THE ORACLE TESTIFIES: FACIAL RECOGNITION TECHNOLOGY AS EVIDENCE IN CRIMINAL COURTROOMS

By Jessica Gabel Cino, Heather Kleider-Offutt, Beth Stevens, Kat Albrecht, Robert Evans, & Emma Riedley[⊗]

ABSTRACT

Criminal investigatory tools are advancing faster than the courts are prepared to deal with them, leaving significant gaps in evidentiary standards when it comes to technological innovation. One such innovation is Facial Recognition Technology (FRT), which was recently catapulted into broader use following the January 6th Capitol riot hearings. This Article analyzes a myriad of evidentiary challenges related to the use of FRT in criminal courtrooms, cautioning its use given concerns about algorithmic bias, proprietary information, and obfuscated accuracy thresholds. These concerns are drawn out across several legal issues that are particularly relevant to FRT, including admissibility issues under Daubert, Fourth and Sixth Amendment concerns, and potential Brady violations. FRT is not only ethically and legally complex in its own right, but it can also be usefully compared with eyewitness identification, a more traditional method of identifying criminal defendants that has its own well-documented shortcomings. In making this comparison, this Article then offers a targeted legal analysis that uncovers the complexity of evidentiary challenges with using FRT and the lack of protections for criminal defendants compared to eyewitness identification. This comparison is conducted across several legal issues, including Daubert standards, the confrontation clause, search and seizure protections, and Brady violations.

INTRODUCTION

When the FBI struggled to identify trespassers from the riots at the United States Capitol Building on January 6, 2021, they turned to a machine

---

[⊗] Jessica Gabel Cino is a Partner at Krevolin & Horst. Heather Kleider-Offutt is an Associate Professor at Georgia State University in the psychology department. Beth Stevens is a PhD student in psychology at Georgia State University. Kat Albrecht is an Assistant Professor at Georgia State University in the Andrew Young School of Policy Studies. Robert Evans is a law student at Georgia State University. Emma Riedley is a law student at Georgia State University.

for assistance.[1] After running a photograph taken from the riots through "an open source facial comparison tool," agents got a hit on their suspect from his girlfriend's public Instagram page.[2] The agents then went to his girlfriend's public Facebook page to search for individuals with the same first name in order to determine their suspect's last name, using this information to search Kentucky Driver's License records to locate his residence.[3] After surveilling their suspect at his home and place of employment, the agents engaged him in a conversation, which they recorded, where the suspect admitted to taking part in the riots on January 6.[4] In submitting their affidavit, the agents relied heavily on the identification they received from the facial recognition software, despite never identifying the software by name or providing any evidence regarding its reliability.[5]

The expansive use of facial recognition technology (FRT) in identifying suspects from the Capitol riots proves that law enforcement's use of FRT as a tool in the legal system can no longer be ignored. 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.

Law enforcement's use of FRT has been steadily increasing with little oversight from the government and a lack of a comprehensive understanding of its accuracy and potential uses.[6] Although there have been a handful of criminal cases involving identifications made by law enforcement's use of FRT, the events at the United States Capitol likely represent the largest scale use of FRT in domestic American history, bringing this problem into stark contemporaneous focus as it establishes precent for other use cases.[7] As these and other defendants identified by FRT come to court, judges will be forced to grapple with FRT's place as evidence with little guidance as to its reliability and accuracy.[8]

---

[1] Jones Aff. at 7, Apr. 16, 2021.

[2] *Id.* ("The facial recognition tool yielded results associated with the Instagram page of an individual ("Individual-1") from Kentucky who appeared to be the girlfriend of the SUBJECT. Individual-1's publicly available Instagram account contained numerous photographs of the SUBJECT who, according to the comments section of some of the posts, is named [redacted here].")

[3] *Id.* at 8.

[4] *Id.*

[5] *Id.*

[6] U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-526, FACIAL RECOGNITION TECHNOLOGY: CURRENT AND PLANNED USE BY FEDERAL AGENCIES (2021).

[7] Lynch v. State, 260 So. 3d 1166, 1169 (Fla. Dist. Ct. App. 2018); Complaint and Demand for Trial by Jury at 4–5, Parks v. McCormack, No. PAS-L-003672-20, 2020 WL 7773857 (N.J. Sup. Ct. Law Div. 2020); Complaint at 2, Williams v. City of Det., No. 2:21-cv-10827 (E.D. Mich. 2021).

[8] *Id.*

This Article seeks to outline the limitations present within FRT and argue that its current use in criminal cases is questionable due to novel algorithmic and evidentiary challenges that have not been rigorously interrogated by the court. This Article contributes to the current understanding of FRT evidentiary challenges by providing extensive analysis of its functioning and accuracy while directly comparing its treatment under the law with eyewitness identifications, a related source of evidence. This allows the analysis herein to move beyond the false dichotomy of 'scientific evidence' and 'other evidence' and instead consider a multiplicity of potential evidentiary challenges related to the use of FRT.

