearheaded FRT regulation up to this point, but enacting an FRT warrant requirement

---

and Biometric Technology Moratorium Act of 2023, S. 681, 118th Cong. (2023–2024), https://www.congress.gov/bill/118th-congress/senate-bill/681/text.

187. Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084, 116th Cong. (2019–2020), https://www.congress.gov/bill/116th-congress/senate-bill/4084/text?ref=static.internetfreedom.in.

188. For more information on the Byrne program, see *Edward Byrne Memorial Justice Assistance Grant (JAG) Program*, U.S. DEP'T OF JUST.: BUREAU OF JUST. ASSISTANCE (July 23, 2025), https://bja.ojp.gov/program/jag/overview.

189. *Id.*

190. Laperruque, *supra* note 157 (noting that the "Moratorium Act . . . would halt government use of [FRT] until Congress can enact a comprehensive set of rules to mitigate the threats to human rights").

191. *See Moratorium*, BLACK'S LAW DICTIONARY (12th ed. 2024) ("An authorized postponement, usu[ally] a lengthy one, in the deadline for paying a debt or performing an obligation.").

192. Also, the Moratorium has been stalled in legislation for the past few congressional sessions. If we relied on a moratorium to achieve the kind of reformation needed with FRT, we would be back to square one once it expires.

193. The Moratorium was originally drafted before the majority of states began regulating.

would provide stringent protection for individual liberties and acknowledge LEAs' responsibilities.[194]

V. FRT WARRANTS: BALANCING PUBLIC SAFETY AND INDIVIDUAL LIBERTIES

How should FRT be regulated?[195] Complete abolition shuts the door on FRT use without any regard to its beneficial uses.[196] Permitting LEAs to use FRT only if a warrant authorized that use protects individuals from wrongful arrests, disparity, and unwarranted surveillance without sacrificing the government's public safety duty.[197] That warrant requirement should specifically cover the authorization, execution, and post-execution process.

A. Authorization to Execute FRT Investigations

The authorization process carries a lot of significance. FRT results should not be the sole basis for establishing probable cause to

194. Mapp v. Ohio, 367 U.S. 643, 660 (1961) (noting that, in the context of the Fourth Amendment, the Court's decisions should be "founded on reason and truth, give[] to the individual no more than that which the Constitution guarantees him, to the police officer no less than that to which honest law enforcement is entitled, and, to the court, that judicial integrity so necessary in the true administration of justice"). *Mapp* recognizes the inherent tension between an individual's interest, the government's interest, and the judiciary's interest but nevertheless suggests that the Fourth Amendment should recognize and preserve each.

195. *See* COLE, *supra* note 128 (discussing the invalidation of fingerprint evidence absent careful discernment between certainty and conjecture). This should be avoided with FRT.

196. *See* Anne McNamara, *"Colorblind" Policing: Facial Recognition Technology's Interplay in the Fourth Amendment's Race Problem*, 56 SUFFOLK U. L. REV. 731, 759 (2023) (advocating for a complete abolition of FRT to prevent inequitable, racist policing and to protect individual liberties); *see also* Crockford, *supra* note 159 ("Banning face surveillance won't stop systemic racism, but it will take one powerful tool away from institutions that are responsible for upholding it."). *But see* Stokes, *supra* note 11 (recounting how FRT enabled one family to solve the murder of their loved one by tracing his movement); *Biometrics*, *supra* note 17 (describing FRT's ability to identify known terrorists).

197. U.S. COMM'N ON C.R., THE CIVIL RIGHTS IMPLICATIONS OF THE FEDERAL USE OF FACIAL RECOGNITION TECHNOLOGY 1–7 (2024), https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf.

make arrests or to conduct searches. Other states should look to Washington, Colorado, Montana, and Utah to implement warrant requirements for FRT use in criminal investigations.[198] This would spur them to enact legislation that requires a reviewing judge to determine whether LEAs have met the probable cause standard, ensuring that when FRT searches and seizures do occur, they are based on sufficient reasoning and justification. Judges issuing FRT warrants should be required to keep a record of each application stating whether it was granted or denied, the reasons, the scope of authorized use, and the identity of the requesting officer and the officer authorized to use the system. Furthermore, warrants should only be issued if the systems utilized by LEAs meet minimum accuracy standards across races to mitigate racial disparity.[199]

States should also defer to the approach adopted by Maryland and Utah, which would limit FRT searches to investigating serious or violent crime as defined by the jurisdiction's statute.[200] FRT should not be used to investigate petty crimes or constitutionally protected activities.[201] LEAs should be allowed to use FRT outside of investigating serious or violent crime only if authorized by Congress, the U.S. Supreme Court, a state legislature, or a state supreme court. Furthermore, there should be exceptions allowing use to identify deceased and

198. WASH. REV. CODE ANN. § 43.386.080(1)(a) (West 2025); COLO. REV. STAT. ANN. § 24-18-308(2) (West 2025); MONT. CODE ANN. § 44-15-106(3) (West 2025); UTAH CODE ANN. § 77-23d-106(1)(a) (West 2025).

