WITNESS-WASHING FACIAL RECOGNITION TECHNOLOGY

NATHAN E. ROUSE*

ABSTRACT

Law enforcement investigations are increasingly driven by hidden algorithmic tools, without disclosure of those tools to the people being prosecuted or the public at large. Facial Recognition Technology, for example, has been used by police to identify suspects in investigations since 2001. Despite the widespread and growing use of Facial Recognition Technology in police investigations, its scientific validity has never been tested in court, and its secret use has prevented it from being challenged on constitutional grounds.

This Article coins the term "witness-washing" to describe the mechanism by which this immense evasion has occurred. Witness-washing occurs when law enforcement uses algorithmic technology such as facial recognition, incorporates the results into a human decision-making process, and then hides their use of the algorithm by presenting the result as an exclusively human decision. For facial recognition, this means that a law enforcement officer runs an image from a surveillance video through an algorithm that is designed to find images of similar faces in a database of mug shots and driver's license photos. One of the images that the algorithm returns is then used as part of a traditional photo lineup procedure. But the State only discloses the results of the lineup, without mentioning the use of the algorithm. By using this technique, prosecutors have presented tens or hundreds of thousands of cases as if they originated in run-of-the-mill eyewitness identifications, while evading disclosure and examination of the use of speculative technology.

This Article uses Facial Recognition Technology as a case study to demonstrate law enforcements' increasing, hidden use of untested algorithmic tools. In doing so, it makes three central contributions. First, it offers a thorough descriptive account of witness-washing and the flawed technology that it has hidden. Second, it shows how witness-washing allows algorithmic tools to evade the traditional legal and practical limitations on investigative techniques—statutes, constitutional litigation, and limited resources—and how witness-washing distorts the assumptions that underly ongoing attempts to restrict these tools. Finally, this Article argues

* Acting Assistant Professor of Lawyering, New York University School of Law. For generous guidance on this project, I am grateful for Anna Arons, Daniel Harawa, Madeleine Gyory, Emma Kaufman, Christopher Lau, Stephen Schulhofer, and Maneka Sinha, as well as participants in NYU's Clinical Legal Writing Workshop and Lawyering Scholarship Colloquium. Cleo Nevakivi-Callanan, John Travis, Asha Ramachandran, and Lex Uttamsingh provided excellent research assistance. I also owe thanks to the excellent editors of the *Denver Law Review*.

that the lack of examination caused by witness-washing has allowed the carceral logic of modern law enforcement and the commercial logic of technology vendors to override the inherent logic of the tools themselves. Ultimately, this Article shows that the transition to a criminal legal system driven by algorithms will not be announced—it is happening already, under the cover of witness-washing.

TABLE OF CONTENTS

INTRODUCTION

> "Police action ends up in court. Policing technology gets litigated in court." –Andrew Guthrie Ferguson, *The Rise of Big Data Policing*[1]

> "Facial profiling technology is a new weapon in the investigative arsenal . . . . Reliability does not matter, however, because the

1. ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING 140 (2017).

> computerized identification is not ultimately evidence in court. It is simply a guide to put the investigator on the right track." –Geiger v. State[2]

A police department first deployed Facial Recognition Technology (FRT) as a tool for the identification of suspects in 2001.[3] In the twenty-four years since FRT's first formal deployment, appellate courts have examined it in only three decisions.[4] None of these decisions evaluated the underlying reliability of the technology. Police have used this technology regularly for almost a quarter of a century,[5] but FRT has fully evaded the processes by which courts purport to evaluate the use of new technologies in the criminal law.

There is no doubt that innocent people have been arrested due to police use of this untested investigative tool. In February 2023, an FRT algorithm identified an image of Porcha Woodruff as sharing some level of similarity to an image of a person in a surveillance video of a carjacking.[6] Detectives included Ms. Woodruff's image in a photo lineup, and a witness selected her.[7] Even a cursory investigation would have revealed that Ms. Woodruff was eight months pregnant, while the victim indicated the carjacker was not.[8] But the Detroit Police Department nevertheless arrested Ms. Woodruff in front of her children, based solely on the FRT-derived witness identification.[9] She spent eleven hours in jail and was prosecuted for a month before her case was dismissed.[10]

Ms. Woodruff experienced the most common law enforcement use of FRT.[11] An FRT identification starts with an officer retrieving an image—typically a screenshot from a surveillance video—of a suspect.[12] The officer then uses a commercial FRT algorithm to search for similar faces in a database comprised of mug shots, driver's license photographs, or images scraped from the internet.[13] The officer then selects one of the results from the algorithm for inclusion in a photo array, which consists of an

2. Geiger v. State, 174 A.3d 954, 965 (Md. Ct. Spec. App. 2017).

3. Clare Garvie, *What Defense Counsel Should Know About Facial Recognition Technology*, THE CHAMPION, May 2023, at 18 ("The first law enforcement system was established in 2001 by the Pinellas County Sheriff's Office in Florida.").

4. State v. Arteaga, 296 A.3d 542, 558 (N.J. Super. Ct. App. Div. 2023) (reversing a lower court decision denying discovery regarding the use of FRT); Lynch v. State, 260 So. 3d 1166, 1169–70 (Fla. Dist. Ct. App. 2018) (affirming a lower court decision denying relief under *Brady*); *Geiger*, 174 A.3d at 965 (holding that "[r]eliability does not matter").

5. Garvie, *supra* note 3, at 18.

6. Kelly Kasulis Cho, *Woman Sues Detroit After Facial Recognition Mistakes Her for Crime Suspect*, WASH. POST (Aug. 7, 2023), https://www.washingtonpost.com/nation/2023/08/07/michigan-porcha-woodruff-arrest-facial-recognition/.

7. *Id.*

8. *Id.*

9. *Id.*

10. *Id.*

11. CLARE GARVIE, GEORGETOWN L. CTR. ON PRIV. & TECH., A FORENSIC WITHOUT THE SCIENCE: FACE RECOGNITION IN U.S. CRIMINAL INVESTIGATIONS 9–13 (2022) [hereinafter GARVIE, FORENSIC WITHOUT THE SCIENCE].

12. *Id.* at 9–10.

13. *Id.* at 10.

image of the person selected by FRT along with filler images of known-innocent people.[14] Finally, the officer shows the photo array to a witness, who may make an identification.[15]

If eyewitness identification was a reliable investigative tool, this could serve to check any errors made by the machine. Unfortunately, eyewitness identification is notoriously inaccurate even without untested technologies. The Supreme Court has acknowledged that "[t]he vagaries of eyewitness identification are well-known," that "the annals of criminal law are rife with instances of mistaken identification,"[16] and that eyewitness identification is "the single greatest cause of wrongful convictions in this country."[17] Approximately 37% of witnesses in one study selected known-innocent fillers as perpetrators of crimes.[18] While eyewitness identification is deeply flawed, it is generally considered to be persuasive evidence against a defendant: "[T]here is almost nothing more convincing [at trial] than a live human being who takes the stand, points a finger at the defendant, and says 'That's the one!'"[19]

FRT is an immensely complex technology that interacts with a source of evidence that is notoriously unreliable—and surprisingly persuasive. Despite this confluence, law enforcement's use of FRT has almost completely evaded review. Law enforcement employs FRT in tens or hundreds of thousands of investigations each year,[20] but the accuracy of its use by law enforcement has never been evaluated in court.

This Article defines and describes witness-washing, the powerful mechanism of avoidance that has allowed FRT to evade review. Witness-washing is the process of using an algorithmic technology, incorporating the results of that technology into a human decision-making process, and then presenting the result as an exclusively human decision. The witness testimony is all that the State discloses. Consequently, law enforcement's use of algorithmic technology goes unnoticed and unexamined.

For FRT, this means that after the officer has confirmed the algorithmic results with a human eyewitness, the eyewitness identification is all that is introduced into the proceeding. The use of FRT is never mentioned. The technology disappears behind the eyewitness identification. The FRT identification has been witness-washed.

---

14. *Id.* at 12; *see* Cho, *supra* note 6.

15. GARVIE, FORENSIC WITHOUT THE SCIENCE, *supra* note 11, at 12.

16. United States v. Wade, 388 U.S. 218, 228 (1967).

17. Perry v. New Hampshire, 565 U.S. 228, 263 (2012) (Sotomayor, J., dissenting) (quoting State v. Henderson, 27 A.3d 872, 885 (N.J. 2011)).

18. Gary L. Wells, Margaret Bull Kovera, Amy Bradfield Douglass, Neil Brewer, Christian A. Meissner, & John T. Wixted, *Policy and Procedure Recommendations for the Collection and Preservation of Eyewitness Identification Evidence*, 44 L. & HUM. BEHAV. 3, 5, 19 (2020) [hereinafter Wells et al.] (excluding cases in which an innocent suspect was selected, as these are nearly impossible to measure in the field).

19. Watkins v. Sowders, 449 U.S. 341, 352 (1981) (Brennan, J., dissenting) (emphasis omitted) (quoting ELIZABETH F. LOFTUS, EYEWITNESS TESTIMONY 19 (1979)).

20. *See* discussion *infra* Section II.A.

The descriptive account of witness-washed FRT yields two insights. First, witness-washing shields investigative technologies from the sorts of limitations that, according to the traditional narrative of science in the courtroom, should rein in in the use of police investigative tools. Second, in the absence of scrutiny of these tools, the logic inherent in the tools themselves is overridden by the logic that structures the system in which they are deployed. For FRT, this means the carceral logic of the law enforcement agencies deploying it and the commercial logic of the companies developing it have drowned out the essentially exculpatory logic of the tool. This Article offers a corrective account of the function and use of the technology that witness-washing obscures, grounded in an array of technical sources and law enforcement materials.

This Article is a necessary intervention in existing scholarship on FRT and other algorithmic technologies. This body of scholarship has focused on the traditional pathways by which courts evaluate new technologies.[21] In the traditional account, courts hold hearings regarding the scientific validity of new technologies. They also make determinations about whether these technologies implicate rights such as the rights to privacy, confrontation, and due process. FRT scholarship has primarily focused on applying existing case law to this new technology to prepare litigators and judges to make decisions about these hearings when they eventually occur. But as this Article reveals, witness-washing prevents these hearings from occurring at all. This Article's descriptive account thus surfaces an overlooked and critical avenue for future scholarship.

This Article proceeds in five parts. Part I describes the traditional account of the pathway by which a forensic science technique such as FRT should enter the courtroom, as well as the traditional account of the failures of that pathway. Part II describes witness-washing, the mechanism that has allowed algorithmic technologies such as FRT to bypass this traditional pathway. Part III surfaces the underlying complexity of FRT, showing why the technology is in desperate need of further examination. Part IV analyzes the three traditional limitations on law enforcement use of investigative tools. It shows that statutes could constrain witness-washing but currently do not, that constitutional litigation is ill-suited to the task of restricting law enforcement use of FRT, and that the vital practical limitation of limited resources is almost entirely subverted by algorithmic tools. Finally, Part V describes the internal logic of FRT, and the ways in which that logic has been fully submerged in the carceral logic of law enforcement and the commercial logic of the profit-driven vendors who develop the technology.

Consider another case of facial similarity: the exoneration of Richard Jones. In 2000, Mr. Jones was wrongfully convicted of armed robbery and

21. *See* discussion *infra* Section I.D.

sentenced to nineteen years in prison.[22] People in prison would occasionally tell him that he looked just like another Ricky they knew, a man named Richard Amos.[23] The two men bore a striking resemblance, and further investigation revealed that Amos had lived at an address involved in the crime.[24] The witness who originally identified Mr. Jones was shown images of the two men, side-by-side, and asked if they could tell the two men apart.[25] The witness acknowledged that they could not.[26] Mr. Jones's conviction was vacated, and he was released after nearly two decades of incarceration.[27]

Mr. Jones's facial similarity resulted in an exoneration. Ms. Woodruff's resulted in a false arrest. Mr. Jones discovered his doppelgänger by luck. But Ms. Woodruff's false arrest was driven by FRT, a powerful algorithmic technology that law enforcement has widely and secretly adopted. In Mr. Jones's case, facial similarity gave rise to the defense that the crime he was convicted of was actually committed by someone who looked enough like him to be easily mistaken for him. But in a witness-washed environment with no opposing views, the facial similarities identified by FRT have been used solely to arrest people—like Ms. Woodruff—who are marked by the algorithm.

I. THE TRADITIONAL ACCOUNT OF SCIENTIFIC KNOWLEDGE IN THE COURTROOM

Science enters the courtroom through the adversarial expert witness. When a party seeks to offer evidence that is based on "scientific, technical, or other specialized knowledge," including the results of an algorithmic comparison tool such as FRT, they are required to call a witness who is qualified to testify to that knowledge.[28] Witness-washing is a mechanism that allows this requirement to be evaded. It allows a lay witness to introduce testimony that stems from a scientific technique without examination of the technology's accuracy and impact on the defendant's rights. In order to understand witness-washing, it is necessary to understand the history and current status of the introduction of scientific testimony through expert witnesses.

A. A Brief History of the Expert Witness

For the substantial majority of the history of the jury trial, there was great skepticism about the ability of jurors to accurately determine the

22. Christine Hauser, *Man Who Wrongfully Spent 17 Years in Prison in 'Doppelgänger Case' Seeks $1.1 Million*, N.Y. TIMES (Aug. 30, 2018), https://www.nytimes.com/2018/08/30/us/kansas-doppelganger-richard-jones.html.
23. *Id.*
24. *Id.*
25. *Id.*
26. *Id.*
27. *Id.*
28. FED. R. EVID. 702.

truth of a matter.[29] For hundreds of years after the inception of the jury trial in 1215, there was very little sense that the jury's job to puzzle out the facts of what had happened in the past.[30] Jury verdicts were guaranteed by the oath,[31] by confessions elicited through torture,[32] or—if it came to it—by counting the number of sworn witnesses on a given side.[33] This was in keeping with trial by ordeal and trial by combat, the forms of adjudication that predominated prior to the rise of the jury.[34] The adjudicatory principle was "*judiciam dei*": the accuracy of a verdict was guaranteed by an agreed-upon deity.[35]

There was very little notion of specialized knowledge during this time. The rules of evidence had long incorporated a distaste for "opinion testimony" and a strong preference for testimony regarding things a witness had seen, heard, or otherwise experienced firsthand.[36] Witnesses related their experiences, and the jury made common-sense deductions from that information. The law of proof initially required either direct testimony of multiple witnesses who had directly observed the crime as it occurred or that a suspect be caught with evidence of the crime in their possession.[37] Common types of criminal expert testimony—such as chemical analysis, DNA evidence, fingerprinting, handwriting analysis, and photography—had not been invented yet, and there were no organized police forces to start developing them.

When specialized knowledge was needed, it was not typically introduced through expert witnesses. Instead, courts used "(1) special juries, in which the decision-makers themselves had specialized knowledge that could help achieve a just resolution; and (2) advisors called by the court to

29. *See* George Fisher, *The Jury's Rise as Lie Detector*, 107 YALE L.J. 575, 579–80 (1997).

30. *Id.* at 583 (showing that criminal defendants could not call sworn witnesses until 1696); *see also* ALISON ADAM, A HISTORY OF FORENSIC SCIENCE: BRITISH BEGINNINGS IN THE TWENTIETH CENTURY 15 (2016) ("'Fact' and 'matters of fact' developed in law and were then taken up in other disciplines to the extent that they became part of general culture and intellectual life in the seventeenth and early eighteenth centuries in Britain."); MICHEL FOUCAULT, DISCIPLINE AND PUNISH 225 (Alan Sheridan trans., Vintage Books 2d ed.1995) (1975) ("The investigation as an authoritarian search for a truth observed or attested was thus opposed to the old procedures of the oath, the ordeal, the judicial duel, the judgement of God or even of the transaction between private individuals.").

31. Fisher, *supra* note 29, at 580 ("In the early years of the criminal trial jury, the system sought to stake its claim to legitimacy primarily in the oath and in the perceived divine power of the oath to compel truthful testimony.").

32. John H. Langbein, *Torture and Plea Bargaining*, 46 U. CHI. L. REV. 3, 3 (1978) ("Under certain circumstances the law permitted the criminal courts to employ physical coercion against suspected criminals in order to induce them to confess.").

33. 7 JOHN HENRY WIGMORE, WIGMORE ON EVIDENCE: EVIDENCE IN TRIALS AT COMMON LAW § 2032, at 330 (1978) ("The vital force of this quantitative view of a witness' testimony is seen pressing to the surface in abundant casual instances down into the 1700's [sic]. . . .").

34. Fisher, *supra* note 29, at 585–86.

35. *See id.*

36. In other instances there were no independent witnesses at all. Some juries were "self-informing" and consisted of people who were already familiar with the parties and the facts. *Id.* at 591–92.

37. Langbein, *supra* note 32, at 4 ("[I]t would not have mattered in this system that the suspect was seen running away from the murdered man's house and that the bloody dagger and the stolen loot were found in his possession. Since no eyewitness saw him actually plunge the weapon into the victim, the court could not convict him of the crime.").

assist either the judge or the jury in understanding the issues."[38] These methods shared the advantage of relying on neutral experts, who were not paid by or beholden to either party.

The current system of expert testimony appears to have arisen as an accident of history. As one scholar explains, "[t]he earliest case in which scientific expert testimony was used and where the experts testified as partisan witnesses is widely taken to be the 1782 civil case *Folkes v. Chadd*."[39] The case involved the decay of a harbor.[40] One party objected to the other party calling an engineer as a witness.[41] The engineer had specialized knowledge of harbors but had not personally witnessed the event that sparked the litigation.[42] The judge allowed the engineer to testify, stating that "[he could not] believe that where the question is, whether a defect arises from natural or an artificial cause, the opinions of men of science are not to be received. . . . The cause of the decay of the harbor is also a matter of science."[43]

Unfortunately, the decision did not address *how* the opinions of men of science should be introduced, and the method it settled on created perverse incentives. Well-resourced parties began to shop for technical witnesses in any case in which they could be helpful.[44] This demand created institutions of knowledge dedicated solely to providing testimony in courts, which began to develop and present evidence in line with their financial incentives.[45] "[O]ver a period of centuries, the move was made from juries as witnesses, to juries without witnesses with expert witnesses as court advisers, and finally to the system of partisan expert witnesses."[46]

The flaws of this system quickly became apparent. "The modern expert witness was . . . roundly criticized and condemned from just about the moment of its invention."[47] In 1901, for example, Judge Learned Hand characterized the adversarial use of expert witnesses as "not satisfactory to any one" and noted that "the criticism comes with great unanimity."[48] This Article discusses these criticisms in greater detail below, but first, it is necessary to understand the doctrinal framework in which they appear.

---

38. Jennifer L. Mnookin, *Idealizing Science and Demonizing Experts: An Intellectual History of Expert Evidence*, 52 VILL. L. REV. 763, 767 (2007).

39. ADAM, *supra* note 30, at 21; *see also* Mnookin, *supra* note 38, at 769 ("A 1782 civil case, Folkes v. Chadd, in which a well-respected engineer named John Smeaton testified on behalf of one party, is often cited as providing official judicial sanction of adversarial expert testimony . . . .").