Part I of this Article briefly contextualizes the terrain of evidentiary challenges relevant to FRT. Part II provides an explanation of how FRT is designed and its rapid growth within law enforcement. Part III describes the current testing available to determine FRT's accuracy and its limitations. Part IV examines factors impacting FRT's accuracy rates and strategically compares FRT to eyewitness identifications, a more traditional form of criminal evidence. Part V outlines legal issues inherent to FRT's use as evidence in criminal trials compared to current use of eyewitness identifications. Part VI briefly concludes and offers policy suggestions.

I. Challenges with Criminal Evidence

On their face, requirements for the admissibility of criminal evidence seem simple.[9] To be admissible, criminal evidence must be relevant and not outweighed by other exclusionary criteria.[10] This is laid out plainly in Federal Rule of Evidence 402, which states that relevant evidence is admissible, provided it is not precluded by other Federal Rules of Evidence, the U.S. Constitution, federal statutes, or other prescriptions from the Supreme Court.[11] Evidence is relevant if it "has any tendency to make a fact more or less probable than it would be without the evidence; and [if] the fact is of consequence in determining the action."[12] Also excluded is evidence that would be overly prejudicial, confuse relevant issues, mislead the jury, or cause undue delay, weighed against the probable effectiveness of any limiting instructions.[13] This seemingly straightforward edict is, of course,

---

[9] FED. R. EVID. 402.
[10] *Id.*
[11] FED. R. EVID. 402.
[12] FED. R. EVID. 401.
[13] FED. R. EVID. 403.

then immediately complicated by the flurry of potential exclusions that interact with different types of criminal evidence in different ways.[14]

A. *Evidentiary Challenges Related to Facial Recognition Technology*

This Article does not endeavor to exhaustingly discuss all such complications; instead, it focuses on a set of admissibility exemptions and accuracy issues most relevant to FRT. This Article previews a number of these issues in order, including admissibility issues, protections under the Fourth and Sixth Amendments, and evidentiary protections under *Brady v. Maryland*.[15] The domains of these conversations are admittedly broad, but this paper also advocates for a broader understanding of the impact of FRT. Following this overview, the design and functioning of FRT will be discussed. Following this discussion, the foreshadowed legal issues and technical workings of FRT will be brought together in a targeted legal analysis comparing evidentiary issues across FRT and the more traditional, eyewitness identification to demonstrate how current evidentiary use strategies for FRT are ethically and legally questionable.

1. *Daubert* and Admissibility Issues Concerning Scientific Evidence

Federal Rule of Evidence 702 governs expert testimony and states that an expert may offer a scientific or technical opinion if: (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue; (b) the testimony is based on sufficient facts or data; (c) the testimony is the product of reliable principle and methods; and (d) the expert has reliably applied the principles and methods to the facts of the case.[16] While Rule 702 dictates expert testimony, the standard set forth in *Daubert v. Dow Pharmaceutical, Inc.* assesses the underlying reliability of scientific expert testimony.[17] The Supreme Court, in *Daubert*, intended to create a "gatekeeping" function for federal judges to determine whether evidence should be admitted by "ensuring that an expert's testimony both rests on a reliable foundation and is relevant to the task at hand."[18] In doing so, the Court noted that, although it did not intend to "set out a definitive checklist or test," some factors are to be considered, including: (1) whether the technique can be or has been tested;

---

[14] *Id.*

[15] U.S. CONST. amend. IV; U.S. CONST. amend. VI; Brady v. Maryland, 373 U.S. 83, 87 (1963).

[16] FED. R. EVID. 702.

[17] Daubert v. Merrell Dow Pharms. Inc., 509 U.S. 579, 590 (1993).

[18] *Id.* at 597.

(2) whether the technique has been subjected to peer review and publication; (3) the technique's known or ascertainable rate of error; (4) whether there are recognized standards for using the technique; and (5) whether the technique has been generally accepted in the relevant specialty fields.[19] The Court has subsequently clarified that courts may only use the *Daubert* factors that they determine to be reasonable measures of reliability in any particular case and can assign whatever weight they choose to each factor.[20] This gives judges substantial discretion in determining whether an underlying technique is reliable enough to allow in as evidence, resulting in questionable scientific testimony being admitted as evidence despite failing to satisfy each factor.[21]

A number of empirical studies of *Daubert* have been conducted in the intervening years, concluding that *Daubert* raised the bar for the admissibility of criminal evidence.[22] Other post-*Daubert* examinations agree that *Daubert* raised the bar for what scientific evidence is considered admissible but argue that it was not via the reliability factors laid specifically out in *Daubert*.[23] Instead, these scholars argue that *Daubert's* cultural education was more instructive than the actual factor-list it proscribed, calling for a list of useful criteria yet to be constructed.[24] Some remain doubtful about *Daubert,* citing some unintended consequences of the ruling, including limiting the acceptable universe of evidence, endorsing unscientific rulings, overreaching, false modesty, and sending mixed signals, among other critiques.[25] Scholars also criticize *Daubert* as effectively putting scientists on trial, with reputational damage a risk for scientists who are presenting scientific evidence to a non-expert judge.[26] Important for considering new

---

[19] *Id.* at 593–94.