199. *See generally* NLC, *supra* note 63 (suggesting that there be a high probability threshold for matches before systems can be used).

200. MD. CODE ANN., CRIM. PROC. § 2-503(a)(1)(i)(1) (West 2025); UTAH CODE ANN. § 77-23e-103(2)(c)(i) (West 2025). The FBI, for example, defines "violent crime" as "murder and nonnegligent manslaughter, forcible rape, robbery, and aggravated assault"—crimes which involve force or the threat thereof. U.S. DEP'T OF JUST., UNIFORM CRIME REPORT: CRIME IN THE UNITED STATES, 2010, at 1 (2011), https://ucr.fbi.gov/crime-in-the-u.s/2010/crime-in-the-u.s.-2010/violent-crime/violentcrimemain.pdf.

201. Such use deprives an individual of an ability to freely exercise their rights, discourages individuals from engaging in protected activities, and risks profiling on the basis of a protected class. *See* U.S. COMM'N ON C.R., *supra* note 197, at 51, 89 (highlighting that using FRT when individuals are engaged in protected activities can "result[] in negative outcomes that have a disparate impact on protected classes").

incapacitated individuals.[202] These recommendations still give LEAs considerable leeway to combat crime and enhance public safety while also preventing the indiscriminate use of FRT.

B. Execution of FRT Warrants

Following authorization, FRT can be used for facial comparisons. States should look to Utah's independent visual comparison provision to guide their reviewing process.[203] Under this scheme, only trained officers who were authorized via warrant should be involved in conducting the comparison. At this stage, FRT results must be treated as possible matches. A trained officer should conduct their own independent assessment to confirm that possibility. Then, a second trained officer should review the possible match. Only if both trained officers reach the same conclusion should the results be treated as a probable match. Moreover, human review should be conducted by a person of the same race as the suspect in question.[204]

These requirements recognize that there are benefits when AI and human intelligence are combined. The multiple layers of verification are consistent with the requirement that there be sufficient evidence that an arrestee is the perpetrator before being deprived of life or liberty. If the same result is reached at each verification point, meaningful review also reduces the risk of wrongful arrest.

---

202. Several states permit LEAs to use FRT in the context of identifying incapacitated or deceased individuals. *See, e.g.*, UTAH CODE ANN. § 77-23e-103(2)(c)(ii) (West 2025); MONT. CODE ANN. § 44-15-106(2)(c) (West 2025); ME. REV. STAT. ANN. tit. 25, § 6001(2)(B)(2) (2025); WASH. REV. CODE ANN. § 43.386.080(1)(c) (West 2025).

203. UTAH CODE ANN. § 77-23e-103(4)(b) (West 2025).

204. *See* Cutler & Wells, *supra* note 70, at 104 (discussing own-race bias). *See also* Ryan, *supra* note 72, at 119 ("Cross-racial identifications have been shown to be particularly unreliable due to 'own-race bias,'" which leads to wrongful convictions). Furthermore, "[a]s minorities are per capita more likely to be brought into the courtroom as criminal defendants, wrongful convictions based entirely or in part on faulty cross-racial identifications almost certainly disproportionately affect people of color." *Id.*

C. Post-Execution of FRT Warrants

States should look to the Federal Moratorium Act to establish procedures for enforcement mechanisms.[205] An arrestee must be immediately informed that FRT was used in connection with their arrest. Furthermore, any evidence obtained in violation of the warrant requirement cannot be used against an arrestee or defendant. States should be allowed to bring criminal actions against LEAs on behalf of their residents, or aggrieved individuals should be afforded a civil cause of action for their injuries. These are necessary enforcement mechanisms to disincentivize violating warrant requirements.

VI. CONCLUSION

What does the face of criminality look like? The disproportionate criminalization of Black individuals manifests itself in long-established policing tactics and is perpetuated through the use of pervasive, unregulated technology.[206] FRT provides a convenient alternative to traditional policing practices. At the same time, it can cause great harm if exploited or misused. Therefore, the widespread, warrantless use of FRT must be rectified. The relative ease of FRT computing massive amounts of information necessitates heightened scrutiny and a statutory FRT warrant requirement.