40. ADAM, *supra* note 30, at 21.

41. Folkes v. Chadd (1782) 99 Eng. Rep. 589, 589 (KB).

42. ADAM, *supra* note 30, at 21.

43. *Folkes*, 99 Eng. Rep. at 590.

44. Mnookin, *supra* note 38, at 770.

45. *Id.* at 771–72.

46. ADAM, *supra* note 30, at 21.

47. Mnookin, *supra* note 38, at 770.

48. Learned Hand, *Historical and Practical Considerations Regarding Expert Testimony*, 15 HARV. L. REV. 40, 52–53 (1901).

B. The Traditional Account of Forensic Science in Law

Doctrinally, the entry point for a technology like FRT into the courtrooms is governed by the rules for the admission of expert testimony. One party to a dispute calls an expert witness to testify about the technology, and a judge decides whether to allow their testimony.

Prior to the adoption of the Federal Rules of Evidence, the most common test for this question was the test articulated in *Frye v. United States*.[49] *Frye* framed the inquiry in terms of a "twilight zone" of accuracy, in which a scientific technique crosses, at some point, "the line between the experimental and demonstrable stages."[50] The judge looks to "general acceptance in the particular field in which [the scientific principle or discovery] belongs" to determine whether the technology has crossed this line in the twilight zone.[51] In *Frye*, the court applied this test to determine that a defendant could not introduce the results of a lie detector test as proof of innocence—lie detectors were not generally accepted as accurate—but the court gave little guidance as to how courts should measure general acceptance of a technology.[52]

In 1993 the Supreme Court, in *Daubert v. Merrell Dow Pharmaceuticals, Inc.*,[53] set out a new multifactor test for the admission of expert testimony in federal courts, later codified through an amendment to the Federal Rules of Evidence.[54] "Scientific validity" is the underlying question in the *Daubert* analysis.[55] The judge asks whether the specialized knowledge "rests on a reliable foundation and is relevant to the task at hand" and considers falsifiability, peer review, known error rates, and general acceptance in the relevant scientific community.[56] The literature elaborating upon and criticizing *Daubert* is immense, and a comprehensive account of it is well beyond the scope of this Article. But the goal of *Daubert* is the same as *Frye*: to determine whether there is good reason to believe that an expert is testifying to science that works.

The standard narrative of science in courts does not stop at admissibility. Scientific evidence can be reliable, accurate, and correctly applied, but still run afoul of a defendant's rights or other principles embedded in the legal system. This Article examines primarily the criminal legal system rights that FRT could impact: (1) the right to be free from unreasonable searches and seizures guaranteed by the Fourth Amendment, (2) the right

49. 293 F. 1013 (D.C. Cir. 1923); *see also* DAVID L. FAIGMAN, EDWARD K. CHENG, ERIN E. MURPHY, JOSEPH SANDERS, & CHRISTOPHER SLOBOGIN, MODERN SCIENTIFIC EVIDENCE: THE LAW AND SCIENCE OF EXPERT TESTIMONY § 1:4 (2024–2025 ed.) (demonstrating that the *Frye* test was the most common test prior to the adoption of the Federal Rules of Evidence).

50. *Frye*, 293 F. at 1014.

51. *Id.*

52. *Id.* ("Just when a scientific principle or discovery crosses the line between the experimental and demonstrable stages is difficult to define.").

53. 509 U.S. 579 (1993).

54. FED. R. EVID. 702.

55. *Daubert*, 509 U.S. at 594.

56. *Id.* at 597.

to confront witnesses enshrined in the Sixth Amendment, (3) the right to the disclosure of exculpatory information articulated in *Brady v. Maryland*,[57] and (4) the right to be protected from unduly suggestive eyewitness identification procedures as articulated in *United States v. Wade*.[58] When a defendant believes that a particular piece of scientific evidence violates one of these rights, they can file a pretrial motion requesting a hearing and suppression of that evidence.

In this narrative, scientific techniques are introduced into litigation through an expert witness who a party intends to call if the case reaches trial. Courts screen these scientific techniques to make sure that they are accurate in general, and also accurate as applied in a particular case. The defense then files motions contesting the use of the technology in the case, which guarantees that the technology does not violate rights to freedom from unreasonable searches, confrontation, due process, or any other embedded principles of the criminal legal system.

This account appears to be a fairly accurate representation of how police technology came to be deployed in criminal law throughout the twentieth century. Law enforcement in the United States first adopted fingerprint analysis for identification of suspects around 1904.[59] An appeals court examined the reliability of fingerprint analysis for the first time seven years later, in 1911.[60] Even bite mark evidence, which was later shown to be entirely lacking in an empirical basis, was subjected to a hearing regarding its admissibility as soon as law enforcement began using it.[61]

The most well-known example of this process is the introduction of modern DNA profiling.[62] The technology was first used in 1987,[63] and the first appeals court ruled on the use of the technology in *People v. Castro*[64] in 1989. The initial hearing regarding admissibility "took place over a 12-week period producing a transcript of approximately 5,000 pages."[65] The introduction of DNA evidence also prompted litigation regarding impacted rights. The Supreme Court has held that routine government

57. 373 U.S. 83, 87 (1963).

58. 388 U.S. 218, 236–37 (1967).

59. Jeffery G. Barnes, *History*, *in* NAT'L INST. OF JUST., THE FINGERPRINT SOURCEBOOK 1–5, 1–16 (2011).

60. People v. Jennings, 96 N.E. 1077, 1082 (Ill. 1911) (noting that four expert witnesses were called in the first American appeals case regarding the admissibility of fingerprints).

61. People v. Marx, 126 Cal. Rptr. 350, 353 (Cal. Ct. App. 1975). *See generally* M. CHRIS FABRICANT, JUNK SCIENCE AND THE AMERICAN CRIMINAL JUSTICE SYSTEM 220 (2022) (narrating the "Bite Mark Wars" regarding admissibility of bite mark evidence in courts). Given the shaky foundations of bite mark analysis, it is difficult to determine a point at which the technique was "developed."

62. *See generally* ERIN E. MURPHY, INSIDE THE CELL: THE DARK SIDE OF FORENSIC DNA 8, 106–19 (2015) (analyzing the growth and various failures of forensic DNA testing).

63. DAVID H. KAYE, THE DOUBLE HELIX AND THE LAW OF EVIDENCE 67 (2010) (describing a hearing regarding VNTR profiling that "dragged on for more than three months and produced a transcript of 5,000 pages" in 1989, after the development of a technique in 1987).

64. 545 N.Y.S.2d 985 (N.Y. Sup. Ct. 1989).

65. *Id.* at 986.

collection of DNA on arrest is not an unreasonable search,[66] that due process does not require disclosure of untested DNA evidence to challenge a conviction,[67] and that defendants have a right to confront DNA technicians.[68] The new technology prompted extensive litigation by defense attorneys regarding the protected rights of their clients, and an extensive literature about how to file and argue these motions[69] and how judges should decide them.[70]

The introduction of DNA analysis provides a clear example of the traditional approach to forensic science in courts. Courts reviewed the theoretical and practical accuracy of the technique as soon as prosecutors began using it in criminal proceedings, and defendants immediately began litigating to protect the rights that the new technology implicated.

C. The Traditional Failures of Forensic Science in Law

There is a general academic consensus that the integration of science into legal proceedings has been a disaster, and that the integration of forensic science into criminal prosecutions has been even worse. As one legal scholar summed up the history of the *Frye* test in 1980, "[t]he *Frye* test, which has cast its shadow over the admissibility of scientific evidence for more than a half-century, has proved unworkable."[71] "Commentators," he noted, "have not been restrained in their criticism of the *Frye* test."[72] The Supreme Court's guidelines in *Daubert* have hardly fared better. The literature elaborating upon and criticizing *Daubert* is immense.[73] A full accounting of the criticisms of adversarial expert testimony is beyond the scope of this Article, but the core criticisms are, roughly, that (1) courts are under-resourced and unspecialized;[74] (2) judges are fundamentally

66. Maryland v. King, 569 U.S. 435, 465–66 (2013).

67. Dist. Att'y's Off. for Third Jud. Dist. v. Osborne, 557 U.S. 52, 74–75 (2009).

68. Williams v. Illinois, 567 U.S. 50, 57–58 (2012); *see also* Smith v. Arizona, 602 U.S. 779, 783, 785 (2024) (clarifying the Supreme Court's Confrontation Clause jurisprudence with regards to lab technicians).

69. *See, e.g.*, NACDL Press, *DNA Evidence Trial Pack: Practical DNA Solutions*, MYNACDL, https://my.nacdl.org/s/product-details?id=a1B8Z000013wAIKUA2 (last visited Feb. 12, 2025) ("Understanding DNA evidence is difficult. You're an attorney, not a scientist.").

70. *See, e.g.*, David H. Kaye & George Sensabaugh, *Reference Guide on DNA Identification Evidence*, *in* REFERENCE MANUAL ON SCIENTIFIC EVIDENCE 129, 131 (The Nat'l Acads. Press ed., 3d ed. 2011).

71. Paul C. Giannelli, *The Admissibility of Novel Scientific Evidence:* Frye v. United States*, a Half-Century Later*, 80 COLUM. L. REV. 1197, 1250 (1980).

72. *See id.* at 1206 n.59 and accompanying text.

73. FAIGMAN, CHENG, MURPHY, SANDERS, & SLOBOGIN, *supra* note 49, § 1:7 n.2 ("Thousands of articles have been published in response to the *Daubert* decision.").

74. Jules Epstein, *The National Commission on Forensic Science: Impactful or Ineffectual?*, 48 SETON HALL L. REV. 743, 757 (2018) ("Studies have shown an appalling lack of understanding of *Daubert*/Rule 702 terms such as 'error rate.' Judges, when surveyed, have acknowledged 'that their [scientific] education had left them inadequately prepared to serve as gatekeepers under *Daubert*[;]' and on specifics such as the scientific concept of 'falsifiability,' at best, thirty-five percent of those surveyed grasped the essence of the term, while only four to six percent were able to clearly articulate the meaning of the term.").

unqualified to evaluate the validity of an expert's opinions;[75] (3) litigants can buy any opinion that they seek, and paid experts are incentivized to stretch scientific techniques to their limits (or beyond them);[76] and (4) prior admissions by any court create a cascading effect in which courts save time by admitting evidence without evaluating its validity just because other courts have admitted it before.[77] Adversarial litigators push questionable science before overwhelmed courts, and any eventual admission can cascade into a wave of "junk science."

The admission of forensic science into criminal courts has met with even greater criticism than the admission of science into courts more generally. In 2009, the National Academy of Sciences (NAS) released a report, *Strengthening Forensic Science*, finding that "[i]n a number of forensic science disciplines, forensic science professionals have yet to establish either the validity of their approach or the accuracy of their conclusions, and the courts have been utterly ineffective in addressing this problem."[78] Seven years later, the President's Council of Advisors on Science and Technology (PCAST) followed up on the state of forensic science in the courts and found that only two of seven common forensic sciences had achieved foundational validity—most did not produce results that were not repeatable, reproducible, and accurate.[79] Studies show that courts strongly favor admission of evidence offered by the State, even when that evidence lacks foundational validity.[80] It is impossible to know how many innocent people have been convicted based on evidence that lacked scientific validity, but by one estimate, 43% of people who have been exonerated by DNA

75. Edward K. Cheng, *The Consensus Rule: A New Approach to Scientific Evidence*, 75 VAND. L. REV. 407, 471–72 (2022) ("[T]he *Daubert* framework should be scrapped. It invites dilettantism, asking lay judges and jurors to learn just enough about an area of expertise in a short period of time to be dangerous."); *id.* at 414 (describing the "expert paradox," in which judges are expected to evaluate the validity of expert knowledge, despite their lack of that knowledge being why the expert was called in the first place).

76. Edith Beerdsen, *Litigation Science After the Knowledge Crisis*, 106 CORNELL L. REV. 529, 565 (2021) ("When expert witnesses are retained to conduct analyses or experiments, just like their colleagues in academic science, they face powerful incentives to produce a particular type of result . . . .").

77. Jennifer L. Mnookin, *Scripting Expertise: The History of Handwriting Identification Evidence and the Judicial Construction of Reliability*, 87 VA. L. REV. 1723, 1742 (2001) ("[H]andwriting evidence became reliable (or at least came to be believed reliable) because courts declared it admissible.").

78. COMM. ON IDENTIFYING THE NEEDS OF THE FORENSIC SCIS. CMTY., NAT'L RSCH. COUNCIL, STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD 53 (2009).

79. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., FORENSIC SCIENCE IN CRIMINAL COURTS: ENSURING SCIENTIFIC VALIDITY OF FEATURE-COMPARISON METHODS 7–14 (2016) (finding that single-source and simple mixture DNA analysis and latent fingerprint analysis had achieved scientific validity, and complex DNA analysis had achieved validity in very limited circumstances); *see also id.* at 47–54 (defining foundational validity).

80. Erin Murphy, *Neuroscience and the Civil/Criminal Daubert Divide*, 85 FORDHAM L. REV. 619, 627 (2016) ("When faced with evidence offered by prosecutors or civil defendants, courts tend to take a generous approach, whereas even the same kind of evidence offered by civil plaintiffs is met with great skepticism."); *see also* Jim Hilbert, *The Disappointing History of Science in the Courtroom: Frye, Daubert, and the Ongoing Crisis of "Junk Science" in Criminal Trials*, 71 OKLA. L. REV. 759, 762 (2019) ("Since *Daubert*, courts have not used the decision to reign in the junk science of criminal prosecutions.").

evidence were convicted in part due to the misapplication of forensic science.[81]

The NAS and PCAST reports mostly address technologies that were developed in the twentieth century, and the introduction of digital technologies like FRT has only made the problem worse. Professor Erin Murphy locates the problem in a shift in the nature of modern technologies.[82] Most new law enforcement technologies are "second generation forensic," which are distinguished by database dependency, privatization, and technological sophistication.[83] Many scholars have also pointed to the surveillant nature of new technologies, which makes them less likely to trigger judicial scrutiny.[84] The law enforcement culture of secrecy only exacerbates the lack of disclosure and evaluation.[85] Many new technologies are developed by private companies that also insist on secrecy, and as a result, police departments have even resorted to parallel construction of investigations to keep technology secret.[86]

There is also an academic consensus that criminal courts are failing to rigorously defend constitutional safeguards and other embedded principles as technology develops. Current Fourth Amendment enforcement is "an embarrassment,"[87] widely regarded as having so many exceptions that the rule barely applies anymore,[88] and especially ill-suited to addressing developing technology.[89] The right to exculpatory information under *Brady* is generally considered a "failed promise"[90] because its doctrinal framework makes it almost impossible to enforce.[91] The right to eyewitness identification procedures that are not unduly suggestive is also barely

81. *DNA Exonerations in the United States (1989–2020)*, INNOCENCE PROJECT, https://innocenceproject.org/dna-exonerations-in-the-united-states (last visited Feb. 1, 2025).

82. Erin Murphy, *The Mismatch Between Twenty-First-Century Forensic Evidence and Our Antiquated Criminal Justice System*, 87 S. CAL. L. REV. 633, 636–37 (2014).

83. *Id.*

84. Barry Friedman, Farhang Heydari, Max Isaacs, & Katie Kinsey, *Policing Police Tech: A Soft Law Solution*, 37 BERKELEY TECH. L.J. 705, 717 (2022); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 803–04 (2004). *See generally* STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER 115 (2012) (addressing the Supreme Court's ongoing failure to apply the Fourth Amendment to developing technology).

85. Christina Koningisor, *Police Secrecy Exceptionalism*, 123 COLUM. L. REV. 615, 655–62 (2023) (listing a variety of ways in which police departments routinely evade transparency laws).

86. *See, e.g.*, Jonathan Manes, *Secrecy & Evasion in Police Surveillance Technology*, 34 BERKELEY TECH. L.J. 503, 516 (2019) (defining "parallel construction" as "the practice of conducting a second, parallel investigation designed to 'discover' evidence that was previously identified using the secret technology").

87. Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 757 (1994) ("The Fourth Amendment today is an embarrassment.").

88. MICHELLE ALEXANDER, THE NEW JIM CROW 61 (2010) ("With only a few exceptions, the Supreme Court has seized every opportunity to facilitate the drug war, primarily by eviscerating Fourth Amendment protections against unreasonable searches and seizures by the police.").

89. Maneka Sinha, *The Automated Fourth Amendment*, 73 EMORY L.J. 589, 630 (2024) ("Fourth Amendment doctrine has not kept pace with technology-driven policing.").

90. THOMAS L. DYBDAHL, WHEN INNOCENCE IS NOT ENOUGH: HIDDEN EVIDENCE AND THE FAILED PROMISE OF THE BRADY RULE, ch. 9 (2023).

91. *See* Justin Murray, *Prejudice-Based Rights in Criminal Procedure*, 168 U. PA. L. REV. 277, 295–318 (2020) (critiquing the standard of review for *Brady* claims).

enforced[92]—many law enforcement agencies continue to regularly employ showups,[93] which are among the most suggestive procedures.[94] And the Confrontation Clause is poorly adapted to address developing technologies due to its focus on human testimony.[95] Each of these topics is the subject of decades of scholarship.[96] The important point here is not the contours of that scholarship but simply that the hearings that are evaded by witness-washing are deeply flawed even when they do occur.

FRT is situated at the nadir of the layered failures of science in the courtroom. It is a second-generation forensic science that would be offered by the prosecution, and the rights that it impacts are poorly guarded. But no one doubts that the principles of accuracy, privacy, confrontation, and due process are incredibly important, and there are strong reasons to believe that law enforcement use of FRT violates them. The existing scholarship on FRT mostly tracks the traditional narrative and the traditional flaws. For FRT, those flaws are severe.

D. The Traditional Account of FRT

Although FRT has almost entirely evaded judicial review, there is a growing body of legal scholarship regarding the technology. This literature follows the traditional narrative.[97] These arguments assume that FRT will begin to be litigated as it is used more often, as predicted by the traditional narrative.[98] In this account of FRT's intergration into the criminal legal system, prosecutors will soon begin moving FRT into evidence through expert witnesses. This will trigger inquiries into accuracy under *Frye* or *Daubert*, depending on the jurisdiction. Defendants will then file motions arguing that their rights have been impacted by the technology. As discussed in Part II, this moment is unlikely to arrive because

92. *See* discussion *infra* Section IV.B.

93. Stephen P. Bertelsman, *Defending Due Process: The Case for Abolishing the Show-Up Line-Up*, 68 WASH. U. J.L. & POL'Y 245, 263 (2022) ("Despite reams of court decisions denouncing suggestive evidence, show-ups continue to be admitted into evidence and remain a common police investigatory tactic.").

94. *See* Stovall v. Denno, 388 U.S. 293, 302 (1967) ("The practice of showing suspects singly to persons for the purpose of identification, and not as part of a lineup, has been widely condemned.").

95. *See generally* Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 2046–47 (2017) (explaining that litigants have difficulty convincing courts that evidence from technology such as machine conveyances is testimonial under the Confrontation Clause).

96. *See generally, e.g.*, ANTHONY G. AMSTERDAM & RANDY HERTZ, 3 TRIAL MANUAL 8 FOR THE DEFENSE OF CRIMINAL CASES (8th ed. 2023); FAIGMAN, CHENG, MURPHY, SANDERS, & SLOBOGIN, *supra* note 49.