[20] *Id.*; Kumho Tire Co v. Carmichael, 526 U.S. 137, 141 (1999).

[21] *Kumho Tire Co.* at 147–49.

[22] *See generally* Douglas B. Maddock, *Federal Rules of Evidence: Raising the Bar on Admissibility of Expert Testimony: Can Your Expert Make the Grade After Kumho Tire Co. v. Carmichael?*, 53 OKLA. L. REV. 507 (2000); *see generally* LLOYD DIXON & BRIAN GILL, RAND INST. FOR CIV. JUST., CHANGES IN THE STANDARDS FOR ADMITTING EXPERT EVIDENCE IN FEDERAL CIVIL CASES SINCE THE DAUBERT DECISION (2001); *see generally* Carol Krafka et al., *Judge and Attorney Experiences, Practices, and Concerns Regarding Expert Testimony in Federal Civil Trials*, 8 PSYCH., PUB. POL'Y, & L. 309 (2002).

[23] A. Leah Vickers, Daubert*, Critique and Interpretation: What Empicial Studies Tell Us About the Application of* Daubert, 40 U.S.F. L. REV. 109, 146–47 (2005).

[24] *Id.* at 147; *see also* Edward K. Cheng & Albert H. Yoon, *Does Frye or Daubert Matter? A Study of Scientific Admissibility Standards*, 91 VA. L. REV. 471 (2005) (noting that, at the state level, many states have chosen to retain a non-Daubert standard and use this differentiation as sort of a natural experiment to argue that the most influential effects of Daubert was actually its influence in creating science-skeptical judges who demanded higher quality science even if the Daubert standard was rejected in their jurisdiction).

[25] Lisa Heinzerling, *Doubting* Daubert, 14 J.L. & POL'Y 65, 65–66 (2006).

[26] George P. Lakoff, *A Cognitive Scientist Looks at* Daubert, 95 AM. J. PUB. HEALTH S114, S117 (2005).

technology like FRT are findings that courts inconsistently apply *Daubert,* including inconsistencies across what type of testimony is allowed, from whom courts accept causal arguments, and what type of testing might be required.[27] For example, scholars Fradella, O'Neill, and Fogarty describe the case of forensic handwriting experts, where some courts do not allow experts to opine if there is a match between a defendant and a sample and other courts do allow such conclusions to be made.[28]

These inconsistencies in application are particularly relevant to analyses of FRT. FRT is often largely opaque, with little information given about its accuracy or proprietary elements even when it is introduced in court.[29] It is also unclear how FRT makes use of expert testimony and whether it is required that a scientific expert empirically justify the use of the technology at all.[30] As noted above, in the affidavit for the January 6th Capitol riots, investigators relied on FRT as an investigatory tool, but did not name the specific technology or give any information about its general legal acceptability or reliability.[31]

2. Digital Search and Surveillance Under the Fourth Amendment

The Fourth Amendment provides a second salient domain of analysis.[32] The Fourth Amendment of the U.S. Constitution protects the right of the people to be secure against unreasonable search and seizure including their persons, their houses, and their effects.[33] As technology has advanced significantly, so have police surveillance and search technologies, creating new legal questions about what rights to privacy individuals actually have against such digital surveillance technologies.[34] These technologies range from video surveillance, drone surveillance, thermal imaging, environmental audio sensors, and of course, FRT.[35] This rapid expansion of surveillance technologies characterizes a shift in U.S. society more broadly to a surveillance-heavy state.[36] As these technologies have become key parts of

---

[27] Henry F. Fradella et al., *The Impact of Daubert on Forensic Science*, 31 PEPP. L. REV. 323, 359–360 (2004).

[28] *Id.* at 361.

[29] *See, e.g.*, Bertuccelli v. Universal City Studios LLC, No. 19-1304, 2020 U.S. Dist. LEXIS 195295, at *5–6 (E.D. La. Oct. 21, 2020).

[30] *Id.*

[31] Jones Aff., *supra* note 1, at 7.

[32] U.S. CONST. amend. IV.

[33] *Id.*

[34] DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE 23 (2017).

[35] *Id.* at 30, 40–41.