Evidence of bias and disparate impact makes FRT's application to criminal justice highly suspect as the increased risk of misidentification unreasonably exposes minorities to wrongful arrests.[207] Mass incarceration, use of mugshot databases, and concentrating FRT surveillance in minority communities also subject them to higher rates of false positives and arrests.[208] The stakes are high, leaving little room for an

---

205. Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084, 116th Cong. (2019–2020), https://www.congress.gov/bill/116th-congress/senate-bill/4084/text?ref=static.internetfreedom.in.

206. *See* MARSHALL, *supra* note 27 (discussing the history of discriminatory policing); *see also* Crockford, *supra* note 159 (describing the use of FRT as a mechanism that "exacerbates racism in a criminal legal system that already disproportionately polices and criminalizes Black people").

207. *See* Buolamwini & Gebru, *supra* note 43 and its accompanying text.

208. *See* Hamann & Smith, *supra* note 56, at 10–11 (describing how the utilization of FRT as a surveillance and identification tool perpetuates racial disparities); *see*

overreliance on flawed technology.[209] There is a higher risk of disparate impact where FRT use by LEAs is unregulated, especially with the global market for FRT forecasted to reach $12.67 billion by 2028.[210]

Despite such intolerable ramifications, FRT should remain accessible to LEAs. FRT is a resourceful way to enhance public safety.[211] And LEAs have a duty to protect communities and deter crime, so individual liberties cannot be absolute.[212] Nevertheless, public safety protects the individual right to be free from crime and violence.[213] LEAs should not be allowed to employ pervasive tools without oversight. Every state has a recognized "strong [] interest in the administration of its criminal laws."[214] Therefore, state legislatures should exercise their authority to regulate the use of FRT to prevent LEAs from using it in abusive ways. It is unlikely that the Court will rule definitively on the constitutionality of FRT by establishing a bright-line rule, and we need

---

also ROBERTS, *supra* note 27, at 277 ("'[M]ass incarceration is a mischaracterization of what is better termed *hyperincarceration*' because this excessive confinement is finely targeted (at 'one particular category, *lower-class African American men trapped in the crumbling ghetto*') rather than spread among the masses.").

209. Convictions are often accompanied by stigma, reputational damage, loss of liberty or life, and economic loss. *See generally* Brandon L. Garrett, *Innocence, Harmless Error, and Federal Wrongful Conviction Law*, 2005 WIS. L. REV. 35, 52 (2005) (suggesting that many wrongful convictions are undetected, and that the criminal justice system tolerates excessive error where life and death may be at stake).

210. *See* Ahmed, *supra* note 74.

211. *See* NAT'L ACADS., *supra* note 9, at 23 (discussing FRT's ability to sift through large amounts of data in seconds—a task impossible for humans); *see also* FACEPTION, *supra* note 33 (noting how FRT enables us to combat crime and prevent danger in a more efficient manner).

212. *Redefining the Role of Local Police and Public Safety*, U.S. CONF. OF MAYORS, https://www.usmayors.org/issues/police-reform/redefining-the-role-of-local-police-and-public-safety/ (last visited Dec. 14, 2025).

213. Lindsey McLendon, Rachael Eisenberg & Nick Wilson, *Improving Public Safety Through Better Accountability and Prevention*, CTR. FOR AM. PROGRESS (May 16, 2024), https://www.americanprogress.org/article/improving-public-safety-through-better-accountability-and-prevention/; *see* Cwiek, *supra* note 74 (describing how only negative aspects of FRT are emphasized); *see also* Emani Pollard, *Fourth Amendment Balancing and its Disparate Impact*, 47 N.Y.U. REV. L. SOC. CHANGE 124, 131–32 (2023) ("Public safety is at stake just as much when the police unreasonably search or seize as when crime happens in the neighborhood.").

214. Holmes v. Giarrusso, 319 F. Supp. 832, 834 (E.D. La. 1970).

clear mandates.[215] FRT's usefulness should not be an excuse for the lack of regulation, its high error rate, or its disproportionate effect on Black individuals. FRT warrants may not solve all FRT-related issues, but FRT warrants will hold LEAs accountable with authorization, execution, and post-execution requirements that increase the validity of subsequent searches and seizures. By enacting FRT warrant requirements, Congress and state legislatures can demonstrate their commitment to promoting the integrity of criminal investigations.

215. As technology evolved, Justice Alito cautioned that the Court is ill-suited to develop workable standards for modern technologies and suggested that state legislatures are better positioned to balance law enforcement interests against individual privacy rights. Riley v. California, 573 U.S. 373, 406–08 (2014) (Alito, J., concurring).