97. *See, e.g.*, Laura Moy, *Facing Injustice: How Face Recognition Technology May Increase the Incidence of Misidentifications and Wrongful Convictions*, 30 WM. & MARY BILL RTS. J. 337, 366 (2021) (addressing barriers to traditional litigation).

98. *See* GARVIE, FORENSIC WITHOUT THE SCIENCE, *supra* note 11, at 50 ("[I]t is only a matter of time before a prosecutor seeks to introduce a face recognition match as evidence in a criminal case."); Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1166 (2021) (asking "[i]f facial recognition becomes a preferred policing tool, does the Fourth Amendment offer any constitutional protection?"); Jessica Gabel Cino, Heather Kleider-Offutt, Beth Stevens, Kat Albrecht, Robert Evans, & Emma Riedley, *The Oracle Testifies: Facial Recognition Technology as Evidence in Criminal Courtrooms*, 61 U. LOUISVILLE L. REV. 137, 138 (2022) ("As the technology advances, it will become increasingly prevalent in all types of criminal cases, making it necessary to make important informed decisions about its evidentiary use now.").

witness-washing obstructs the traditional pathway. But the scholarship gives strong reason to believe that FRT would face grave challenges at each step in the traditional process.

There are strong reasons to believe that FRT (1) lacks foundational validity, (2) evades Fourth Amendment concerns regarding search and seizure on convoluted doctrinal grounds, (3) lacks an avenue for meaningful confrontation, (4) is unnecessarily suggestive in violation of Due Process rights, and (5) always creates exculpatory information that must be disclosed under *Brady*.

Regarding the scientific validity of the technology, FRT scholar Clare Garvie has identified many of FRT's failures in her report *A Forensic Without the Science*.[99] She concludes that "[f]ace recognition overwhelmingly fails the *Daubert* standard."[100] No peer-reviewed studies have analyzed the reliability of law enforcement uses of FRT; there are no set standards for the use of the technology; as-applied error rates are unknown; and there is no consensus regarding the scientific validity of FRT within the relevant scientific community.[101] Current uses of FRT fail every prong of the *Daubert* analysis. Part III discusses several of these factors at greater length.

With regards to the rights implicated by the technology, law and technology scholar Andrew Guthrie Ferguson has comprehensively analyzed the privacy concerns that FRT raises.[102] He concludes that FRT identification does not trigger Fourth Amendment privacy protections because faces are not protected and there is no doctrinal hook to prevent the government from using legally obtained images of faces in any way it sees fit.[103] If law enforcement uses FRT more aggressively, such as for "data aggregation, data permanence, long-term tracking, arbitrary monitoring, and the permeation of surveillance technologies," then the technology may trigger Fourth Amendment protections under a mosaic theory of privacy that protects against systems of surveillance even as individual invasions are not protected.[104] But current practices are unlikely to trigger Fourth Amendment protections, even though they raise serious privacy concerns.[105]

Literature on the intersection of the Confrontation Clause and FRT is minimal,[106] but the literature on machine tools generally suggests that FRT

---

99. *See* GARVIE, FORENSIC WITHOUT THE SCIENCE, *supra* note 11, at 46 (describing four factors that face recognition fails to meet).

100. *Id.* at 45 (italics added).

101. *Id.* at 46.

102. *See generally* Ferguson, *supra* note 98, at 1108; *see also* David Gray, *Bertillonage in an Age of Surveillance: Fourth Amendment Regulation of Facial Recognition Technologies*, 24 SMU SCI. & TECH. L. REV. 3, 9 (2021) (addressing FRT and the Fourth Amendment).

103. Ferguson, *supra* note 98, at 1128.

104. *Id.* at 1134–35.

105. *Id.* at 1152 ("Under current doctrine, there is no constitutional check on the use of [FRT identification], allowing police to use it at-will without legal process.").

106. *See, e.g.*, Emma Lux, *Facing the Future: Facial Recognition Technology Under the Confrontation Clause*, 57 AM. CRIM. L. REV. 20, 21 (2020).

raises Confrontation Clause concerns. Professor Andrea Roth, in her thorough analysis of machine testimony in courts, argues that "the 'distributed cognition' between man and technology that underlies machine conveyances" requires confrontation of both the "human programmers" and the algorithm itself for "meaningful impeachment" regarding accuracy and bias.[107] She argues that "the more inscrutable a machine process, the more its accusatory conveyances threaten the dignity of the accused and the perceived legitimacy of the process."[108] FRT is an inscrutable machine process that leads to the accusation of a defendant, and which threatens the dignity of defendants and the legitimacy of the process.[109]

With regards to unduly suggestive eyewitness identification, Professor Laura Moy provides a compelling account of how the use of FRT leads to unduly suggestive eyewitness identifications. The core problem is that "[u]nrelated people can sometimes resemble each other" extremely closely.[110] The presence of very similar faces in a photo array drastically decreases the accuracy of identification because people are not skilled at telling very similar faces apart.[111] There is a strong argument that the use of FRT to select between very similar faces creates a substantial likelihood of misidentification through the introduction of nearly indistinguishable doppelgängers.

There is a gap in the academic literature on FRT and the due process right to exculpatory information.[112] Section V.A. will discuss FRT and the right to exculpatory information at some length. In short, FRT algorithms typically output a list of very similar-looking individuals. This list provides any given person in the list with a strong third-party guilt defense—that the crime was committed not by them but by another person on the list who looks so much like them that they are easily mistaken for one another.

There is a relatively robust academic engagement with FRT through the lens of the traditional narrative of forensic science in courts. There are very strong grounds on which to challenge the scientific validity of FRT as applied, and persuasive arguments that the technology violates many of the principles that are embedded in the legal system. The problem with this traditional narrative is that FRT is almost completely evading the

107. Roth, *supra* note 95, at 2036.

108. *Id.* at 2042.

109. *See* discussion *infra* Section III.C (describing how FRT introduces a confounding variable in the eyewitness identification procedure, causing unreliable results with the witness and harming the defendant).

110. Moy, *supra* note 97, at 350.

111. Wells et al., *supra* note 18, at 17 (reporting a study in which "using [a] large database of faces for selecting fillers resulted in a reduction in accurate identifications of the culprit by producing too much similarity between the fillers and the suspect").

112. It has been the subject of a student note. *See generally* Rebecca Darin Goldberg, *You Can See My Face, Why Can't I? Facial Recognition and* Brady, 5 COLUM. HUM. RTS. L. REV. ONLINE 261, 265 (2021).

traditional channels through which new scientific tools are tested in courtrooms.

II. WITNESS-WASHING

This Part describes the mechanism that currently allows FRT to evade review. Courts have not subjected FRT to any tests of reliability and accuracy, defendants have filed only a handful of motions alleging that law enforcement's use of FRT violated their rights, and law enforcement has only disclosed its reliance on FRT to defendants and the public in very limited ways. The primary reason for this silence is that the technology is subject to witness-washing.

A. Witness-Washing: A Definition

The increasing prevalence of machine processes in the criminal law has created a new role for the witness. Witnesses now frequently function as ciphers for the use of complex technology. Prosecutors present mixed human–machine decision-making processes as entirely human, preventing any inquiry into the accuracy, appropriateness, or effectiveness of new technologies.

Witness-washing has three steps. First, a complex technology is deployed in a process that will end up in court, and in a way that is critical to the integrity of the proceedings. In the case of FRT, this means that the algorithm searches a database for similar-looking faces, with the aim of assisting in an identification. Second, the algorithm's output is used as the basis of a subsequent decision by a person. With FRT, this typically means that a detective includes a picture of a person that the algorithm suggested in a photo lineup. Finally, that result is presented solely as a result of a human decision, without any mention of the use of a complex algorithmic process. For FRT, this means that law enforcement presents the identification solely as if the witness had selected a photo in a traditional identification process, with no mention of the use of FRT to select the individual who appeared in the lineup.

It is difficult to find examples of a secret process. Fortunately, an example of how FRT might enter into a proceeding without mention of the technology is available in the testimony in *Lynch v. State*.[113] In *Lynch*, the defendant was able to depose a witness prior to trial, which is allowed in Florida but generally rare in criminal law.[114] The deposition showed that law enforcement used FRT in their investigation by using FRT on an image of a suspect that was taken by the detectives.[115] But at trial, the use of FRT was witness-washed. The prosecution called two detectives, Prescott and Canaday, who had participated in an undercover drug buy:

113. 260 So. 3d 1166, 1169 (Fla. Dist. Ct. App. 2018).
114. *See id.*; *see also* FLA. R. CRIM. P. 3.220(h)(1).
115. *Lynch*, 260 So. 3d at 1168–69.

> [Detective Prescott] testified that a few weeks after the transaction he obtained Appellant's name as a potential suspect through investigation. He testified that he then looked at pictures of Appellant in a "known database" and concluded that it was Appellant who sold him the cocaine. Prescott then identified Appellant in court as the man who sold him the crack . . . . [Detective] Canaday testified that the photos entered into evidence as State's 1, 2, and 3 were of the individual who sold them the crack cocaine. Canaday then identified Appellant in court as the man who sold them the cocaine.[116]

Here, the algorithmic process was turned , which explained the identification in the same way they would have explained without the FRT. In this case, the detectives testified as one would expect from a photo showup, a process in which a witness is shown a single photograph and asked if it is a person they have seen before. The witness then makes an in-court identification at trial. Photo showups are as old as photography, and in-court identifications are as old as courts. This precise testimony—with a physical book of mug shots instead of a computer database—could have appeared in an American court a hundred years ago.[117]

In *Lynch*, we know that FRT was used because of the facial recognition analyst's prior deposition. She testified that "the software would assign a number of stars indicating the likelihood of a match, but she did not know how many stars were possible or how the program worked."[118] She did know that Mr. Lynch's photo had one star below it, but she did not know what the star meant.[119]

Lynch is the rare case in which the use of witness-washed FRT is known. The testimony clearly shows the vital third step in witness-washing. Algorithmic tools secretly enter proceedings through vague references such as "through investigation," or simply through the omission of any testimony about algorithmic processing prior to an in-court identification. The proponent of the evidence makes the decision to strategically hide the use of technology. The technology disappears entirely behind the witness. Witness-washing allows prosecutors to avoid litigating a complex technological issue in favor of presenting evidence as a direct eyewitness identification, which litigators traditionally consider both very strong for the prosecution and very straightforward.[120] The litigation costs are much

116. Initial Brief of Appellant at 7, 9, Lynch v. State, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018) (No. 1D16-3290).

117. *See, e.g.*, Manson v. Brathwaite, 432 U.S. 98, 108 (1977) ("[A] trained police officer . . . . gave a detailed description . . . . it enabled [a detective] to pick out a single photograph that was thereafter positively identified by [the police officer] . . . . [at] the in-court identification, [the officer] had 'no doubt' that Brathwaite was the person who had sold him heroin.").

118. *Lynch*, 260 So. 3d at 1169.

119. *Id.*

120. Watkins v. Sowders, 449 U.S. 341, 352 (1981) (Brennan, J., dissenting) (emphasis omitted) ("[T]here is almost nothing more convincing [at trial] than a live human being who takes the stand, points a finger at the defendant, and says 'That's the one!'").

lower than moving to admit the technology itself, and the result still appears in court as powerful evidence.

The scope of witness-washing is generally unclear, but we know that law enforcement has used FRT in hundreds of thousands, if not millions, of investigations. Around 10% of law enforcement agencies in the United States reported operating FRT in June of 2020, but there is minimal data on the scope of their use.[121] Pinellas County, Florida, at one point reported conducting 8,000 searches per month.[122] The U.S. Government Accountability Office (GAO) found that federal agencies had recorded at least 60,000 FRT searches as of 2023 despite having no training requirements or use policies.[123] In response to a Freedom of Information Act request, the New York Police Department (NYPD) disclosed that it has used FRT since 2011, with at least 22,000 searches between 2016 and 2019.[124] State agencies have also used FRT for at least a decade to trawl Department of Motor Vehicles (DMV) databases for potential duplicate or fraudulent driver's license applications, resulting in an unknown number of prosecutions.[125]

Despite the constant use of FRT, witness-washing has allowed FRT to almost entirely evade review: appeals courts have examined FRT only three times since it was first used in 2001. It is currently impossible to determine how many investigations, pretrial proceedings, and trials have involved witness-washed FRT. We do not know how often law enforcement statements that read exactly like statements from a hundred years ago are in fact ciphers for the use of powerful algorithmic technology. Witness-washing has allowed a shadow system of algorithmic technology to emerge.

B. Witness-Washed FRT

Witness-washing has allowed law enforcement use of FRT to proliferate free from meaningful review. In most instances, witness-washing has completely prevented FRT from even being mentioned. Even when its use

---

121. Mariana Oliver & Matthew B. Kugler, *Surveying Surveillance: A National Study of Police Department Surveillance Technologies*, 54 ARIZ. ST. L.J. 103, 123 (2022) ("Despite widespread concerns about facial recognition and debates over the accuracy of facial recognition software, we lack evidence as to how many local police departments have access to this high-tech tool. Efforts have been made to compile such a list but have largely been limited to small samples.").

122. GARVIE, FORENSIC WITHOUT THE SCIENCE, *supra* note 11, at 2.

123. U.S. GOV'T ACCOUNTABILITY OFF., GAO-23-105607, FACIAL RECOGNITION SERVICES: FEDERAL LAW ENFORCEMENT AGENCIES SHOULD TAKE ACTIONS TO IMPLEMENT TRAINING, AND POLICIES FOR CIVIL LIBERTIES 19 (2023) [hereinafter GAO, FACIAL RECOGNITION SERVICES].

124. Nadine El-Bawab & Kiara Alfonseca, *More Facial Recognition Technology Reported in Non-White Areas of NYC: Amnesty International*, ABC NEWS (Feb. 14, 2022, 5:01 PM), https://abcnews.go.com/US/facial-recognition-technology-reported-white-areas-nyc-amnesty/story?id=82798528.

125. People v. Byrd, 946 N.Y.S.2d 642, 643–44 (N.Y. App. Div. 2012) ("Although the defendant applied for the license using a false name, facial recognition software used by the New York State Department of Motor Vehicles . . . caused the defendant's outstanding warrant to come up when the defendant applied for the license.").

is disclosed, courts have endorsed witness-washing in a way that avoids meaningful analysis of the technology.

The most direct endorsement of witness-washing in a court opinion—and the clearest warning of the difficulties it creates for meaningful evaluation—is the Court of Special Appeals of Maryland's opinion in *Geiger v. State*.[126] The decision is worth quoting at length because it illustrates many of the difficulties litigants face with witness-washed technologies:

> Facial profiling technology is a new weapon in the investigative arsenal, but it is one increasingly familiar to any aficionado of modern-day detective dramas on television. A photograph of a face, such as the one from the fake North Carolina driver's license in this case, is fed into the system. The system then compares that photograph with the thousands or even millions of known faces already in the system, as it searches for a counterpart. It is akin to computerized searching for identical fingerprints. Precisely how the computer does this is something well beyond our ken. There is no suggestion, however, that these computerized identification methodologies are not now perfectly reliable investigative tools.
>
> Reliability does not matter, however, because the computerized identification is not ultimately evidence in court. It is simply a guide to put the investigator on the right track. The only evidentiary identification that mattered was the one-on-one identification made in the courtroom between the face on the fake North Carolina driver's license and the face on the appellant's known Maryland driver's license . . . . How Detective Kelly found his way to the appellant's Maryland driver's license, therefore, was immaterial. That license spoke for itself.
>
> Detective Kelly himself did not testify in any way about facial profiling technology . . . . If Judge Bragunier was influenced by repeated references to such technology, it was defense counsel who did the referencing. The State never mentioned the subject.[127]

The holding in *Geiger* is that "[r]eliability does not matter."[128] The use of FRT did not trigger any further inquiries because the State did not move to introduce testimony regarding FRT through an expert witness. This is a total endorsement of witness-washing's core logic: a machine process is irrelevant if a human witness confirms its results.

This reasoning also appears in the only other cases that address witness-washed FRT. In *Lynch*, the court denied the defendant's motion regarding the prosecution's failure to disclose the exculpatory evidence of other individuals who appeared in the FRT search results.[129] The denial was in part because "the jury convicted only after comparing the photo the

126. *See* 174 A.3d 954 (Md. Ct. Spec. App. 2017).
127. *Id.* at 965.
128. *Id.*
129. Lynch v. State, 260 So. 3d 1166, 1169–70 (Fla. Dist. Ct. App. 2018).

officers took to Lynch himself and to confirmed photos of Lynch."[130] And in *State v. Arteaga*,[131] the court held that "[t]he reason why a particular individual is a suspect and consequently included in the array is not relevant" to the question of whether a witness identification process was unduly suggestive.[132] Because the only evidence that the prosecution sought to introduce was witness testimony regarding the result of the lineup, the court looked only to the witness and ignored the underlying technology.

Consider the principles of the traditional scientific narrative entering the courtroom, discussed above in Part I. In this view, courts should inquire into the scientific validity and accuracy of a technology and decide whether its use implicates any protected rights. But the holding in *Geiger* is not that the mixed human-machine process is scientifically valid or accurate, or that it does not violate the right to privacy, or that it is not suggestive, or that it produces no exculpatory evidence. It is a holding that these questions *will not be asked*.

C. The Flawed Reasoning of Witness-Washing FRT

The core reasoning that courts use to endorse witness-washing is that the use of technology is only relevant to litigation if a party moves to introduce the results of that use to a factfinder. In the first sentence of his treatise on evidence, John Henry Wigmore divides the litigation process into five stages, and places evidence at the third stage: "the attempt at demonstration by the parties of their respective positions at *trial*."[133] If an action by a party isn't being introduced to prove a fact at trial, then it simply is not evidence. Because it is not evidence, it is not subject to scrutiny by the court. Many investigative tools used by the police evade scrutiny in this way.

Consider law enforcement's use of psychics. Despite psychics' universally acknowledged lack of effectiveness, police departments have occasionally turned to psychics for help in solving crimes. In 2001, for example, a police DNA analyst, lacking further leads, "transported the mattress pad [that was evidence in a murder investigation] in a paper bag by car to Orlando to have a psychic conduct an inspection."[134] The Research and Analysis Section of California's Department of Justice produced a document titled *Use of Psychics in Law Enforcement*, which advises law enforcement officers on how to select and work with psychic investigators. It including the note that "[just because] a person['s]…psychic ability is demonstrated in laboratory conditions does not necessarily mean that the same person would perform well in a criminal case."[135] Prosecutors have

130. *Id.* at 1170.
131. 296 A.3d 542 (N.J. Super. Ct. App. Div. 2023).
132. *Id.* at 556–57.
133. 1 WIGMORE, *supra* note 33, § 1, at 2.
134. *See* Overton v. State, 976 So. 2d 536, 551 (Fla. 2007).
135. CENT. INTEL. AGENCY, CIA-RDP96-00788R000100280009-3, USE OF PSYCHICS IN LAW ENFORCEMENT (2000).

turned to psychics to help pick juries,[136] police have used them to try to find dead bodies,[137] and detectives have asked them to describe the faces of people in their visions so the detectives could use sketches of those people in eyewitness identification procedures.[138] In reporting on the use of psychic detectives, the *New York Times* wrote: "[S]everal New York detectives said that when they are immersed in an emotionally wrenching case with no leads to follow, they find themselves thinking: What else is there to lose? 'It's just another investigative tool, and if it helps you, why not use it?'"[139] The default rule for law enforcement is that they can do anything that does not infringe on an individual's rights. The first time any law enforcement action will be subject to further evaluation is the point when it is moved into evidence.[140]

The doctrinal landscape also reflects this basic assumption. Defendants cannot force the prosecution to call certain witnesses or present evidence in a certain way; parties have essentially unlimited discretion to present a case in the way that they please. Criminal defendants do not even have a due process right to force the prosecution to test scientific evidence in the State's possession.[141] Certain disclosure requirements are triggered only by an intent to introduce an item at trial.[142] And well-funded criminal defendants can consult with expert witnesses but decide against presenting them or disclosing their conclusions. There is a vast category of evidence that a party considers prior to litigation but does not present to or have evaluated by courts.