[36] *Id.*

criminal investigations, courts have largely left law enforcement to decide what types of surveillance devices to use and when.[37] This has led to scholarly concern that Fourth Amendment privacy protections are being eroded in the face of technological advance.[38] Scholars note that this concern becomes particularly salient as public spaces become ripe for surveillance, arguing that courts ought to protect private elements of public life which may occur in technically public spaces.[39]

There are some signs that courts endeavor to protect certain elements of privacy against surveillance technologies in the United States.[40] In *Kyllo v. United States,* the courts prevented use of thermal imaging technology in a criminal investigation on the grounds that it was not in 'general public use', employing what legal scholar Raymond Shih Ray Ku argues is a return toward stronger Fourth Amendment disruption of unreasonable search and surveillance.[41] There are also some significant regulatory decisions about criminal evidence that suggest aspirationally protecting a privacy interest.[42] Take for example, forensic genealogy. Forensic genealogy works much like its traditional genealogical counterpart except that the creation of a family tree is motivated using a search of genetic ancestry database.[43] Law enforcement searches for a relation to a DNA sample, perhaps finding a third or fourth cousin, and then uses traditional policework tactics to contact the relative and procure familial information that allows them to generate a family tree.[44] Famously, this technique was used to identify and arrest the Golden State Killer, who had evaded arrest since the 1980s.[45] Ancestry websites are arguably pseudo-public spaces, where users upload their genetic information in the hopes of it being found by unknown relatives.[46] However, this pseudo-public space is still regulated by the courts who have determined that only two repositories, FTDNA and GEDmatch, can be used for criminal investigations.[47] Notably, these repositories have added language alerting

---

[37] Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1327–28 (2002).

[38] Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. LAW. R. 1349, 1481 (2004).

[39] *Id.* at 1406–11.

[40] Ku*, supra* note 37, at 1329–30.

[41] *Id.* at 1329; Kyllo v. U.S., 533 U.S. 27, 40 (2001).

[42] Christi J. Guerrini et al., *Four Misconceptions About Investigative Genetic Genealogy,* 8 J. L. & BIOSCIENCES 1, 12 (2021).

[43] Chris Phillips, *The Golden State Killer Investigation and the Nascent Field of Forensic Genealogy*, 36 FORENSIC SCI. INT'L. GENETICS 186, 187 (2018).

[44] *Id.*

[45] *Id.* at 186.

[46] *Id.*

[47] Guerrini et al., *supra* note 42, at 8.

users that their genetic information can be used to facilitate criminal prosecutions.[48] Thus, forensic genealogy is an example of how a broadly available digital technological innovation has not been granted free reign as an investigatory tool or site of criminal evidence.

FRT poses particularly acute problems for protecting individual privacy in public spaces.[49] At present, there is no parallel form of required consent (like in forensic genealogy) safeguarding the public images of individuals when it comes to FRT.[50] The use of FRT is complicated by its potential inaccuracies and the downstream consequences of those inaccuracies.[51] There have already been at least three known cases of Black or African American men being wrongly identified by FRT, leading to wrongful arrests and detainment.[52] These wrongfully accused individuals were therefore damaged, not by any of their own actions, but rather by simply being in public spaces without privacy rights to their own images.

3. Sixth Amendment Confrontation Clause Concerns

Next, FRT can be interestingly analyzed under the Confrontation Clause.[53] The Confrontation Clause of the Sixth Amendment provides that "[i]n all criminal prosecutions, the accused shall enjoy the right…to be confronted with the witnesses against him…"[54] The Supreme Court in *Crawford* clarified that this requirement means that "[t]estimonial statements of witnesses absent from trial [can be] admitted only where the declarant is unavailable, and only where the defendant has had a prior opportunity to cross-examine," but "[left] for another day any effort to spell out a comprehensive definition of 'testimonial."[55] As a practical matter, under *Crawford*, the court must determine that the relevant evidence being offered contains a hearsay statement.[56] In *Melendez-Diaz v. Massachusetts* and

---

[48] *Id.* at 3.

[49] Blitz, *supra* note 38, at 1419.

[50] *Id.* at 1356, 1359.

[51] *See, e.g.* Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Dec. 29, 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[52] *Id.*

[53] *See* U.S. CONST. amend. VI; *see also* Gabrielle M. Haddad, *Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom*, 23 VAND. J. ENT. & TECH. L. 891 (2021).

[54] U.S. CONST. amend. VI.

[55] Crawford v. Wash., 541 U.S. 36, 59, 68 (2004).