The flaw in this reasoning when applied to FRT is that the technology fundamentally changes the nature of other evidence that is presented to the courts. Specifically, FRT introduces a confounding variable into the eyewitness identification process—a hidden variable that prevents correlation from indicating causation. The classic example of a confounding variable is the correlation between ice cream sales and murder. The two are strongly correlated: a study examining only ice cream and murder would show that when ice cream sales go up, then murders increase, and when

136. State v. Myers, No. 2000-CA-35, 2001 WL 929934, at *23 (Ohio Ct. App. Aug. 17, 2001) ("Exhibit M was an article written by Lynn Hulsey of the Dayton Daily News entitled 'Psychic helped pick Myers jury: assisted Greene Prosecutors.'").

137. State v. Edwards, No. E–01–010, 2003 WL 22828167, at *4 (Ohio Ct. App. Nov. 26, 2003) ("[Police Detective] Muehling further testified that in 1994, prompted by information from a psychic, he and others conducted a search for Robertson's body at a pig farm in Huron Township.").

138. People v. Memro, 700 P.2d 446, 451–52 (Cal. 1985), *overruled by* People v. Gaines, 205 P.3d 1074 (Cal. 2009) ("Sims contacted one Joan Julian, a psychic. Julian helped a police artist prepare a sketch of a person whom she visualized as having been with Carl Jr. at the time of his disappearance. On Friday, October 27, 1978, Detective Sims went to the missing boy's parents' house and showed them the sketch.").

139. Dan Barry, *When Technology Fails, Detectives Call on a New Jersey Woman's 'Visions*,*'* N.Y. TIMES (July 21, 1997), https://www.nytimes.com/1997/07/21/nyregion/when-technology-fails-detectives-call-on-a-new-jersey-woman-s-visions.html.

140. *See* discussion *infra* Section IV.A.

141. Dist. Att'y's Off. v. Osborne, 557 U.S. 52, 52 (2009).

142. *See, e.g.*, FED. R. CRIM. P. 16(a)(1)(E) (requiring disclosure of items in federal criminal cases if the prosecution intends to use an item as part of its case-in-chief).

ice cream sales are down murders correspondingly decrease. The actual, unexamined cause of the correlation—the confounding variable—is the temperature. When it is hot outside, people are more likely to both eat ice cream and kill each other.[143]

For FRT, the confounding variable arrives in the eyewitness identification procedure. An eyewitness identification procedure is essentially an experiment. A witness is asked whether they have seen a certain person before. If they say yes, the best explanation is that they have in fact seen the person. But FRT adds an alternative explanation: they may be saying yes because the person in the photograph bears such a strong resemblance to a person that they have seen before that they are unable to distinguish between the person they have seen and the similar-looking person in the image in front of them. "The association between two variables may be driven by a lurking variable that has been omitted from the analysis."[144] Before FRT, this was less of a problem—the odds of law enforcement presenting an image of an unrelated stranger who happened to bear a strong resemblance to the actual perpetrator were extremely low. After FRT, the odds of law enforcement presenting an image of a suspect who coincidentally resembles the actual perpetrator are astronomically higher. The creation of a list of similar-looking people is precisely what FRT is designed to do.

The core logic of witness-washing is that an investigative tool only matters to a court if a party chooses to introduce it through a witness. This logic has been rendered obsolete by algorithmic tools. Even if the identifying witness is confronted in court, that witness may not know that FRT was used to create the lineup from which they made an identification. Powerful algorithmic tools are now in the background of litigation, and many of them function by distributing a decision-making process across a person and a machine. In the case of FRT, calling the witness without mentioning the machine fundamentally misrepresents what has happened. Distributed decision-making has introduced a confounding variable. Presenting those distributed decisions as if they were solely human decisions—witness-washing them—hides the confounding variables.

D. Witness-Washing in Other Contexts

Other law enforcement technologies distribute decision-making across an algorithm and a person, and are therefore subject to witness-washing. Three common examples are place-based predictive algorithms, ShotSpotter, and person-based predictive algorithms.

143. *See* Andrew W. Lehren & Al Baker, *In New York, Number of Killings Rises with Heat*, N.Y. TIMES (June 18, 2009), https://www.nytimes.com/2009/06/19/nyregion/19murder.html.

144. David H. Kaye & David A. Freedman, *Reference Guide on Statistics*, *in* REFERENCE MANUAL ON SCIENTIFIC EVIDENCE 211, 262 (The Nat'l Acads. Press ed., 3d ed. 2011).

Place-based predictive policing algorithms are tools that create "hot spots" that are predicted to be sites of crime in the future.[145] Many law enforcement agencies use these algorithms to direct police patrols to certain blocks.[146] Because they incorporate a wide array of factors that are influenced by race, these algorithms disproportionately direct law enforcement to race–class subjugated neighborhoods.[147] In the court system, the presence of the algorithm in the background is witness-washed as police discretion: there is no requirement for any police officer to explain why they were in a certain area when writing a ticket or making an arrest. Residents are never told why there is an increased police presence in their neighborhood.

ShotSpotter is an algorithmic technology consisting of a series of high-sensitivity microphones placed in communities and an algorithm that purports to monitor those microphones and detect only gunshots so law enforcement can respond to gunshots more quickly.[148] ShotSpotter's accuracy and efficacy as a law enforcement tool has never been proven,[149] but police in cities such as New York City, Detroit, and Los Angeles have installed extensive networks of ShotSpotter microphones.[150] These microphones are also almost universally placed in race–class subjugated communities.[151] When the algorithm identifies a loud noise as a gunshot, it attempts to triangulate the location of the noise, and police respond to that location. These responses are frequently recorded in police reports as generic instances of responding to gunshots in the area.[152] The potential problems with the technology are not surfaced because its use is hidden behind a witness-washed report by police.

Person-based predictive policing algorithms are algorithmic tools that create "heat lists" of individuals who police and prosecutors target for more aggressive enforcement.[153] These algorithms purport to identify the

145. Will Douglas Heaven, *Predictive Policing Algorithms are Racist. They Need to be Dismantled*, MIT TECH. REV. (July 17, 2020), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/.

146. *Id.* ("The tools identify hot spots, and the police plan patrols around [them].").

147. Sandra G. Mayson, *Bias in, Bias Out*, 128 YALE L.J. 2218, 2218 (2019) ("In a racially stratified world, any method of prediction will project the inequalities of the past into the future."). *See generally* Aziz Z. Huq, *Racial Equity in Algorithmic Criminal Justice*, 68 DUKE L.J. 1043, 1043 (2019) (describing racial disparities reproduced by algorithmic tools).

148. Elizabeth E. Joh, *The Unexpected Consequences of Automation in Policing*, 75 SMU L. REV. 507, 516 (2022) (describing ShotSpotter).

149. BRAD LANDER, N.Y.C. COMPTROLLER, FP23-074A, AUDIT REPORT ON THE NEW YORK CITY POLICE DEPARTMENT'S OVERSIGHT OF ITS AGREEMENT WITH SHOTSPOTTER INC. FOR THE GUNSHOT DETECTION AND LOCATION SYSTEM 1 (2024) ("During the sampled months of review in 2022 and 2023, ShotSpotter alerts only resulted in confirmed shootings between 8% and 20% of the time.").

150. Dhruv Mehrotra & Joey Scott, *Here Are the Secret Locations of ShotSpotter Gunfire Sensors*, WIRED (Feb. 22, 2024, 8:18 PM), https://www.wired.com/story/shotspotter-secret-sensor-locations-leak/.

151. Joh, *supra* note 148, at 518.

152. *Id.* at 522–23.

153. FERGUSON, *supra* note 1, at 2–3 (reviewing the use and effectiveness of various predictive policing programs).

individuals who are more likely to commit crimes.[154] The idea behind them is that people who are more likely to commit crimes in the future should be removed from their communities by more aggressive policing and prosecution, as this removal will reduce the crime rate. These aggressive prosecution decisions are witness-washed[155] as prosecutorial discretion, which requires no justification or explanation. Perhaps unsurprisingly, they are racially disproportionate. "Any form of risk assessment that relies on criminal history will have a disparate impact on [B]lack communities, and on [B]lack men in particular."[156] Every day, thousands of people are living their lives on algorithmically created lists of undesirables, without ever being informed of why they are being targeted in this way by the government.

Each of these instances of witness-washing raises different kinds of concerns. FRT raises accuracy concerns through an unexamined confounding variable, while predictive algorithms do not. Place-based algorithms are problematic not because of their accuracy or lack of accuracy, but because they may exacerbate historical dynamics between police and marginalized communities. ShotSpotter is effectively a surveillance tool.[157] What they have in common is that they are all instances of powerful algorithms making law enforcement decisions. The algorithm decides who may be guilty, who should be aggressively policed and prosecuted, and where police officers should focus their attention. Each of these algorithmic processes is hidden from the courts—and the public—because the people who do what the algorithm tells them to will testify as if the algorithm did not exist. This prevents a meaningful analysis of and engagement with the underlying complexity of these algorithmic processes.

III. THE UNDERLYING COMPLEXITY OF FRT

As a result of witness-washing, this immense complexity goes unexamined. The FRT technician in *Lynch* articulated their understanding of the technology with the testimony: "[J]ust hit search and it gives you a photo."[158] This Part excavates the history, functioning, and pitfalls of the technology.

FRT is a biometric identification tool.[159] Biometric identification is the identification of a person through information about their body. It is an attempt to shift identity from the things we carry, such as driver's licenses,

154. *Id.* at 35 ("This is the promise of big data policing. What if big data techniques could predict who might be violent?").

155. Prosecutors aren't witnesses, so the term is somewhat inaccurate here. "Human-washed" covers more cases but is truly awkward.

156. Mayson, *supra* note 147, at 2229–30.

157. Vincent M. Southerland, *The Master's Tools and a Mission: Using Community Control and Oversight Laws to Resist and Abolish Police Surveillance Technologies*, 70 UCLA L. REV. 2, 20–21 (2023) (discussing audible gunshot detection systems as means of police surveillance).

158. Lynch v. State, 260 So. 3d 1166, 1169 (Fla. Dist. Ct. App. 2018).

159. U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-267, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY 7 (2016) ("[B]iometrics, such as face recognition technology.").

to the things we are, such as a person with a certain set of ridges on our fingers. Other examples include iris patterns and DNA.[160] Biometric identification promises to increase the speed and accuracy with which individuals can be identified, both in real time and in the past. For law enforcement, this is discussed in terms of an increased ability to respond to ongoing crises by identifying people in the present, and to solve crimes by determining the identity of someone in the past.[161] Uncooperative people may decide not to provide their names, but their faces may be visible. People rarely leave their driver's license at crime scenes, but they do leave DNA. In the future, police may be able to quickly and easily identify anyone through the use of biometric identification tools such as FRT.[162]

A. A Brief History of Biometric Identification

In order to understand the role of FRT in modern law enforcement, it is necessary to understand where it comes from.[163] Biometric identification originated in the late nineteenth century in France and England.[164] It promised to solve a problem that was comparatively new for law enforcement. Historically, the law had been mostly concerned with small and integrated communities, in which identity was a matter of general knowledge. Within a close-knit community, concerns about misidentification were minimal because people simply recognized each other by sight. The oldest statutes dealt with the potential of strangers committing crimes by simply requiring a night watchman to detain any stranger that they encountered.[165] In 1769, William Blackstone divided strangers whose origins and destinations were unknown to a community into three categories: "[I]dle and disorderly persons, rogues and vagabonds, and incorrigible rogues."[166] They were all subject to arrest under criminal laws outlawing vagabonds and idleness, which carried sentences of hard labor.[167] Anyone sheltering such a person

160. *Id.* at 5 ("Technologies have been developed to identify people using biometrics, such as their faces, fingerprints, eye retinas and gait, among other things.").

161. L.A. CNTY. REG'L IDENTIFICATION SYS., FACIAL RECOGNITION POLICY (2023) ("FR technology can be a valuable tool to create investigative leads, reduce an imminent threat to health or safety, and help in the identification of deceased persons or persons unable to identify themselves."); N.Y.C. POLICE DEP'T, FACIAL RECOGNITION: IMPACT AND USE POLICY 4 (2023) ("Since 2011, the NYPD has successfully used facial recognition technology to investigate criminal activity" and "aid in the identification of persons unable to identify themselves.").

162. The right to be let alone is less present in the law enforcement dialogue. *See* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("The makers of our Constitution . . . . conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men.").

163. *See* Oliver Wendell Holmes, *The Path of the Law*, 10 HARV. L. REV. 457, 469 (1897) ("The rational study of law is still to a large extent the study of history.").

164. Anil K. Jain, Debayan Deb, & Joshua J. Engelsma, *Biometrics: Trust, but Verify*, 4 IEEE TRANSACTIONS ON BIOMETRICS, BEHAV., & IDENTITY SCI. 303, 303 (2022) ("The origin of modern day biometric recognition has its roots in the 'Habitual Criminals Act' passed by the British Parliament in 1869.").

165. The Statute of Winchester 1285, 13 Edw., ¶4 ("And if any stranger do pass by them he shall be arrested until morning; and if no suspicion be found he go quit[.]").

166. 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 97 (Lonang Inst. 2003) (1769).

167. *Id.*

for more than two nights became liable for any crimes that they might commit within the community.[168] Remaining doubts about the identity of the perpetrator of a crime were addressed by a strong law of proof.[169] Conviction required the sworn testimony of two witnesses who had directly witnessed the crime, or a confession by the criminal—typically obtained through torture.[170]

As populations grew and mobilized, communities increasingly encountered the problem of anonymity.[171] Identifying particular strangers who committed crimes became a problem, as did keeping track of what we would now call a criminal record. People convicted of crimes had historically been marked by the knowledge of their communities, but the rise of mobility allowed them to simply move to another place and take another name. The oldest way of preventing this was a crude form of biometrics: the creation of marks on people's bodies, through either branding or mutilation. Cutting off someone's ear did not convey the exact identity of a person, but it did convey the information that courts were most concerned with: whether the person had previously been convicted of a crime.[172] Branding and mutilation generally fell out of favor in Europe and America in the early nineteenth century, leaving the more complicated problem of actual identity.[173]

The first systematic attempt to identify strangers who did not want to be identified is typically attributed to Alphonse Bertillon, a French police officer who developed a system of biometric identification in the late 1870s. At the time, the French penal system imposed harsher punishments on people with previous convictions, but people who qualified for these harsher punishments frequently evaded detection by changing their identities. In Bertillon's view, the problem was that, among criminals, "a somewhat intelligent individual changes his name like his shirt . . . ."[174] Bertillon's system involved taking precise measurements of various body parts of an offender, along with the progenitor of the modern mug shot—photographs of suspects' faces from standardized distances and angles.[175] The measurements and photographs were recorded on index cards, and the measurements were manually compared to individuals as they were

168. *Id.*

169. Langbein, *supra* note 32, at 4.

170. *Id.* ("Thus, for example, it would not have mattered in this system that the suspect was seen running away from the murdered man's house and that the bloody dagger and the stolen loot were found in his possession. Since no eyewitness saw him actually plunge the weapon into the victim, the court could not convict him of the crime.").

171. *See* LAWRENCE M. FRIEDMAN, CRIME AND PUNISHMENT IN AMERICAN HISTORY 12–14 (1993) ("[T]he pathologies of a mobile society [arising in the nineteenth century] demanded new techniques of control.").

172. *Id.* at 40 ("Dozens of detached ears, in fact, litter the record books.").

173. *See id.* at 63.

174. ALPHONSE BERTILLON, UNE APPLICATION PRATIQUE DE L'ANTHROPOMÉTRIE 3 (G. Masson & Co. eds., 1881).

175. Gray, *supra* note 102, at 10.

arrested.[176] Bertillonage, as it was called, was widely adopted but proved to be inaccurate and inefficient.[177]

Fingerprinting arose as the next solution to strangers, and remains the most common form of biometric identification used by law enforcement.[178] Fingerprinting originated in 1892, when the British polymath Francis Galton published a manuscript on the comparison of fingerprints.[179] He claimed that individuals could be identified beyond doubt by the particular marks on the papillary ridges of their fingers.[180] He identified two primary uses for his system of identification:

> [I]n civilised lands and in peaceable times, the chief use of a sure means of identification is to benefit society by detecting rogues, rather than to establish the identity of men who are honest . . . . In India and in many of our Colonies the absence of satisfactory means for identifying persons of other races is seriously felt. The natives are mostly unable to sign; their features are not readily distinguished by Europeans; and in too many cases they are characterized by a strange amount of litigiousness, wiliness, and unveracity.[181]

Neither Bertillon nor Galton conceived of their systems primarily as means of determining the identity of someone who had committed a crime. The originators of biometric identification were instead seeking two things: first, the ability to confirm whether a person was the person they said they were, and second, some way to differentiate what type of person a person was, in terms of race, class, or criminal disposition.[182] The project was not limited to individual identity—it also included group identity and the promoted theories of eugenics.

These concepts are still present in the language used to describe FRT: it is billed as a tool that helps law enforcement "find the bad guys" or "know who we're dealing with." The ultimate aim of biometric identification was to have an identifying mark for a certain type of unknown person, who was seen as a potential source of danger.[183] For Bertillon and Galton, this included not only individuals who had in fact committed crimes, but also groups of people who they believed were more likely to.

FRT is the pinnacle of biometric identification's original promise: "In one word, to fix the human personality, to give to each human being an

176. *Id.*
177. *Id.* at 11.
178. *Id.*
179. *See generally* FRANCIS GALTON, FINGER PRINTS (Macmillan & Co. 1892).
180. *Id.* at 1–2, 11.
181. *Id.* at 149.
182. *Id.* at 192–93 ("Chapter 12, Races and Classes").
183. This dichotomy between dangerous, unknown people and safe, known people is replicated in many sources, but largely inaccurate. Most murders, for example, are committed by known parties. ERIKA HARRELL, BUREAU OF JUST. STATS., NCJ 239424, VIOLENT VICTIMIZATION COMMITTED BY STRANGERS, 1993–2010, at 1 (2012). It does, however, help to explain much of the pushback against FRT by people who are surprised and angered to learn that they are in FRT databases.

identity, an individuality that can be depended upon with certainty, lasting, unchangeable, always recognisable and easily adduced . . . ."[184]

B. How FRT Works

FRT, as it is deployed today, is a mixed human–machine process consisting of (1) a human input, (2) an algorithmic comparison, and (3) an integrated output. The first step is for a user or a prior algorithm to select a digital image—called a probe image—to submit to the algorithm.[185] The algorithm then isolates faces in the image and reduces each face into a dataset known as a "faceprint," by analogy to fingerprints.[186] The second step is for the algorithm to compare that faceprint to a database of digital images that have been identified as other images of faces.[187] Finally, the algorithm produces results in a format—typically as a list of potential matches, or a binary determination of whether a sufficiently similar faceprint is present in the database being searched.