[56] *Id.* at 40. *Crawford* identifies various examples of "the class of testimonial statements covered by the Confrontation Clause," including "affidavits, custodial examinations, prior testimony that the

Bullcoming v. New Mexico, the Supreme Court held that forensic laboratory reports that contain statements by an analyst about the results of a scientific test fall under the category of testimonial evidence that invokes *Crawford* protection.[57] The Court, in *Melendez-Diaz*, noted that the certificates created by the analysts reporting that the substance found on the defendant was in fact cocaine were "functionally identical to live, in-court testimony, doing 'precisely what a witness does on direct examination.'"[58] The Court, in *Bullcoming*, built on this requirement by holding that "[a] document created solely for an 'evidentiary purpose'... made in aid of a police investigation, ranks as testimonial" and that the person who conducted the particular test must be present to testify as to its results rather than a substitute familiar with the process.[59] The Court reasoned that a substitute analyst cannot testify to the factual circumstances surrounding any testing and reiterated its holding in *Crawford* that "the obvious reliability of a testimonial statement does not dispense with the Confrontation Clause."[60]

The Confrontation Clause poses obvious difficulties for FRT, which is still largely opaque in its application. It is not yet legally settled what rights the accused has to confront various stakeholders in the development of FRT.[61] Is the person to cross-examine the architect of the algorithm or is scrutiny simply applied to the algorithm itself? There are also relevant considerations about how this process is likely further complicated by the present opacity of proprietary technology.

4. *Brady* and Exculpatory Evidence

Finally, there exists a layer of legal analytical concerns surrounding potential *Brady* violations and FRT.[62] *Brady v. Maryland* requires the Prosecution to disclose all potential evidence that might exonerate the defendant to the Defense.[63] This evidence, called exculpatory evidence, includes any evidence favorable to the defendant, including evidence that might negate guilt, reduce a criminal sentence, or affect the credibility of a

---

defendant was unable to cross-examine, or similar pretrial statements that declarants would reasonably expect to be used prosecutorially," among others. *Id.* at 51–52.

[57] Melendez-Diaz v. Massachusetts, 557 U.S. 305, 311 (2009); Bullcoming v. New Mexico, 564 U.S. 647, 668 (2011).

[58] *Melendez-Diaz*, 557 U.S. at 310–11.

[59] *Bullcoming*, 564 U.S. at 664.

[60] *Id.* at 661 (internal citations and quotations omitted).

[61] *See* Haddad, *supra* note 53.

[62] *See* Brady v. Maryland, 373 U.S. 83 (1963); *see also* Legal Info. Inst., *Brady Rule*, CORNELL L. SCH. (Dec. 2021), https://www.law.cornell.edu/wex/brady_rule.

[63] *Brady*, 373 U.S. at 87.

witness.[64] Importantly, the defense is not required to request this information; rather, the prosecution has a constitutional duty to disclose it.[65] *Brady* obligations are not as expansive as they seem; in the case *Turner v. United States*, the Prosecution was able to avoid a *Brady* disclosure requirement on the technicality that the at-issue witness statements were immaterial.[66] Scholars contend, though, that even if *Brady* disclosures were harder to avoid, they still would not be sufficient to prevent flawed scientific evidence in criminal courts because *Brady* protections do not alleviate inequalities prior to trial and because they are limited only to materials that are favorable and material to the defense.[67]

A substantial amount of scholarly work has considered how FRT is specifically complicated under *Brady*.[68] FRT has been considered under the framework of trade secrecy, with courts often finding in favor of law enforcement protection of the FRT trade secrets in ways that threaten the due process rights of criminal defendants.[69] Prosecutors often do not introduce FRT evidence at trial, leaving defendants unable to challenge FRT evidence under *Brady* at all.[70] In recent cases, judges have rejected the requests of the defense to view other potential FRT matches (to individuals other than the defendant) on the grounds that they are neither material nor favorable to the defense.[71] These limitations to *Brady* significantly change the terrain of FRT evidence to be less favorable to the defendant, a stark difference from interpretations of defendant rights to other types of criminal evidence and *Daubert*-related protections from 'junk science'.[72]

---

[64] *See* Legal Info. Inst., *supra* note 62.

[65] Kyles v. Whitley, 514 U.S. 419, 433–34 (1995); U.S. v. Bagley, 473 U.S. 667, 674–76 (1985).

[66] Turner v. U.S., 137 S. Ct. 1885, 1895 (2017).

[67] *See* Jennifer D. Oliva & Valena E. Beety, *Discovering Forensic Fraud*, 112 NW. U. L. REV. ONLINE 1 (2017) (arguing that Brady protections would still be insufficient with the support of arguments from other scholars).

[68] *See* Rebecca D. Goldberg, *You Can See My Face, Why Can't I? Facial Recognition and Brady*, 5 HRLR ONLINE 263, 264 (2021); *see also* Jaylla Brown, *We Don't All Look the Same: Police Use of Facial Recognition and the Brady Rule*, 74 FED. COMM. L.J. 329, 332 (2022); *see also* Ari B. Rubin, *A Facial Challenge: Facial Recognition Technology and the Carpenter Doctrine*, 27 RICH. J. L. & TECH. 1, 36 (2021).