For a user, this entire process is likely to feel intuitive because the programs are sold by vendors who have a financial interest in their program's ease of use. This structure is intuitive because it is common in other contexts. Searches of the internet, for example, involve the same sort of three-step process. The human input is the set of words describing what the user is looking for. A search algorithm processes the input according to a bewildering array of factors, which incorporate both accuracy and the financial interests of various actors.[188] Then, a user makes a selection from a set of results. FRT has the same basic pattern-matching search structure, but with an image of a face as the input. The law enforcement technician whose use of FRT resulted in Willie Lynch's conviction explained her intuitive understanding of the process:

> I took the image [of the suspect], uploaded into the computer program. There are certain selections. You can let it be an open ended search. In this case I know the race and I know the gender, this case being a [B]lack male, and I also wanted to only consider Duval County booking photos . . . So those selections were chosen in this case with a

184. GALTON, *supra* note 179, at 169 (quoting with approval remarks by M. Herbette).

185. GARVIE, FORENSIC WITHOUT THE SCIENCE, *supra* note 11, at 9–11.

186. *Id.* at 4 ("A 'latent face' is left behind in a photograph or on video footage, collected and then compared against a database of 'face prints' on file to determine whether there is a possible match.").

187. *Id.*; *see, e.g.*, ERIN M. PREST, FED. BUREAU OF INVESTIGATION, PRIVACY IMPACT ASSESSMENT FOR THE NEXT GENERATION IDENTIFICATION-INTERSTATE PHOTO SYSTEM 1 (2019) (stating that in 2019 the FBI had a target database of "over 38 million criminal photos [that] are available for facial recognition searching by law enforcement agencies"); *Revolutionary Facial Recognition Platform*, CLEARVIEW AI, https://app.hubspot.com/documents/6595819/view/454213073?accessId=c85a92 (last visited July 28, 2024) (advertising a "50+ billion facial image database").

188. *See, e.g.*, Charles Duhigg, *The Case Against Google*, N.Y. TIMES MAG. (Feb. 20, 2018), https://www.nytimes.com/2018/02/20/magazine/the-case-against-google.html (detailing ongoing changes to Google's search algorithm that reduced competition).

> photo and *then just hit search and it gives you a photo*—(unintelligible)—almost like a photo line-up.[189]

Many law enforcement agencies that use FRT do not have written policies or trainings regarding the use of the technology, but simply assume that the programs are accurate, self-explanatory, and work as intended. For example, when the GAO inquired into federal agencies' use of FRT, it found that seven agencies were regularly using FRT but none of them required training on the use of facial recognition until April 2023.[190] FRT vendors reinforce this misconception by emphasizing the user-friendly nature of their technology, promising quick and ready-to-use installations.[191]

Despite these appearances, each step of the FRT process is, in fact, immensely complicated. There is a substantial literature on the complexity of FRT,[192] but very little of it is directed towards use in the criminal legal system. This Article does not aim to give a full descriptive account of the technology, but to give a sense of the immense complexity lurking beneath the brief descriptions that are most often offered by courts and law enforcement using FRT.

The primary complexity at the input stage is whether the probe image is obtained through cooperative or non-cooperative capture.[193] Digital images are two-dimensional fields of pixels, faces are three-dimensional objects. Computer scientists refer to this problem as the "curse of dimensionality."[194] An algorithm must make determinations about three-dimensional relationships based on the color, shading, and relationship of two-dimensional pixels. In cooperative capture scenarios, such as mug shots, this problem is minimal. Images are taken from the same angle, distance, and lighting conditions as every other face involved in the process.

But law enforcement use of FRT in the field is a non-cooperative capture scenario because people are not intentionally presenting themselves for identification. Slight alterations in pose constantly create "self-occlusions," where a part of a face that is needed for measurement is blocked by another part of the face. Faces may be smaller or larger due to

189. Lynch v. State, 260 So. 3d 1166, 1169 (Fla. Dist. Ct. App. 2018) (emphasis added).

190. GAO, FACIAL RECOGNITION SERVICES, *supra* note 123, at ii ("All seven agencies initially used these services without requiring staff take facial recognition training.").

191. *Face Recognition Technology for Image and Video Investigations, and Database Matching*, COGNITEC SYS., www.cognitec.com/files/tao/downloads/FaceVACS-DBScan-LE-1-4-flyer.pdf (last visited July 28, 2024).

192. *See, e.g.*, HANDBOOK OF FACE RECOGNITION (Stan Z. Li & Anil K. Jain eds., Springer-Verlag London Ltd. 2d ed. 2011); THE CAMBRIDGE HANDBOOK OF FACIAL RECOGNITION IN THE MODERN STATE (Rita Matulionyte & Monika Zalnieriute eds., Cambridge Univ. Press 2024) [hereinafter THE CAMBRIDGE HANDBOOK]; NAT'L ACADS. OF SCIS., ENG'G, & MED., FACIAL RECOGNITION TECHNOLOGY: CURRENT CAPABILITIES, FUTURE PROSPECTS, AND GOVERNANCE (2024) [hereinafter FACIAL RECOGNITION TECHNOLOGY]; GARVIE, FORENSIC WITHOUT THE SCIENCE, *supra* note 11.

193. *See* FACIAL RECOGNITION TECHNOLOGY, *supra* note 192, at 1; GARVIE, FORENSIC WITHOUT THE SCIENCE, *supra* note 11, at 9–11.

194. HANDBOOK OF FACE RECOGNITION, *supra* note 192, at 20 (discussing the computational difficulties created by "the so-called curse of dimensionality").

distance, or occluded due to the angles involved. Lighting conditions are unpredictable—especially outdoors. Shaded pixels that might indicate cheeks in a mug shot, for example, could be absent in an image of a person looking towards the sun, and the passage of clouds can darken pixels in ambiguous ways.

Inputs also raise the problem of image quality. Closed-circuit television (CCTV) is nearly universal, but the quality of images from surveillance is generally lower than that of images taken for identification purposes, such as mug shots or driver's license photos.[195] Images captured from low-quality video have fewer pixels and therefore provide less information. When FRT attempts to compare low quality images, the accuracy of the algorithm can drop precipitously.[196]

To address the problems of quality, distance, and angle, most FRT programs include tools that allow users to modify probe images before using them in a search. Detectives can "[use a] blur tool to add pixels into a low-quality image; [cut and paste] new features into the subject photograph; [combine] photographs of two different people to generate a single image; and [use] 3D modeling to recreate an approximation of facial features not visible in the original image."[197] FRT algorithms are generally trained on images of people with their eyes open, for example, so law enforcement will occasionally Google open eyes and paste a pair into a probe image of a suspect with closed eyes.[198]

In addition to tools that modify images before submission, law enforcement has also used probe images that were not gathered in relation to the case. NYPD detectives investigating a shoplifting case recovered a video that showed a suspect but was too low-quality to be used with FRT.[199] The detectives noted that the person in the video looked like the actor Woody Harrelson, however, so they decided to use a high-quality image of Woody Harrelson from the internet as an input. This search resulted in an arrest in the case.[200]

The second step in the FRT process—the algorithmic comparison itself—is immensely complicated because modern FRT is a product of machine learning. Originally, FRT was very similar to Bertillon's system of measuring bodies. The goal was to extract a multitude of specific facial

195. FACIAL RECOGNITION TECHNOLOGY, *supra* note 192, at 1 ("Non-cooperative capture, in which subjects may not even realize that their image is being captured, such as images taken from security cameras, generally results in lower-quality images.").

196. Philipp Terhörst, Marco Huber, Naser Damer, Florian Kirchbuchner, Kiran Raja, & Arjan Kuijper, *Pixel-Level Face Image Quality Assessment for Explainable Face Recognition*, 5 IEEE TRANSACTIONS ON BIOMETRICS, BEHAV., & IDENTITY SCI. 288, 288 (2023) ("Consequently, the performance of FR systems is strongly dependent on the quality of their samples.").

197. GARVIE, FORENSIC WITHOUT THE SCIENCE, *supra* note 11, at 11.

198. CLARE GARVIE, GEORGETOWN L. CTR. ON PRIV. & TECH., GARBAGE IN, GARBAGE OUT: FACE RECOGNITION ON FLAWED DATA (2019).

199. *Id.*

200. Michael R. Sisak, *NYPD Used Woody Harrelson Photo to Find Lookalike Beer Thief*, AP NEWS (May 16, 2019, 8:25 PM), https://apnews.com/article/4ef0d4bf24764fe3b9b4311c576062b4.

measurements—such as the distance between the eyes and the precise fullness of lips—in the hope that adding up enough of these features would allow for identification.[201] "The idea was that, if you took enough measurements, every person was unique."[202] For early FRT tools, a person's faceprint consisted of these accumulated measurements.

Currently, however, FRT algorithms are typically deep convolutional neural networks created through machine learning.[203] These algorithms are modeled on human learning processes. The algorithm is designed to teach itself through an automated feedback loop of failure and improvement.[204] An algorithm essentially takes a guess at the correct result, is told if the result was correct or not, and then modifies itself in response along programmed lines of improvement.

This ongoing self-modification means that a human programmer does not write most of the code that makes up the algorithm, so it is no longer possible to precisely explain what the algorithm does or how it does it. The final algorithm is a black box, where the people who designed the initial program have "limited understanding of the learned model," and "predictions generated by the system are often not explainable as to why the system generated this output for that input."[205] The original concept of taking and comparing specific measurements of parts of faces no longer applies:[206] the convolutional neural networks that make up most FRT algorithms do not pay attention to the same kinds of features that people do.[207]

---

201. A. Jay Goldstein, Leon D. Harmon, & Ann B. Lesk, *Identification of Human Faces*, 59 PROCEEDINGS OF THE IEEE 748, 749 (1971).

202. Shaun Raviv, *The Secret History of Facial Recognition*, WIRED (Jan. 21, 2020, 6:00 AM), https://www.wired.com/story/secret-history-facial-recognition/; THE CAMBRIDGE HANDBOOK, *supra* note 192, at 48 ("In essence, Bledsoe had computerised the mug shot into a 'fully automated Bertillon system for the face.'"); *see also* Gray, *supra* note 102, at 12 ("Modern facial recognition technology leverages digital imaging, data storage, and computer analysis to fulfill Bertillon's vision of a reliable biometric method for confirming identity.").

203. *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II*: *Hearing Before the H. Comm. on Homeland Sec.*, 116th Cong. 24 (2020) (statement of Charles H. Romine, Dir., Info. Tech. Lab'y, Nat'l Inst. of Standards & Tech.) ("The findings . . . showed that massive gains in accuracy have been achieved since the FRVT in 2013 . . . [t]he accuracy gains observed in the 2018 FVRT study stem from the integration, or complete replacement, of older facial recognition techniques with those based on deep convolutional neural networks."); Jain, Deb, & Engelsma, *supra* note 164, at 313 ("[N]early all face recognition systems employ the use of 'black-box' deep networks for encoding and matching.").

204. THE CAMBRIDGE HANDBOOK, *supra* note 192, at 38–39.

205. Jonathan R. Williford, Brandon B. May, & Jeffrey Byrne, *Explainable Face Recognition*, *in* COMPUTER VISION—EECV 2020, at 248 (Andrea Vedaldi, Horst Bischof, Thomas Brox, & Jan-Michael Frahm eds., Springer 2020).

206. Bangjie Yin, Luan Tran, Haoxiang Li, Xiaohui Shen, & Xiaoming Liu, *Towards Interpretable Face Recognition*, *in* 2019 INTERNATIONAL CONFERENCE ON COMPUTER VISION 9347, 9348 (Conference Publishing Services 2019) ("In early days . . . most models use[d] hand-craft features . . . . Back then visual cues include[d] . . . body parts . . . .").

207. Williford, May, & Byrne, *supra* note 205, at 251 ("[P]airwise similarity between faces is heavily dominated by the periocular region and nose . . . ."); *see also id.* at 252 fig.2 (showing an attentional map paying intense attention to Barack Obama's right nostril).

The grist for this machine-learning mill consists of vast training databases of identified faces.[208] These training databases—with names such as Labeled Faces in the Wild and Megaface—are often packaged and sold to FRT developers.[209] The lighting levels, camera angles, and racial composition of the images in these training databases are integrated into the results of the machine learning process. FRT algorithms are never trained at the generalized task of recognizing faces, but always on the task of recognizing the specific faces within the database they were trained on.

After being purchased for use, the algorithm is no longer used with a training database but instead with a target database. A target database is the database of faces that the algorithm searches through.[210] The scope and contents of these databases are government secrets, but they are known to include DMV records of people who have never been suspected of criminal activity.[211] The Georgetown Privacy Center estimated that, as of 2016, half of Americans were in an FRT target database.[212] The acknowledged FBI database for FRT alone included 38 million mug shots as of 2019.[213] These numbers only grow over time.

In the final stage, the results of an FRT comparison are integrated into a human decision-making process. The most common law enforcement use of FRT is a process known as "1:many identification," in which an image of an unknown person—typically taken from a surveillance camera near a crime scene—is compared to a target database.[214] The output for this process consists of a list of the highest-ranked results, which can be used as leads for further investigation. This use of FRT is the primary focus of this Article because it is currently the most common law enforcement use of FRT. The pitfalls of this process are discussed in the next Section.

One alternative way of integrating the output of FRT is face surveillance, also known as a "many:many comparison."[215] With face surveillance, live video is constantly run through an FRT algorithm to offer potential identifications for many people in real time.[216] Law enforcement already deploys extensive camera surveillance networks and body-worn

208. Jason M. Schultz, *The Right of Publicity: A New Framework for Regulating Facial Recognition*, 88 BROOK. L. REV. 1039, 1040–43 (2023) ("Today's biometric identification systems are typically built through the massive appropriation of the visual likenesses of individuals.").

209. *See MegaFace Dataset*, MEGAFACE, https://megaface.cs.washington.edu/dataset/download.html (last visited July 28, 2024); *see also* Schultz, *supra* note 208, at 1043 (analyzing how these datasets are created).

210. THE CAMBRIDGE HANDBOOK, *supra* note 192, at 29.

211. CLARE GARVIE ET AL., GEORGETOWN L. CTR. ON PRIV. & TECH., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 2 (2016).

212. *Id.* at 1 ("One in two American adults is in a law enforcement face recognition network.").

213. PREST, *supra* note 187, at 1.

214. GARVIE, FORENSIC WITHOUT THE SCIENCE, *supra* note 11, at 3–4.

215. Ferguson, *supra* note 98, at 1116.

216. *Id.* at 1117 ("Another potential form of face surveillance technology is real-time public monitoring. The technology already exists (and is being used in countries like China) to watch the streets and identify people in public spaces using pattern-matching technology.").

cameras.[217] With face surveillance "[i]t is possible for [FRT] software to be integrated into police body worn cameras or city-wide surveillance camera networks, on a 24/7 basis, and for the resultant data to be subject to automated analysis."[218]

The London Metropolitan Police Department used FRT in this manner in several trials between 2016 and 2019.[219] The report on this experiment in face surveillance concluded that it was "highly possible" that the use of FRT for face surveillance "would be held unlawful" if a court reviewed it.[220] The Chinese government has moved beyond the trial stage of this technology and has been using FRT to surveil Uyghurs for years: "The facial recognition technology, which is integrated into China's rapidly expanding networks of surveillance cameras, looks exclusively for Uighurs based on their appearance and keeps records of their comings and goings for search and review."[221]

Generally, FRT consists of the input of a digital image of a face through a user-friendly interface, a search that is bewilderingly complex in its particulars, and an output that is integrated thoughtlessly into an existing decision-making process.

C. How FRT Does Not Work

The algorithmic element of FRT identification works incredibly well under ideal conditions of high-quality images and uniform lighting and pose. The National Institute of Standards and Technology (NIST)—an agency of the U.S. Department of Commerce—engages in ongoing tests of facial recognition algorithms as they are developed and improved. In NIST's initial series of tests, the accuracy rates were comparatively low.[222] Under ideal conditions, as of July 2024, many commercially available algorithms are 99.9% accurate in listing the correct individual at rank one within a database of 12 million photographs.[223] In these perfect testing

217. *Law Enforcement Management and Administrative Statistics (LEMAS)*, BUREAU OF JUST. STAT., https://bjs.ojp.gov/data-collection/law-enforcement-management-and-administrative-statistics-lemas (last visited July 28, 2024).

218. PETE FUSSEY & DARAGH MURRAY, THE HUM. RTS., BIG DATA & TECH. PROJECT, INDEPENDENT REPORT ON THE LONDON METROPOLITAN POLICE SERVICE'S TRIAL OF LIVE FACIAL RECOGNITION TECHNOLOGY 20 (2019).

219. *Id.* at 5.

220. *Id.* at 15.

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

222. PATRICK J. GROTHER, GEORGE W. QUINN, & P. JONATHON PHILLIPS, NAT'L INST. OF STANDARDS & TECH., NISTIR 7709, REPORT ON THE EVALUATION OF 2D STILL-IMAGE FACE RECOGNITION ALGORITHMS 2 (2010) (listing a rank 1 accuracy rate of 92% with the most accurate algorithm under ideal conditions in a 1.6 million individual dataset).

223. PATRICK GROTHER, MEI NGAN, & KAYEE HANAOKA, NAT'L INST. OF STANDARDS & TECH., NISTIR 8271, FACE RECOGNITION VENDOR TEST (FRVT) PART 2: IDENTIFICATION 2 (2019) (listing a rank 1 accuracy rate of 99.9% for most algorithms under ideal conditions in a 12 million individual dataset).

conditions, FRT has developed to a point where the best algorithms work almost flawlessly.

Perfect testing conditions are not the conditions encountered in actual police work, however.[224] Law enforcement acknowledges this by treating FRT results merely as leads. No prosecutor has ever attempted to introduce an FRT identification into evidence.[225] Law enforcement agencies do not endorse FRT identification as a sufficient basis for probable cause to arrest a suspect.[226] Even NIST, which publishes the research results showing high accuracy rates, characterizes the highest-ranked match from FRT identification merely as a lead requiring investigative follow-up.[227] There are at least six aspects of FRT use that lower accuracy in the field and result in the universal agreement that FRT alone is insufficient for legal determinations.

The first source of error is inaccuracy introduced through probe image manipulation, in which law enforcement officers alter images prior to submission.[228] This categorically prevents the result from being truly accurate. No algorithm can accurately identify a person with a chin copied from the internet because no such person exists. These modifications also interact with the algorithms in unforeseeable ways. Many algorithms "pay attention" to nostrils and areas near the eyes in ways that are counterintuitive for a person, for example, and what may seem like a minor edit to a human has the potential to entirely disrupt the FRT process.[229]

A second source of error is the wide variance in algorithmic accuracy. "Recognition accuracy is very strongly dependent on the algorithm."[230] FRT is often discussed as a monolith, but it consists of a highly diverse landscape of commercially developed algorithmic tools. Law enforcement agencies rarely have requirements regarding the acquisition and use of FRT, so it is unclear how thoroughly the individual algorithms are being evaluated. The crime analyst who runs the Detroit Police Department's FRT searches, for example, testified that he has "no idea" what algorithm his department uses.[231] Additionally, some FRT developers charge users

224. *See supra* Section II.D.

225. GARVIE, FORENSIC WITHOUT THE SCIENCE, *supra* note 11, at 43.

226. *Id.* at 43–44.

227. PATRICK GROTHER, MEI NGAN, & KAYEE HANAOKA, NAT'L INST. OF STANDARDS & TECH., NISTIR 8271 DRAFT SUPPLEMENT, FACE RECOGNITION TECHNOLOGY EVALUATION (FRTE) PART 2: IDENTIFICATION 16 (2024) [hereinafter FRTE] (listing "no claim" of identification for investigative purposes).

228. GARVIE, FORENSIC WITHOUT THE SCIENCE, *supra* note 11, at 11, 22.

229. Williford, May, & Byrne, *supra* note 205, at 251 (showing how FRT algorithms focus on counterintuitive details).

230. FRTE, *supra* note 227, at 9.

231. Brief of Amici Curiae American Civil Liberties Union & American Civil Liberties Union of Massachusetts, Inc. et al. in Support of Appellee and Affirmance at 26 n.12, Commonwealth v. Arrington, 226 N.E.3d 851 (Mass. 2024) (SJC-13499) ("*See, e.g.*, Dep. Tr. of Nathan Howell at 24:19–20, Williams v. City of Detroit, No. 2:21-cv-10827 (E.D. Mich. June 16, 2023), ECF No. 50-4 (Detroit Police Department crime analyst who runs FRT searches testifying that he has 'no idea' what algorithm the Department uses for such searches); Dep. Tr. of Krystal Howard at 39:16–21, Williams v.

for updated versions of their software, which means that law enforcement agencies may be using older versions that do not incorporate recent improvements in accuracy.[232]

A third source of error is racial bias, which is primarily a result of training database pitfalls.[233] Developers frequently train their algorithms on databases in which white men are overrepresented, and as a result, these algorithms are more likely to misidentify people of color and women.[234] An algorithm that is accurate for some groups of people may perform poorly when used in an attempt to identify a different group of people. This racialized inaccuracy continues to occur in a criminal legal system which has a long history of criminalizing the actions of people of color,[235] and which continues to arrest and incarcerate people of color at a disproportionate rate.[236]

A fourth source of error is the inevitable presence of artifacts that degrade algorithmic accuracy by changing what faces look like, including aging, facial hair, glasses, injuries, and cosmetics.[237] In early feasibility studies, FRT algorithms "had trouble with smiles . . . which 'distort the face and drastically change inter-facial measurements.'"[238] Solutions to the problem of facial change have improved over time, but algorithms still struggle with the more permanent alterations of age and injury.[239] For this reason, databases that include photographs taken years in the past are less

City of Detroit, No. 2:21-cv-10827 (E.D. Mich. July 7, 2023), ECF No. 60-3 (Director of Michigan State Police unit that conducts FRT searches unable to testify to the accuracy threshold setting in the FRT algorithms used by the agency; states that 'I think that [question] would be better for our vendor').").

232. FRTE, *supra* note 227, at 11 ("[D]ifferent versions give an order of magnitude fewer misses.").

233. Steve Lohr, *Facial Recognition Is Accurate, if You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html; Natasha Singer & Cade Metz, *Many Facial-Recognition Systems Are Biased, Says U.S. Study*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html; Shira Ovide, *A Case for Banning Facial Recognition*, N.Y. TIMES (Aug. 1, 2021), https://www.nytimes.com/2020/06/09/technology/facial-recognition-software.html; Davey Alba, *Facial Recognition Moves Into a New Front: Schools*, N.Y. TIMES (Feb. 6, 2020), https://www.nytimes.com/2020/02/06/business/facial-recognition-schools.html; Cade Metz, *Who Is Making Sure the A.I. Machines Aren't Racist?*, N.Y. TIMES (June 23, 2023), https://www.nytimes.com/2021/03/15/technology/artificial-intelligence-google-bias.html; Eduardo Medina, *Rite Aid's A.I. Facial Recognition Wrongly Tagged People of Color as Shoplifters*, N.Y. TIMES (Dec. 21, 2023), https://www.nytimes.com/2023/12/21/business/rite-aid-ai-facial-recognition.html.

234. GARVIE, FORENSIC WITHOUT THE SCIENCE, *supra* note 11, at 21.

235. *See generally* KHALIL GIBRAN MUHAMMAD, THE CONDEMNATION OF BLACKNESS: RACE, CRIME, AND THE MAKING OF MODERN URBAN AMERICA 1 (Harv. Univ. Press 2010).

236. Bureau of Just. Stats., NJC 307149, PRISONERS IN 2022—STATISTICAL TABLES SUMMARY (2023) ("The 2022 imprisonment rate for [B]lack persons (1,196 per 100,000 adult U.S. residents) was . . . 5 times the rate for white persons (229 per 100,000) . . . .").

237. FRTE, *supra* note 227, at 9.

238. Raviv, *supra* note 202 ("The computer still had trouble with smiles, for instance, which 'distort the face and drastically change inter-facial measurements.'").

239. FRTE, *supra* note 227, at 9 ("The remaining errors are in large part attributable to long-run ageing, facial injury and poor image quality.").

likely to be accurate. Porcha Woodruff, for example, was misidentified based on a photograph that was taken eight years before her arrest.[240]

A fifth source of error is target database congruity and maintenance. The images in a target database ideally need to have uniformity of characteristics such as lighting and pose. Databases also degrade over time as people get old and their appearances change.[241] The size and quality of the target database also affect FRT's accuracy: broader databases are more likely to include any given individual, but they are also more likely to include doubles and lookalikes.

A final source of error—and ultimately the strongest barrier to scientific validity—is integrated human decision-making. As currently implemented, there is a human component of FRT identification that frequently results in people who are listed lower in the results of an FRT identification becoming the focus of an investigation.[242]

FRT algorithms provide lists of results even when all similarity scores are low. This creates a problem when the person is simply not in the target database. Under these circumstances, "when a fixed number of candidates are returned, the false positive identification rate of the automated face recognition engine will be 100%, because a probe image of anyone not enrolled will still return candidates."[243] The human in the loop is supposed to review each photograph the algorithm returns to prevent error, but this turns out to be both mathematically and practically difficult. From a mathematical perspective,

> [w]hen humans review long lists of candidate photos, there are typically tens of opportunities for false matches: the human review must correctly reject *all* of them to avoid [a false positive]. In terms of binomial statistics, even if a reviewer's false match rate was 1 percent, then the chance of falsely accepting any one of 50 would be $1 - (1 - 0.01)$—which is about 0.4, or about a 40 percent chance that a mistake will be made.[244]

Practically, people are just not good at distinguishing faces, and the grounds for their decision-making in the FRT identification process are unclear. The NYPD, for example, requires its investigators to perform "a visual comparison" and "[p]erform [a] detailed background check to confirm reliability," without any further elaboration.[245] Improvements in algorithmic accuracy mean that the correct person now appears more often

240. Cho, *supra* note 6.

241. Ali Akbari, *Facial Recognition Technologies 101*, *in* THE CAMBRIDGE HANDBOOK OF FACIAL RECOGNITION IN THE MODERN STATE 29, 31 (Rita Matulionyte & Monika Zalnieriute eds., Cambridge Univ. Press 2024).

242. FACIAL RECOGNITION TECHNOLOGY, *supra* note 192, at 61 ("The use of human review is an integral part of the process, used in 100 percent of searches. Moreover, humans are fallible . . . .").

243. FRTE, *supra* note 227, at 17.

244. FACIAL RECOGNITION TECHNOLOGY, *supra* note 192, at 62.

245. N.Y. POLICE DEP'T, PROCEDURE NO. 212-129, PATROL GUIDE: FACIAL RECOGNITION TECHNOLOGY 3 (2020).

as the first-ranked result in a search, but this accuracy is entirely invalidated if law enforcement regularly selects candidates who are further down a list of results.

Each of these sources of error stands in the background of the use of FRT as a potentially corrupting factor in any given use of the technology. Each of them is fully obscured by witness-washing.

D. How FRT May Never Work

In her report *A Forensic Without the Science*, FRT scholar Clare Garvie asserts that FRT must be evaluated for its foundational validity using the same criteria as any other forensic feature comparison method—a process by which two things are compared to determine whether they are associated or, potentially, identical.[246]

In order to establish the foundational validity of FRT identification, studies would need to show that the *entire process* of FRT identification, including the action of the human reviewer, is repeatable, reproducible, and accurate.[247] The reviewer in question is the human operator—typically a detective—who is faced with a list of FRT results and must pick one for inclusion in an eyewitness identification procedure. The studies to establish foundational validity "must involve a sufficiently large number of examiners and must be based on sufficiently large collections of known and representative samples from relevant populations to reflect the range of features or combinations of features that will occur in the application."[248] For FRT, this would require the human operator to be able to repeatedly and accurately select a correct result from the list of candidates generated by the algorithm, while operating under conditions similar to those found in the real world.

The studies on human forensic facial comparison and on fillers in lineups provides good reason to believe that an integrated FRT process will never cross the threshold of scientific validity. Two different groups of people have claimed to have a greater capacity to distinguish faces than the average person: forensic facial examiners and super-recognizers. "[F]acial examiners are highly trained; super-recognizers rely on natural ability."[249] The problem is that neither group is particularly good at it under

246. GARVIE, FORENSIC WITHOUT THE SCIENCE, *supra* note 11, at 13 ("Any attempt to understand how reliance on a face recognition system can lead to police error, then, and how often it happens must be done so within the scientific framework used for evaluating the reliability of a forensic biometric tool.").

247. Fingerprint analysis, for example, has elaborate and empirically tested standards for human reviewers of algorithmic outputs. *See Latent Print Examination Process Map*, NAT'L INST. OF STANDARDS AND TECH., https://ipm.nist.gov/lpe (last visited Apr. 8, 2025).

248. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 79, at 52 (emphasis omitted).

249. Carina A. Hahn, Liansheng Larry Tang, Amy N. Yates, & P. Jonathon Phillips, *Forensic Facial Examiners Versus Super-Recognizers: Evaluating Behavior Beyond Accuracy*, 36 APPLIED COGNITIVE PSYCH. 1209, 1209 (2022).

real-world conditions.[250] The literature on fillers in lineups, which discourages use of images of similar-looking people, also documents this problem: "[e]xtremely high similarity creates a lineup of near-clones, thereby making it too difficult to identify the culprit from a culprit-present lineup."[251] When the suspect looks too much like the fillers, people are unable to make accurate identifications. It is possible that FRT may be highly accurate as a machine process, but will never be able to achieve foundational validity as a mixed human–machine process because people simply lack the capacity to distinguish between highly similar faces.

Much of the supposed accuracy of FRT is actually hidden in the language that is used to describe it. Due to the complexity of new technology, lawyers constantly try to understand technology through metaphors.[252] The overwhelming majority of sources on FRT identification discuss it using the language of matching.[253] NIST, for example, writes that facial recognition identification "determines whether the person in the [probe] photo has any match in a database and can be used for identification" purposes.[254] Law enforcement and other government reports also rely on the language of matching.[255] And the companies that market FRT to law enforcement use the language of actual or potential matches. A website for Amazon's FRT program, for example, informs potential buyers that "[w]ith [Amazon] Rekognition, you can search images, stored videos, and streaming videos for faces that match those stored in a container known as

250. *See, e.g.*, FACIAL RECOGNITION TECHNOLOGY, *supra* note 192, at 63 (asking "So how accurate are humans?" and then really answering adequately); Nicholas Bacci, Joshua G. Davimes, Maryna Steyn, & Nanette Briers, *Forensic Facial Comparison: Current Status, Limitations, and Future Directions*, BIOLOGY, Dec. 2021, at 1, 20.

251. Wells et al., *supra* note 18, at 17.

252. *See* Walter A. Mostowy, *Explaining Opaque A.I. Decisions, Legally*, 35 BERKELEY TECH. L.J. 1291, 1292 (noting that "AI [artificial intelligence] is opaque" and "today's AI is so complicated, it is difficult to understand its reasoning or identify and fix errors in its decisions"); Gabriel Nicholas, *Explaining Algorithmic Decisions*, 4 GEO. L. TECH. REV. 711, 715–16 (2020) (noting that algorithmic explainability varies by the complexity of a model and the sophistication of the explanation's audience).

253. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 159, at 5 ("[A] matching process . . . ."); *Facial Recognition System*, WIKIPEDIA, https://en.wikipedia.org/wiki/Facial_recognition_system (last visited July 20, 2024) ("A facial recognition system is a technology potentially capable of matching a human face from a digital image or a video frame against a database of faces.").

254. *Facial Recognition Technology (FRT): Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. 2 (2020) (statement of Charles H. Romine, Dir., Info. Tech. Lab'y, Nat'l Inst. of Standards & Tech.).

255. U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-106100, FACE RECOGNITION TECHNOLOGY: FEDERAL AGENCIES' USE AND RELATED PRIVACY PROTECTIONS 2 (2022) (noting FRT identification compares photos "to determine if there is a potential match"); *NYPD Questions and Answers Facial Recognition*, N.Y POLICE DEP'T, https://home.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page (last visited July 20, 2024) ("If possible matches are identified, trained Facial Identification Section investigators conduct a visual analysis to assess the reliability of a match . . . .").

a face collection."[256] One law review article simply refers to the technology as "face-matching."[257]

The problem is that the metaphor of "matching" obscures the confidence threshold that is being used. The literature and case law on DNA expert testimony directly addresses this similar issue: "To say that two patterns match, without providing any scientifically valid estimate (or, at least, an upper bound) of the frequency with which such matches might occur by chance, is meaningless."[258] For this reason, the use of "matching" language by DNA experts generally requires them to disclsoure underlying statistical data.[259] But the underlying statistical data needed to validate FRT has not been established.[260] "[W]ithout appropriate empirical measurement of a method's accuracy, the fact that two samples in a particular case show similar features has *no probative value*."[261]

The metaphor of matching is the most common way that users, developers, and scholars write about FRT. Evidence of an FRT "match" would not be allowed in a courtroom, however, because the language of matching is meaningless and has no probative value without a meaningful estimate of the accuracy of the process as applied.

IV. WITNESS-WASHING AND THE LIMITS OF INVESTIGATIVE TOOLS

So far, this Article has aimed to establish that witness-washing has allowed FRT to secretly and steadily proliferate within the criminal legal system. This has obscured the fact that FRT is an extremely complicated technology, has dubious origins, is rife with potential pitfalls, and may never work as its users expect. It is the kind of technology that should be subject to close scrutiny and wide discussion before being used in any decision-making process that could result in state action. This Part addresses the three potential avenues for making sure that FRT use is accurate and fair, and discusses how witness-washing interferes with the operation of each of these traditional limitations.

Generally, investigative tool use is limited by statutory provisions, constitutional rights, and the "practical considerations" of "limited police

256. *What Is Amazon Rekognition?*, AMAZON, https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html (last visited July 20, 2024); *see also Biometric Identification*, DATAWORKS PLUS, https://www.dataworksplus.com/bioid.html (last visited July 20, 2024) (advertising "the latest facial matching technology").

257. Henry H. Perritt, Jr., *Defending Face-Recognition Technology (and Defending Against It)*, 25 J. TECH. L. & POL'Y 41, 49 (2021) (referring to the FRT identification process as "face-matching").

258. NAT'L RSCH. COUNCIL, DNA TECHNOLOGY IN FORENSIC SCIENCE 74 (1992).

259. "[M]ost courts have held that, given the nature of DNA testing, a match is inadmissible unless the expert attaches a scientifically valid number to the figure." FAIGMAN, CHENG, MURPHY, SANDERS, & SLOBOGIN, *supra* note 49, § 30:25; George Bundy Smith & Janet A. Gordon, *The Admission of DNA Evidence in State and Federal Courts*, 65 FORDHAM L. REV. 2465, 2486 (1997) ("It is clear that most states require statistical evidence with the admission of DNA evidence."); Nelson v. State, 628 A.2d 69, 75–76 (Del. 1993) ("We hold that DNA matching evidence is inadmissible in the absence of a statistical interpretation of the significance of the declared match.").

260. GARVIE, FORENSIC WITHOUT THE SCIENCE, *supra* note 11, at 14.

261. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 79, at 53.

resources and community hostility."[262] Witness-washing has prevented any of these avenues from effectively regulating the use of FRT.

A. Statutory Limitations

Two different types of statutes could address the use of algorithmic tools like FRT by law enforcement. The first is the foundational statute that creates a police department and defines its responsibilities. The second is a specific statute that addresses the use of a technology by law enforcement. Witness-washing is only possible due to how broadly most foundational statutes are written, and witness-washing has allowed for end runs around many of the particular statutory provisions that are designed to address FRT.

The statutes that create law enforcement agencies are typically written in extraordinarily broad language. The NYPD's founding statute is typical:

> The police department and force shall have the power and it shall be their duty to preserve the public peace, prevent crime, detect and arrest offenders, suppress riots, mobs and insurrections . . . remove all nuisances in the public streets, parks and places; arrest all street mendicants and beggars . . . enforce and prevent the violation of all laws and ordinances in force in the city; and for these purposes to arrest all persons guilty of violating any law or ordinance for the suppression or punishment of crimes or offenses.[263]

Similarly, the Chicago Police Department is authorized "to preserve order, peace and quiet and enforce the laws and ordinances throughout the city,"[264] and the Los Angeles Police Department's authority is, without further elaboration: "[T]o enforce the penal provisions of the Charter, City ordinances and state and federal law."[265] These are incredibly broad mandates that impose no oversight mechanisms or restraints. They assume that oversight and restraint will be left to constitutional litigation in the courts.

Additionally, police departments are unique in that they do not follow the standard rules of an executive agency. They are not subject to notice and comment rulemaking, or any of the other limitations that typically apply to executive agencies in the regulatory state.[266] If law enforcement agencies were subject to these requirements, then the lack of an empirical

---

262. Illinois v. Lidster, 540 U.S. 419, 426 (2004) (holding that "[p]ractical considerations—namely, limited police resources and community hostility to related traffic tieups—seem likely to inhibit" the proliferation of suspicionless traffic stops); United States v. Jones, 565 U.S. 400, 416 (2012) (describing these two factors as "the ordinary checks that constrain abusive law enforcement practices").

263. N.Y.C., N.Y., CHARTER ch. 18, § 435(a) (2025).

264. CHI., ILL., CODE § 2-84-220 (2024).

265. L.A., CAL., CHARTER § 570 (2024).

266. There is an entire field of scholarship dedicated to this subject. *See, e.g.*, Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1843 (2015) ("Policing agencies—for that is what they are, agencies of executive government—fail to play by the rules of administrative governance.").

basis for FRT's benefits would create a problem at the cost–benefit analysis stage, and hiding the use of algorithmic tools would violate notice and comment regulations. But law enforcement agencies are subject to no such rules.