[69] Deborah Won, *The Missing Algorithm: Safeguarding Brady Against the Rise of Trade Secrecy in Policing*, 120 MICH. L. REV. 157, 157 (2021).

[70] T.J. Benedict, *The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest*, 79 WASH. & LEE L. REV. 849, 859 (2022).

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

[72] That is, the opacity of FRT and inability to interrogate it as 'junk science' seems at odds with the high bar for evidentiary admissibility endorsed under the Daubert standard as previously discussed in this Article.

B. *The Cumulative Challenges of Facial Recognition Technology*

The legal challenges aforementioned here operate not in a vacuum, but in tandem to further complicate the evidentiary use of FRT in criminal courtrooms. Each of the ruminations attached to the discussed legal domains depends on the answers to key technological and ethical questions about how FRT works. That is, to answer some of the legal questions posed in this section, it is necessary to first acquire a basic understanding of how FRT works. After understanding how the technology generally functions, it becomes possible to enumerate its potential shortcomings as it concerns reliability, proprietary knowledge, and potential axes of bias.

Still, even this enumeration is not sufficient to fully understand and contextualize the discussed legal issues. Rather, a comparison against a currently used form of criminal evidence will help elucidate and contextualize challenges inherent to the current use of FRT. By using eyewitness identifications as a foil, holes in legal protections can be more clearly seen. Notably, eyewitness identifications are not without substantial criticism themselves, allowing FRT to be compared to it in a realistic context. These Authors are not the first to consider FRT and eyewitness identifications in some sort of combination.[73] Scholar Laura Moy considers how facial recognition and eyewitness identifications might work together in ways that are harmful, setting up a useful precedent for comparison of the two evidentiary types for this analysis.[74] This Article extends the field by delving into a specific analysis of relevant comparative legal issues facing FRT and eyewitness identifications.

II. HOW FACIAL RECOGNITION TECHNOLOGY WORKS

A. *How Facial Recognition Technology Works*

To evaluate acceptable thresholds for FRT evidence, one must first have a general understanding of how FRT software works. It is beyond the scope of this paper to discuss the mechanics behind FRT software created by every company. Therefore, this analysis merely reviews how FRT technology works in general as provided by previous publications. Regardless of the

---

[73] *See generally* Laura Moy, *Algorithms and the Bill of Rights: Facing Injustice: How Face Recognition Technology May Increase the Incidence of Misidentifications and Wrongful Convictions*, 30 WM. & MARY BILL RTS. J. 337 (2021) (analyzing whether a paired use of facial recognition and eyewitness identification might increase the incidence of wrongful convictions).

[74] *Id.* at 339.

specific technology, the first threshold question should be: "are there enough pixels present to retrieve a quality reading with the technology?"

FRT software uses neural networks and artificial intelligence to form a face print from an image's pixels over three stages.[75] First, a picture is uploaded into the system and the machine analyzes the picture's quality.[76] The system determines a picture's quality by the number of pixels in the picture.[77] These pixels are essentially dots overlaying the facial image.[78] The more pixels a picture has, the higher quality the image with improved clarity.[79] Some benchmarks for reliability are offered based on pixel quantity, but these metrics vary, with one such benchmark suggesting that a picture should have a minimum of 90 pixels between the eyes before a reliable face print can be taken.[80]

The pixels are then processed by the FRT's algorithmic software called "nodes."[81] Nodes are the mechanism which will eventually determine a shape by locating the object's edges.[82] The nodes calculate where the edges are based on the number of pixels in a row.[83] The nodes may even "guess" if an edge is present depending on the picture's quality.[84] For example, three pixels in a row may represent an edge, seven in a row likely represents an edge, and ten in a row are extremely likely to be an edge.[85] These nodes overlay a subject's face and determine facial features by calculating how many pixels may represent the width of the nose or the curvature of the jaw line.[86]

Based on the second layer's edge determinations, the algorithm's third layer of nodes records the location of distinctive features and determines what the picture is or whether it matches previously uploaded pictures.[87] The third layer does this by measuring the nose, the eyes, and other relevant locations identified by the individual product's algorithm and records this

---

[75] Neural networks are a method of machine learning that trains computing systems to operate similarly to collections of neurons in the human brain. *See generally* Hervé Abdi, *A Neural Network Primer*, 2 J. OF BIOLOGICAL SYS. 247 (1994) (providing a general primer on neural networks); *see also* Curtis E.A. Karnow, *The Opinion of Machines*, 19 COLUM. SCI. & TECH. L. REV. 136, 144–45 (2017) (providing a more specific discussion of how FRT operates).

[76] Karnow, *supra* note 75, at 144.

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues,* CTR. FOR CATASTROPHE PREPAREDNESS AND RESPONSE 18 (2009).