It is possible to imagine a founding statute for a police department that requires the department's investigative tools to have an empirical basis, be considered scientifically valid by their relevant scientific community, or at least have survived some sort of approval process.[267] A statute could, for example, require that any investigative tools the department uses be approved by a national commission on forensic science.[268] But this is not the case. This permissive default allows any and all tools to be used for investigation.

Instead of amending founding statutes, legislatures could rein in police departments' use of untested technology by passing statutes that directly restrict use of a specific type of technology. Maine,[269] Utah,[270] and Vermont[271] have enacted legislation specifically regulating the use of FRT.

Vermont passed a full prohibition: in Vermont "a law enforcement officer shall not use facial recognition technology…"[272] Similar bans have been passed in a handful of liberal municipalities, including San Francisco, Portland, Minneapolis, Baltimore, and Boston.[273] Bans address the problem of technological efficacy by reversing the traditional default: new technologies will not be used unless they have been explicitly authorized.

Maine's statute, however, is a prime example of the practical limitation of bans. It allows law enforcement agencies to use FRT in cases with charges involving a potential sentence of one year or more. The question of whether to categorize a crime as a charge carrying a year or more is almost entirely in the law enforcement agency's discretion. A detective who wants to use FRT in a run-of the-mill shoplifting case, for example, could simply write up the paperwork as a felony commercial burglary, which carries a potential sentence of more than one year. Additionally, Maine's statute does not create a method for monitoring, evaluating, or disclosing the use of FRT. It is a ban on paper, but witness-washing ensures that the problematic use of FRT will go unchecked by the statute. Detectives can continue to use FRT in essentially any case, without having to acknowledge their use of the technology or explain their charging

267. *See, e.g.*, 42 U.S.C. § 7408(a)(2) (mandating EPA consider "the latest scientific knowledge" when exercising its authority to establish air pollution standards).

268. *See* Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CALIF. L. REV. 721, 778–87 (2007) (proposing neutral centralized oversight agencies to evaluate law enforcement use of forensics).

269. ME. REV. STAT. ANN. tit. 25, § 6001(2) (2023).

270. UTAH CODE ANN. § 77-23e-103 (West 2024).

271. 2019 Vt. Adv. Legis. Serv. 166 § 14 (LexisNexis).

272. *Id.*

273. *Map*, BAN FACIAL RECOGNITION, https://www.banfacialrecognition.com/map/ (last visited Feb. 1, 2025).

decision, and the use will never be introduced in court or disclosed to the public.

Witness-washing also disrupts the effectiveness of statutes that are meant to regulate the use of FRT without banning it. Utah's statute requires that FRT is only used in felony cases; that technicians check the machine results for accuracy; and that law enforcement only use a facial recognition algorithm that "is produced by a company that is currently in business."[274] But it contains no provisions that require scientific validity or disclosure, or prohibit uses that might violate the embedded principles of the criminal legal system. These statutes appear to operate under the assumption that the standard courtroom safeguards for scientific validity and constitutional rights are working as intended.

The good news is that the underlying problem of witness-washed FRT could easily be addressed by a statute that is attuned to the problem. Internationally, the European Union recently passed a robust law regarding the use of algorithmic decision-making in general, with specific statutory language addressing biometric identification.[275] The Artificial Intelligence Act specifically prohibits member state law enforcement agencies from employing FRT identification in many situations.[276] It also requires disclosure of the use of any algorithmic process in high-risk service systems that impacts a citizen of the European Union.[277] This is a broad law that is designed to continue to control the use of many technologies going forward. It prohibits witness-washing by requiring disclosure of all uses of FRT and restricts FRT use in ways that cannot be manipulated.

In the United States, there is no federal statutory scheme that addresses FRT. A bill that would ban the use of FRT as an investigative tool has been proposed[278] but appears unlikely to pass. Legislators have also proposed bills that require disclosure of algorithmic tool use.[279] Any of these general bills could address the underlying problem of witness-washing and facilitate greater dialogue about and understanding of the tools themselves. But statutes enacted without an awareness of witness-washing will continue to allow the core problems of algorithmic tool use.

---

274. UTAH CODE ANN. §§ 77-23e-103(2)(c)(i), (4)(a)(iii), (4)(b) (West 2024).

275. Council Regulation 2024/1689, 2024 O.J. (L 1689) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689; Future of Life Inst., *High-Level Summary of the AI Act*, EUR. UNION A.I. ACT (Feb. 27, 2024), https://artificialintelligenceact.eu/high-level-summary/.

276. European Parliament Press Release, Artificial Intelligence Act: MEPs Adopt Landmark Law (Mar. 13, 2024) ("The use of biometric identification systems (RBI) by law enforcement is prohibited in principle, except in exhaustively listed and narrowly defined situations.").

277. *Id.*

278. Facial Recognition and Biometric Technology Moratorium Act of 2023, S. 681, 118th Cong. (2023).

279. *See, e.g.*, Algorithmic Justice and Online Platform Transparency Act, S. 2325, 118th Cong. (2023); Algorithmic Accountability Act of 2023, S. 2892, 118th Cong. (2023).

B. Constitutional Limitations

Constitutional litigation can also limit law enforcement use of algorithmic tools such as FRT. Law enforcement is less likely to use an investigative tool if judges regularly grant motions to suppress evidence created by it. Similarly, the people who design the tools are incentivized to respect those constitutional boundaries.

Witness-washing creates a preliminary barrier to any constitutional litigation regarding FRT. Before a litigant is able to address the technology in court, they must first find out if it has been used at all. As a general matter, discovery in criminal cases is weaker than civil discovery.[280] Discovery for complex scientific evidence is even worse.[281] And unlike many forms of scientific evidence, there is no reliable indicator that witness-washed FRT has been used in a case. One article for defense attorneys contemplating FRT litigation suggests, as a starting point, that defense attorneys should file and litigate a specific discovery motion for FRT in every case in which identity is at issue and law enforcement has an image of a suspect.[282] But due to surveillance video's ubiquity, these are very common conditions.

The barrier to disclosure is further complicated by the context in which the majority of these discovery motions would be litigated. The overwhelming majority of criminal cases are resolved by pleas, not by trials. The criminal trial is a "residue of a residue: it is a mechanism for handling survivors of a long filtering process."[283] In 2023, 98% of federal convictions and 95% of state convictions were the result of pleas.[284] Cases are frequently resolved by plea before discovery is complete, and defendants can be informally punished for aggressive discovery litigation with harsher plea offers.[285] Most of this bargaining is done by public defenders, who are notoriously underfunded and overburdened.[286] Under these conditions, defense attorneys are unable to fully litigate every issue in every case and are required to triage their caseload and prioritize the litigation that has the highest probable impact on the outcome of a case. Aggressively litigating preplea discovery in hopes of finding witness-washed FRT use would require a substantial expenditure of limited resources.

280. Murphy, *supra* note 82, at 645 ("[D]iscovery rules tend to be far narrower in criminal cases than in civil ones.").

281. *Id.* at 645–52 (describing the various barriers to meaningful discovery of modern investigative tools).

282. Garvie, *supra* note 3, at 22.

283. FRIEDMAN, *supra* note 171, at 386.

284. Lucian E. Dervan, *Fourteen Principles and a Path Forward for Plea Bargaining Reform*, A.B.A. CRIM. JUST. MAG., Winter 2024, at 24.

285. *See* Stephanos Bibas, *Plea Bargaining Outside the Shadow of Trial*, 117 HARV. L. REV. 2463, 2493–96 (2004) (addressing the problems of information deficits in the plea bargaining system).

286. Murphy, *supra* note 82, at 654 ("Counsel often carry crushing caseloads that leave them little time for deciphering complex evidence, and they may lack the scientific sophistication to comprehend the issues on their own.").

Even if the use of FRT in a case is discovered, the majority of the litigation necessary to address it would occur in state criminal courts. The overwhelming majority of criminal cases are processed in these courts. Like the public defenders who work in them, these courts are also underfunded, overwhelmed, and poorly suited to understand complex scientific tools such as FRT.[287] The majority of the defendants who are processed in these courts are from race–class subjugated communities that lack political power to change law enforcement and judicial practices.[288]And the judges are loathe to grant suppression motions that might result in dismissal on technical grounds.[289] In one survey of state courts, defense attorneys only filed motions to suppress eyewitness identification in around 1% of cases, and judges granted fewer than 6% of those motions.[290]

C. Practical Limitations

In *Illinois v. Lidster*,[291] the Supreme Court outlined two practical considerations that limit the investigative tools of law enforcement.[292] The Court observed that "[p]ractical considerations of limited police resources and community hostility" limit the proliferation of police checkpoints.[293] Justice Sotomayor subsequently described these as "the ordinary checks that constrain abusive law enforcement practices," and expressed concern that advancing technology was eroding these checks.[294]

Witness-washing has hamstrung the first practical limitation of community outrage. As the bans in Maine and Vermont show, there is genuine concern in communities about the use of FRT. People have a good reason to be concerned about being part of a "perpetual line-up."[295] Given the 37% error rate in eyewitness identifications in the field, being constantly subjected to potential misidentification through FRT creates a real threat of false prosecution for any person in a police database—which, by one

287. Robert M. Cover & T. Alexander Aleinikoff, *Dialectical Federalism: Habeas Corpus and the Court*, 86 YALE L.J. 1035, 1051 (1977) ("[G]iven the quite difficult and legitimate objectives of the state court systems, one would hardly expect them to have a Utopian perspective on constitutional rights relevant to the criminal process.").

288. Jocelyn Simonson, *Police Reform Through a Power Lens*, 130 YALE L.J. 778, 805 (2021).

289. Burt Neuborne, *The Myth of Parity*, 90 HARV. L. REV. 1105, 1127 (1977) ("To the extent that the forum is itself subject to the political pressures which shaped the judgment it is asked to review, its capacity to provide sustained enforcement of countermajoritarian constitutional norms will be diminished.").

290. Stephen G. Valdes, *Frequency and Success: An Empirical Study of Criminal Law Defenses, Federal Constitutional Evidentiary Claims, and Plea Negotiations*, 153 U. PA. L. REV. 1709, 1730–31 (2005) (finding motions to suppress evidence due to faulty identification procedures were offered in 1–1.2% of cases in multistate survey of 400 state judges, defense attorneys, and prosecutors, and granted in 6% of those cases).

291. 540 U.S. 419 (2004).

292. *Id.* at 420.

293. *Id.*

294. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

295. GARVIE ET AL., *supra* note 211, at 72.

estimate, is half of all Americans. But most people are unaware that law enforcement is even using FRT,[296] which prohibits outrage and organizing.

The second practical limitation—limited police resources—is the largest concern for witness-washed algorithms. The fundamental purpose of algorithmic technology is to vastly increase what people can do with limited resources. Algorithms are extremely effective at turning tasks that were previously monumental into tasks that happen automatically, without any human intervention at all.

The Supreme Court's acknowledgement of practical considerations is something of a jurisprudential anomaly,[297] but there is good reason to believe that the practical consideration of limited police resources has always been the primary check on law enforcement. Consider automated license plate readers.[298] This technology consists of a network of surveillance cameras that are connected to a pattern-matching algorithm that is designed to isolate and record any passing vehicle's license plate. This data is then cross-referenced with DMV databases of vehicles, which include the names of vehicle owners. The data is aggregated in large databases and connected to mapping technologies. Police departments have deployed this technology in static cameras throughout cities and in police cars to constantly scan the plates of any vehicle it passes. This creates an extensive log of vehicles' movements over time. Before algorithmic technology was deployed, this project would have required immense resources. Law enforcement agencies would have needed to station a police officer at every streetcorner and task them with recording each license plate that passed by. All of these data logs would have had to be submitted to some central agency, which would have had to find some human way to build a map of the movement of each car over time. Additional officers would be employed just to sort and provide the data when requested. When contemplating such an immense use of public resources, there is an intuitive sense that it would immediately be subject to litigation, that some sort of statutory authority would have to be granted or overcome, or that communities would immediately protest. But automated license plate readers have already been invisibly deployed by police departments that complete all of these tasks, with minimal resistance from statutes, litigation, or community organizing. The only thing prohibiting law enforcement from

296. Douglas MacMillan, David Ovalle, & Aaron Schaffer, *Police Seldom Disclose Use of Facial Recognition Despite False Arrests*, WASH. POST (Oct. 6, 2024), https://www.washingtonpost.com/business/2024/10/06/police-facial-recognition-secret-false-arrest/#.

297. George M. Dery, III & Kevin Meehan, *Making the Roadblock A "Routine Part of American Life:"* Illinois v. Lidster's *Extension of Police Checkpoint Power*, 32 AM. J. CRIM. L. 105, 126 (2004) ("Assuming the best from government authorities, however, is a novel approach to constitutional jurisprudence.").

298. *See* Ángel Díaz & Rachel Levinson Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, BRENNAN CTR. FOR JUST. (Sept. 10, 2020), https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations (detailing functionality of automated license plate readers generally).

implementing such a dazzlingly immense surveillance network was the practical consideration of limited resources.

V. AGAINST GOOGLING GUILT

FRT has been described as "the most uniquely dangerous surveillance mechanism ever invented,"[299] as having "apocalyptic capabilities,"[300] and as a technology that "threatens to forever alter our free society . . . turning us all into subjects to be monitored, tracked, and scrutinized wherever we go."[301] It has in fact been used to surveil and oppress racialized populations and to identify people who are potentially opposed to an authoritarian regime.[302] The People's Republic of China, for example, deployed a racist FRT algorithm that was designed to track and monitor only the faces of people who looked like they belonged to a particular ethnic minority.[303] Police departments in the United States have mostly used FRT as a secretive tool to facilitate arrests.

But this path for FRT is not preordained. Like all tools, FRT is well suited for some tasks and poorly suited for others.[304] Section V.A argues that FRT identification is fundamentally exculpatory for any individual who is identified through the current process, because it provides a strong third-party guilt defense. The potential use that is best suited to the technology itself is to provide a strong suggestion of innocence. The tool's most logical use is to reduce the rate at which people are falsely convicted due to the vagaries of eyewitness identification.

Despite this, FRT has primarily been used to identify people and pressure them into pleas. Witness-washing has allowed the carceral logic of police and the commercial logic of the technology's developers to predominate over the strengths and weaknesses of the tool itself.

---

299. Woodrow Hartzog & Evan Selinger, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/@hartzog/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.

300. Raviv, *supra* note 202 ("Unlike other world-changing technologies whose apocalyptic capabilities became apparent only after years in the wild . . . .").

301. Abdullah Hasan, *2019 Proved We Can Stop Face Recognition Surveillance*, ACLU NEWS & COMMENT. (Jan 17, 2020), https://www.aclu.org/news/privacy-technology/2019-was-the-year-we-proved-face-recognition-surveillance-isnt-inevitable#.

302. Lena Masri, *Facial Recognition Is Helping Putin Curb Dissent with the Aid of U.S. Tech*, REUTERS (Mar. 28, 2023, 10:00 AM), https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/.

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

304. Cynthia Lum, Christopher S. Koper, & James Willis, *Understanding the Limits of Technology's Impact on Police Effectiveness*, 20 POLICE Q. 135, 139 (2017) (describing task-technology-fit theory of new technology in law enforcement).

A. The Logic of FRT

FRT is an excellent tool for narrowing a field of possible suspects down to a list of very similar-looking people, and for providing any of those people with a strong, third-party guilt defense.

As discussed above, FRT is a forensic feature comparison technology. Its core logic is the same as that of any other comparison technique. It compares the features of two things, and aims to determine whether the two things are in the same category. A firearms expert, for example, might be able to identify a gun used in a shooting as a certain make and model. Forensic feature comparison's ultimate goal is to be able to determine that two things are in fact the exact same thing. The firearms expert wants to be able to identify a gun as the specific gun that was used in a shooting. The goal is to achieve individualization, "the process of placing an object in a unit category which consists of a single unit."[305]

In everyday life, seeing a person's face is typically sufficient to achieve individualization. We know people by their faces. The frequency with which we see startlingly similar faces is certainly not zero—identical twins make up around 0.25% of deliveries in the world.[306] But most of the time, we know someone is who we think they are because we successfully compare the face we see with the face we remember. However, the intuitive nature of identifying people by their faces breaks down with the use of FRT.

Wigmore on Evidence has the following to say as to the use of comparisons for identity: "A mark common to two supposed objects is receivable to show them to be identical whenever in human experience the mark does not occur with so many objects that the chances of the two supposed objects are too small to be appreciable."[307] The key here is human experience. Consider a small town in which everyone provides their phone number with only seven digits, leaving out the area code. The population is small enough that these seven marks are enough to achieve individualization. Only one person has these seven marks, so you reach who you expect to when you dial the number. But if you move to a large city and provide a seven-digit phone number, everyone will immediately ask for your area code. Seven marks are no longer sufficient to achieve individualization. This is what FRT does with faces. What might be enough facial similarity to identify a person within human experience is simply not sufficient for a database of 12 million people[308]—no human experience will ever include

305. 3 DAVID L. FAIGMAN, EDWARD K. CHENG, JENNIFER L. MNOOKIN, ERIN. E. MURPHY, JOSEPH SANDERS, & CHRISTOPHER SLOBOGIN, MODERN SCIENTIFIC EVIDENCE: THE LAW AND SCIENCE OF EXPERT TESTIMONY § 29:26, at 72 (Thomson Reuters 2017–2018 ed.).

306. Christiaan Monden, Gilles Pison, & Jeroen Smits, *Twin Peaks: More Twinning in Humans Than Ever Before*, 36 HUM. REPROD. 1666, 1668 (2021).

307. 2 WIGMORE, *supra* note 33, § 412, at 480 (emphasis omitted).

308. GROTHER, NGAN, & HANAOKA, *supra* note 223, at 2.

12 million faces. Witness-washed FRT is the big city of technology that misrepresents itself as the small town of human experience.

The insufficiency of individualization in expert testimony occurs when experts are not able to testify with certainty that two things are identical. This is a common problem, but this problem is typically mitigated because judges, juries, and lawyers are aware of it when it appears.

> If a witness were to describe a perpetrator as "tall and bushy haired," jurors could make a reasonable judgment of how many people might match the description. But, if an expert witness were to say that, in two DNA samples, the third exon of the *DYNC1H1* gene is precisely 174 nucleotides in length, most jurors would have no way to know if they should be impressed by the coincidence . . . .[309]

With FRT, a subject that appears to be in the realm of common sense—facial similarity—is distorted into a scientific population claim without notice.

In order to be accurate, scientific population claims must be based on scientific studies of how often common features recur in a population. But these claims function in counterintuitive ways. This is most clearly illustrated in the classic evidence case of *People v. Collins*.[310] In *Collins*, a witness stated that the people who committed a crime were a blonde woman and a Black man with a beard who was driving a yellow car.[311] The police arrested a Black man and a blonde woman with a yellow car.[312] The prosecution called a math professor to speculate about the likelihood of this combination occurring at random.[313] "Applying the product rule to his own factors the prosecutor arrived at a probability that there was but one chance in 12 million that any couple possessed the distinctive characteristics of the defendants."[314] Professor Laurence Tribe has pointed out that this testimony contained a fundamental flaw:

> [T]he prosecutor erroneously equated the probability that a randomly chosen couple would possess the incriminating characteristics, with the probability that any given couple possessing those characteristics would be innocent. After all, if the suspect population contained, for example, twenty-four million couples, and if there were a probability of one in twelve million that a couple chosen at random from the suspect population would possess the six characteristics in question, then one could well expect to find two such couples in the suspect population, and there would be a probability of approximately one in two—

309. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 79, at 45.
310. 438 P.2d 33 (Cal. 1968).
311. *Id.* at 34.
312. *Id.* at 34–35.
313. *Id.* at 36.
314. *Id.* at 37.