[81] Karnow, *supra* note 75, at 144.

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] *Id.*

[87] *Id.*

information for future comparisons by taking a "face print."[88] These relevant locations have also been referred to as "landmarks."[89] Each face print is supposedly unique in that individuals with larger noses, eyebrows, or other distinctive landmarks would trigger the same nodal calculation.[90] But the software cautions its identification against a recorded face print by assigning an error rate to its output.[91]

This error rate is calculated based on the probabilistic values determined during each layer.[92] Each layer's probabilistic value comes from how much "guessing" the algorithm had to do based on different variables.[93] For example, did the software "guess" certain edges were found where only four pixels were aligned because the picture's quality was too poor? Other calculations increasing the error rate include "the viewpoint of the CCTV camera; the image distortion due to the object-to-camera distance or camera lens; the image quality; and operator subjectivity."[94] Any potential miscalculation, even at one layer, would lower the probabilistic value of the total output (the conclusion regarding one's identity) because each layer relies on the prior layer's calculations when refining its conclusions about relevant facial characteristics.[95]

1. How Law Enforcement Uses Facial Recognition Technology

There are two general categories that any given software can fall into: facial verification (1:1) and facial identification (1:N).[96] Facial verification compares an image of one person to another image of that same individual (such as unlocking a smartphone), whereas facial identification compares a photograph of a single person against a database of images to determine if there is a match.[97]

---

[88] Won-Joon Lee et al., *A Preliminary Study of the Reliability of Anatomical Facial Landmarks Used in Facial Comparison*, 64 J. FORENSIC SCI. 519, 520 (2019).

[89] *Id.* at 519.

[90] Jessica Cino, *From the Crime Scene to the Courtroom: The Future of Forensic Science Reform: Deploying the Secret Police: The Use of Algorithms in the Criminal Justice System*, 34 GA. ST. U. L. REV. 1073, 1091 (2018).

[91] Lee et al., *supra* note 88, at 521.

[92] Karnow, *supra* note 75, at 144.

[93] *Id.*

[94] Lee et al., *supra* note 88, at 519–20.

[95] Karnow, *supra* note 75, at 144.

[96] U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-518, FACE RECOGNITION TECHNOLOGY: FEDERAL LAW ENFORCEMENT AGENCIES SHOULD BETTER ASSESS PRIVACY AND OTHER RISKS 4 (2021).

[97] *Id.* at 4–5; *see also* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1113 (2021) (stating that this "involves confirming that a particular human face present before the camera matches a preset digital image of that face").

Although law enforcement typically uses a 1:N search in attempting to generate leads,[98] the full scope of how law enforcement agencies are currently using FRT is not officially available.[99] This is a marked difference from other types of law enforcement evidence technologies, like forensic genealogy, which has precise and official restrictions.[100] In the absence of any oversight, the use of FRT has proliferated through many local and at least twenty federal law enforcement agencies.[101] Law enforcement agencies adopted FRT as an "investigatory tool," which has allowed them to serve as the beta-testers for this new-age tool of identification.[102] The general framework of how FRT is used by police is the same despite the multitude of FRT programs/applications in the marketplace.[103] When a user of the software, an officer, uploads the image of a person, a witness or suspect, the software returns "matches" based on comparisons of the facial anatomy of the "target image" to those contained in the search database.[104]

B. *Factors Affecting the Accuracy of Facial Recognition Technology*

Because of the importance of a picture's quality, it is not a surprise that clear, well-lit mugshots taken by high-quality cameras provide the best specimens to retrieve and compare facial prints.[105] Altogether, this is known as the photo's environment: background, lighting conditions, camera distance, and the size and orientation of the head.[106] The more similar the

---

[98] U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 6, at 13.

[99] *See id.* at 9–10; *see also* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 96, at 11–12.

[100] *See* Guerrini et al., *supra* note 41, at 8 (explaining how FTDNA and GEDmatch are the only genetic genealogy databases that allow law enforcement to use information from their sites specifically to identify human remains and solve violent crimes. Law enforcement is still required to observe terms of service, including opt-outs. FTDNA further requires law enforcement to apply to for access).

[101] U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 6, at 1 (18 of 24 GAO-surveyed agencies reported to own their own FRT system or use that owned by another agency).

[102] Goldberg, *supra* note 68, at 265–66.

[103] *See generally* Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 2: Identification*, NAT'L INST. STANDARDS & TECH. (July 2022), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf; *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies: Hearing Before the H. Comm. on Homeland Sec.*, 116th Cong. (2019–2020) (providing an overview of facial recognition applied to mugshots and how Homeland Security uses facial recognition).

[104] *Id.*

[105] Cino, *supra* note 90, at 1092; Andrew M. Smith et al., *Mistaken Eyewitness Identification Rates Increase When Either Witnessing or Testing Conditions Get Worse*, 43 L. & HUM. BEHAV. 358, 365–66 (2019).