> not one in twelve million—that any given couple possessing the six characteristics would be innocent.[315]

FRT identification identifies a category of similar-looking people who could have committed a crime.[316] Each of them has a strong third-party guilt defense. They are able to argue that the crime was not committed by them, but instead by someone else on the list, or by a person who is in the same category but was not in the searched database.

FRT does not individualize. It creates a small category. A detective then searches through this category and selects someone. As in *Collins*, the probabilities involved will appear highly inculpatory if viewed from the perspective of the general population. A suspect who is identified by FRT may bear a one-in-a-million resemblance to the person in a surveillance video. But if FRT was used to sort a database of 12 million people, then it is probable that there are eleven other individuals who also bear a one-in-a-million resemblance to the person in the surveillance video. The odds of a given person who bears a one-in-a-million resemblance being innocent is not one in a million. It is eleven in twelve. For any particular person identified by FRT, the core logic is exculpatory.

The criminal legal system already recognizes this logic when facial similarity arises in other contexts. Consider identical twins, who defy our typical intuition that people can be distinguished by their faces. When the primary evidence against an identical twin is an eyewitness identification, prosecutors and judges have sometimes dismissed the case.[317] In *State v. Coleman*,[318] for example, police began the process of arresting an identical twin but allowed him to go into a room that he shared with his twin.[319] "[T]he state thereby became disabled to discharge its burden of so identifying the particular defendant on trial as to prove his guilt beyond a reasonable doubt."[320]

Consider the case of Richard Jones—discussed in the Introduction—who was exonerated by evidence that he bore sufficient facial similarity to another suspect and could easily have been mistaken for him. Mr. Jones was not simply granted a new trial. He was fully exonerated, and the state

---

315. Laurence H. Tribe, *Trial by Mathematics: Precision and Ritual in the Legal Process*, 84 HARV. L. REV. 1329, 1336 (1971).

316. This applies to the current use of FRT identification by law enforcement, and could be fixed with threshold settings. This kind of use-specific complexity is a further reason why the technology should not remain unexamined.

317. *See, e.g.*, People v. Luevanos, No. B270781, 2017 WL 1371482, at *5 n.9 (Cal. Ct. App. Apr. 14, 2017) ("The People stated that the third defendant had an identical twin. The People had decided not to proceed with charges against him based on uncertainty as to whether the 'right twin' had been identified."); Roberson v. State, 798 S.W.2d 602, 606 (Tex. App. 1990), *rev. granted and cause remanded*, 810 S.W.2d 224 (Tex. Crim. App. 1991) ("In addition, and in light of the undercover officers' admitted difficulty in distinguishing the twins . . . we conclude that, but for counsel's errors, there is a reasonable probability that the result of the trial would have been different.").

318. 266 S.W.2d 614 (Mo. 1954).

319. *Id.* at 615.

320. *Id.* at 616.

paid him over a million dollars for his years of wrongful confinement.[321] In this case, there was additional information linking the alternative suspect to the crime, but the search began with the discovery of a facial similarity. FRT provides a tool with which substantial facial similarity could be found in essentially any case.

When courts and prosecutors encounter instances of facial similarity outside of the FRT context, they frequently acknowledge the exculpatory value. In some circumstances, twins are not prosecuted because their facial similarity prohibits accurate identification. A witness acknowledging an inability to tell the difference between two similar-looking suspects can result in an exoneration. When comparing individuals, facial similarity generally makes it *less* likely that a particular person committed a crime.

B. Carceral Logic

Witness-washing has prevented defendants from surfacing this exculpatory logic by preventing the technology from entering the adversarial system, where multiple views could be presented regarding the value and implications of FRT evidence. In the absence of external checks, the logic that is inherent in law enforcement organizations has predominated instead. The foreground of this logic is the standard model of policing. The background is mass incarceration.

Most law enforcement departments are committed to what scholars refer to as the "standard model of policing."[322] The standard model of policing emphasizes three axes of efficiency: (1) increasing the percentage of reported crimes in which an arrest is made ("clearance rates"), (2) improving response times to 911 calls, and (3) increasing police presence through general, randomized patrols. Empirical research on the standard model of policing shows that it is not effective in reducing crime rates or improving safety in communities, but that police departments are slow to embrace empirical analyses and cultural change.[323]

Scholars of law and technology describe law enforcement agencies as implementing technology primarily in order to increase the efficiency of existing models of policing.[324] "At the most basic level, technology is a

321. *Richard Jones*, NAT'L REGISTRY OF EXONERATIONS (Nov. 18, 2019), https://www.law.umich.edu/special/exoneration/Pages/casedetail.aspx?caseid=5155 ("A photograph of Amos showed that he looked almost identical to Jones.").

322. Lum, Koper, & Willis, *supra* note 304, at 138 ("This reactive nature of policing, characterized and fostered by an incident-based, response-oriented, and procedures-dominated approach, is often referred to as the standard model of policing.").

323. Cody W. Telep & David Weisburd, *What Is Known About the Effectiveness of Police Practices in Reducing Crime and Disorder*, 15 POLICE Q. 331, 341, 344 (2012) (reviewing empirical literature and finding minimal evidence of effectiveness for random patrol, rapid 911 response, and general reactive arrest policies, although an increase in targeted patrol does correlate with decreases in crime in the targeted areas).

324. Sarah Brayne & Angèle Christin, *Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts*, 68 SOCIAL PROBS. 608, 612 (2021) ("Scholars report that digital tools are often 'translated' in order to fit local priorities and concerns, both in police

means to increase an organization's technical efficiency, defined as maximizing outputs using the lowest cost, time, and resources possible."[325] This efficiency is seen specifically as an efficiency at the level of the individual tasks that law enforcement is already prioritizing: "[T]he ability to respond to crime and to quickly identify suspects, victims, witnesses, and other aspects of crimes to resolve cases."[326] This efficiency is rarely defined in terms of more abstract or higher level outcomes such as reducing crime rates or improving community relationships.[327]

The primary use of FRT identification in law enforcement is to make this standard, ineffective model of policing more efficient. Law enforcement agencies adopt FRT to increase clearance rates by making an arrest in investigations that would otherwise not be resolved. But there is no evidence that an increase in clearance rates will reduce crime rates and improve community safety. Even if there were a relationship between clearance rates and safety, there is minimal empirical support for the idea that FRT and other advanced technology will improve clearance rates. Clearance rates have been slowly declining for the past thirty years, despite the introduction of powerful technological tools such as DNA analysis, mass video surveillance, and powerful information processing tools such as CompStat.

In the background is the carceral logic of mass incarceration.[328] Law enforcement in America has been shaped by one of the largest experiments in social control in human history. The growth of criminal control has been overwhelming in scope and immense in severity for the past fifty years. The United States has radically increased the proportion of its population that is in prison or under government supervision—an increase that has been strongly stratified across the lines of class and race.[329] It has been heavily motivated by political concerns.[330] Although crime rates have fallen over this same time period, polls show that most Americans are

---

departments and criminal courts, which leads practitioners to ignore the tools that they find 'inefficient.'"); Lum, Koper, & Willis, *supra* note 304, at 139 ("Officers likely fit technology use and expectations to their daily tasks, which are much more focused on reaction and arrest.").

325. Lum, Koper, & Willis, *supra* note 304, at 135–36 (emphasis omitted).

326. *Id.* at 151.

327. *Id.*

328. A review of the literature on mass incarceration is well beyond the scope of this article. For a highly accessible overview of the statistics, see Wendy Sawyer & Peter Wagner, *Mass Incarceration: The Whole Pie 2024*, PRISON POL'Y INITIATIVE (Mar. 14, 2024), https://www.prisonpolicy.org/reports/pie2024.html. Root causes and consequences are more complicated. *See, e.g.*, COMM. ON CAUSES AND CONSEQUENCES OF HIGH RATES OF INCARCERATION ET AL., NAT'L RSCH. COUNCIL OF THE NAT'L ACADS., THE GROWTH OF INCARCERATION IN THE UNITED STATES: EXPLORING CAUSES AND CONSEQUENCES (Jeremy Travis, Bruce Western, & Steve Redburn eds., 2014); WILLIAM J. STUNTZ, THE COLLAPSE OF AMERICAN CRIMINAL JUSTICE (2011); DAVID GARLAND, THE CULTURE OF CONTROL: CRIME AND SOCIAL ORDER IN CONTEMPORARY SOCIETY (2002).

329. *See, e.g.*, ALEXANDER, *supra* note 88, at 4; PAUL BUTLER, CHOKEHOLD: POLICING BLACK MEN (2017); MUHAMMAD, *supra* note 235, at 1; LOÏC WACQUANT, PRISONS OF POVERTY (1999).

330. STUNTZ, *supra* note 328, at 68 ("The justice system's institutional arrangements appear to be a bit slapdash, as though the relevant offices and institutions were thrown together by second-rate politicians who gave little thought to the system they were establishing—which is roughly what happened.").

unaware of the massive decrease in crime rates, and aggressive law and order rhetoric continues to be a prominent feature in political debates.[331] In the course of this project, law enforcement has been cast in the role of warriors in a war on crime, and increasingly provided with military equipment, technology, and tactics.[332] The police departments now deploying witness-washed technology have been on the front lines of this carceral project for generations.

The introduction of technology is only empowering the preexisting paths of the criminal legal system. Even when technology is a poor fit for this system's goals, law enforcement agencies use it to further those goals in whatever way they can. Witness-washing has prevented countervailing concerns and opposing parties from having a voice in the adoption and use of technologies, and is allowing the carceral logic of law enforcement to predominate over the logic inherent in the tool itself.

What proliferates in a monoculture is more of the same. Due to the immense efficiency of algorithmic technologies, witness-washed technology promises much more of the same, delivered much more quickly.

C. Commercial Logic

FRT is a multi-billion-dollar growth industry that is driven in large part by law enforcement contracts.[333] FRT's developers are profit-seeking corporations who are required to maximize profits for shareholders. These corporations are not beholden to the values of transparency, theoretical accuracy, accuracy as applied, or respect for the rights of defendants.[334]

The interests of profit-driven developers can distort the inherent logic of the tools that they sell by embedding corporate motivations in design decisions and creating incentives to overstate the usefulness of tools.

---

331. *See, e.g.*, *Trump Promises to Militarize Police, Reincarcerate Thousands, and Expand Death Penalty*, AMER. C.L. UNION (July 19, 2024), https://www.aclu.org/news/criminal-law-reform/trump-promises-to-militarize-police-reincarcerate-thousands-and-expand-death-penalty.

332. *See generally* RADLEY BALKO, RISE OF THE WARRIOR COP: THE MILITARIZATION OF AMERICA'S POLICE FORCES 139–77 (2013); BERNARD E. HARCOURT, THE COUNTERREVOLUTION: HOW OUR GOVERNMENT WENT TO WAR AGAINST ITS OWN CITIZENS (2018).

333. THE CAMBRIDGE HANDBOOK, *supra* note 192, at 27 ("There are also sustained commercial imperatives to continue this technology – not least the emergence of a $5 billion FRT industry that is estimated to grow to $50 billion by 2030.").

334. *See* Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 38 (2016) ("[B]ig data tools are often private market products; police departments are just another group of customers."). Most of the scholarship in this area addresses transparency, which is less of a concern for witness-washed technologies because they already evade review. *See* Hannah Bloch-Wehba, *Visible Policing: Technology, Transparency, and Democratic Control*, 109 CAL. L. REV. 917, 954–57 (2021) (showing how private companies craft law enforcement contracts to evade transparency litigation); Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595, 1598 (2016) ("Surveillance policy making by procurement can short-circuit [the democratic] process when elected officials and the public are left without a meaningful understanding of what technologies their law enforcement agency is acquiring."); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1343 (2018) (analyzing law enforcement technology vendor claims that information about their technology should not be disclosed due to being protected trade secrets).

The commercial logic embedded in design decisions has a large impact on extremely complex algorithmic tools like FRT. The algorithmic technologies that are susceptible to witness-washing are all designed for use by nonexperts. These nonexperts interact not with the algorithm itself but with a user interface designed for their ease.[335] Designers can choose to include (or to ignore) principles such as technical accuracy and defendant's rights when designing these systems.[336] Consider the technician in *Lynch*, who testified that there was a single star displayed beneath Willie Lynch's photograph, but that she did not know what the star meant.[337] The designer of the FRT system decided that a series of stars—without further elaboration—was the most user-friendly way to convey information. But it certainly is not the most informative.

The result is that even the law enforcement agencies that use these technologies do not understand how they work. It is commercially advantageous for the tools to be easy to use and understand, and expensive for law enforcement to independently develop expertise. When the director of the Michigan State Police unit that conducts FRT searches was asked in a deposition about the accuracy threshold setting used by the agency's FRT, they responded "I think that [question] would be better for our vendor."[338] Commercial concerns are the reason why FRT is shipped with editing tools for modifying probe photos—modifications may render the results scientifically useless by searching for a person who does not exist, but they do provide some kind of result for a detective using the system. This is good for the vendor, who can claim to have added value to the investigation. For the detective, it is precisely as useless as employing a psychic.

Vendors are also incentivized to exaggerate their technologies' usefulness and to negotiate contracts that minimize exposure of their technologies to external review. For technologies that are regularly subject to *Daubert* hearings, this takes the form of an appearance of reliability for those courtroom hearings.[339] For witness-washed technologies, this incentive manifests itself in when vendors advocate for broader use of their product, regardless of its technical accuracy. Clearview AI, an early progenitor of law enforcement FRT, provides clear examples of this. In emails

335. Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 101, 124 (2017) ("When one company dominates the market for a surveillance technology, its choices about product design make important decisions about policing before the police themselves have an opportunity to do so.").

336. *See* Andrew Guthrie Ferguson, *Big Data Prosecution and* Brady, 67 UCLA L. REV. 180, 254 (2020) (examining designer decisions to ignore legal requirements to disclose exculpatory information when designing big data technology for law enforcement, and proposing that designers in the future incorporate an automated "*Brady* Button" that would provide exculpatory information when clicked).

337. Initial Brief of Appellant at 14, Lynch v. State, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018) (No. 1D16-3290).

338. Deposition Transcript of Krystal Howard at 39:16–21, Williams v. City of Detroit, No. 2:21-CV-10827 (E.D. Mich. 2023) *dismissed*, June 28, 2024.

339. *See* Maneka Sinha, *Radically Reimagining Forensic Evidence*, 73 ALA. L. REV. 879, 927–37 (2022) (describing the ways in which forensic communities with financial interests in admissibility have manufactured an appearance of reliability).

to law enforcement users, Clearview sales representatives encouraged police to "'run wild' with" searches;[340] stated the more people searching, the more successes;[341] and advised that "[i]nvestigators who do 100+ Clearview searches have the best chances of successfully solving crimes with Clearview in our experience . . . . You never know when a search will turn up a match."[342] The company also regularly approached individual officers and offered them free accounts to use on their cell phones.[343] This tactic fully bypassed any policies that departments might have had in place regarding the accurate use of investigative tools, with the apparent hope that individual, unregulated use would eventually translate into sales to the department that employed the officers.

The commercial logic of FRT is embedded in user-friendly interfaces and vendor representations that are made to encourage use of their product, not to further the ideals of accuracy and fairness. The carceral logic of law enforcement turns these tools into ways to increase the efficiency with which they can clear cases, without considering whether the tool itself is a good fit for this use. Like a Google search, the process of using FRT in modern law enforcement involves inputting a search term, waiting while an inscrutable process occurs, and then getting a result that is usable in some way but ultimately driven by profit motives and user preferences. Witness-washing is dangerous because algorithmic technologies will be adopted and will proliferate, not for the purposes to which they are most logically suited but instead in line with the carceral interests of law enforcement and the commercial interests of technology vendors. Witness-washing hides a regime of Googling guilt.

CONCLUSION

The criminal legal system is transitioning to a new form of adjudication: a mixed human–machine algorithmic process in which human decisions are heavily influenced by algorithmic outputs. It is unclear how far this transition has already progressed, because witness-washing is such an incredibly effective mechanism for preventing the disclosure of information about our progress. FRT, for example, has been in use for over two decades but has barely been examined in the courtroom. A closer look at the technology shows that it is immensely complex, and that its use is full of theoretical and practical pitfalls. The statutory, constitutional, and practical limitations that typically limit law enforcement overreach are

340. Ryan Mac, Caroline Haskins, & Logan McDonald, *Clearview AI Once Told Cops To "Run Wild" with Its Facial Recognition Tool. It's Now Facing Legal Challenges*, BUZZFEED NEWS (Jan. 28, 2020, 1:34 PM), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-cops-run-wild-facial-recognition-lawsuits.

341. *Id.*

342. Caroline Haskins, Ryan Mac, & Logan McDonald, *Clearview AI Wants to Sell Its Facial Recognition Software to Authoritarian Regimes Around the World*, BUZZFEED NEWS (Feb. 5, 2020, 6:51 PM), https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-authoritarian-regimes-22.

343. Complaint at paras. 8 & 61, ACLU v. Clearview AI, Inc., No. 20 CH 4353 (Ill. Cir. Ct. 2021).

ill-suited to address algorithmic technologies like FRT. This commercial, profit-driven technology is being incorporated into law enforcement practices to increase the speed at which they can accomplish their preexisting tasks, regardless of whether the technology is a good fit for that purpose. The result is an unknown number of cases in which eyewitness identification by a person was in fact only the confirmatory part of a multistep process, whose first step was an untested technology.

Most seismic shifts in the nature of the criminal law are announced. In 1215, the jury trial became the dominant form of adjudication after the announcement that priests would no longer take part in trials by ordeal.[344] The War on Crime was announced on national television.[345] The DNA revolution immediately became the subject of extensive court hearings covered by the *New York Times*.[346] But now, witness-washing is allowing for a seismic shift towards algorithmic tools to occur in silence.

The danger of algorithmic tools is that criminal proceedings will be reduced to a subsidiary step in an algorithmic process. Officers will patrol places determined by an algorithm, target people placed on a red list by an algorithm, respond to loud noises identified by an algorithm, and make arrests due to FRT identifications that are driven by an algorithm. But this enormous shift in criminal investigations and prosecutions will enter criminal cases as if it was simply a series of decisions determined by human discretion. Witness-washed FRT is a warning. It shows us that the transition to algorithmic adjudication will not be announced, litigated, and debated. It is happening now, it is happening in secret, and it is being driven by carceral and commercial logics.

344. Fisher, *supra* note 29, at 585–86.

345. Statement by the President on Establishing the President's Commission on Law Enforcement and Administration of Justice, 2 PUB. PAPERS 382 (July 26, 1965).

346. Robert D. McFadden, *Reliability of DNA Testing Challenged by Judge's Ruling*, N.Y. TIMES (Aug. 15, 1989), https://www.nytimes.com/1989/08/15/nyregion/reliability-of-dna-testing-challenged-by-judge-s-ruling.html.