[106] Canon Global, *Facial Recognition Technology*, CANON (May 30, 2022), https://global.canon/en/technology/facial-recognition2022.html.

environments of the images to be compared, the better the FRT will perform.[107]

Therefore, anything affecting or concealing the face will decrease the accuracy of the face print retrieved.[108] The presence of sunglasses or hats decreases FRT's accuracy because the objects conceal critical facial characteristics.[109] FRT's output accuracy also declines significantly while face printing a "non-cooperative" target.[110] For example, someone who is walking through the airport and face printed from a side angle unknowingly would be a non-cooperative target.[111] This accuracy decrease occurs because of alignment errors as landmarks captured on CCTV at different angles are compared against the landmarks in the database samples.[112] This is concerning because most FRT evidence will presumably come from surveillance video capturing the suspect's face print without his or her knowledge. One New York Times experiment, however, was able to accurately identify a SUNY professor walking through Bryant Park via surveillance capturing mostly the top of his head and left side of his face and matching it to a faceprint retrieved from his front facing, professional portrait from the SUNY photo repository.[113] Notably, the match's similarity score (or accuracy rate) declined to 89%, perhaps because of the surveillance footage's extreme angle.[114]

Additionally, there are two not-so-obvious reasons affecting FRT's accuracy: the race or sex of the subject and the size of the database scanned for matching face prints.[115] The primary reason behind this is because FRT algorithms have not been "trained" to accurately identify minorities and women, and the algorithms are more likely to falsely identify matching characteristics when searching extensive databases.[116]

This system can train to increase the overall accuracy of its outputs in two primary ways: via human input or through input from internal

---

[107] Cino, *supra* note 90, at 1092.

[108] *Id.*

[109] *Id.* at 1091–92.

[110] *Id.* at 1092; John Nawara, *Machine Learning: Face Recognition Technology Evidence in Criminal Trials*, 49 U. LOUISVILLE L. REV. 601, 618 (2011).

[111] Nawara, *supra* note 110.

[112] Lee et al., *supra* note 88, at 519.

[113] Sahil Chinoy, *We Built an 'Unbelievable' (but Legal) Facial Recognition Machine*, N.Y. TIMES (Apr. 16, 2019), https://www.nytimes.com/interactive/2019/04/16/opinion/facial-recognition-new-york-city.html.

[114] *Id.* (failing to specify why the similarity match was only 89%).

[115] Karnow, *supra* note 75, at 182*; see also* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* PROC. MACHINE LEARNING RSCH. 81:1-15 at 1 (2018).

[116] Buolamwini & Gebru, *supra* note 115, at 2.

experiments performed by the software's artificial intelligence.[117] Training the machine through human input is a relatively straightforward process. The software analyst simply tests the machine's capabilities by uploading various images and gauging the machine's effectiveness at comparing them to the database images.[118] When the machine is correct, the analyst tells the machine so.[119] Otherwise the analyst identifies areas where the algorithm's nodal layers miscalculate before adjusting accordingly.[120] Of course, these adjustments may depend on the individual analyst's subjective accuracy where he or she programs the FRT algorithm to focus on certain facial landmarks perceived to be more reliable than others during future scans.[121] In that case, the accuracy of future matches may be unknowingly affected.[122]

FRT's accuracy also decreases as the database size increases because the FRT algorithm has more images to compare to the subject in question and the software itself automatically returns a list of candidates after sifting through potentially millions of images.[123] False positives are bound to occur as different individuals look alike and share similar facial characteristics, leaving any identifications to be made by the software's judgment.[124] In a North Carolina FRT operation, one broad sweep matched dozens of people, including a terrorism suspect, with the DMV photo of an Associated Press reporter.[125] One example illustrating the potential expanse of these FRT databases is the FBI's, which contains 30 million photos representing about 16.9 million individuals, mostly taken from mugshots.[126] Each search of the FBI's FRT database brings back between two to fifty results, even if none are a close match.[127] Because of this, the FBI advises its agents to take no enforcement action based on the photo result alone.[128]

Additionally, it may be impossible to verify that the FRT software identified the correct individual if the picture's quality is too poor to ascertain

---

[117] Karnow, *supra* note 75, at 145–47.

[118] *Id.* at 145.

[119] *Id.*

[120] *Id*.

[121] Lee et al., *supra* note 88, at 520.

[122] *Id.*

[123] Nawara, *supra* note 110, at 611; U.S. GOV'T ACCCOUNTABILITY OFF., GAO-16-267, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY 14 (2016).

[124] Nawara, *supra* note 110, at 611.

[125] *Id.* (citing Mike Baker, *FBI Uses Facial-Recognition Technology on DMV Photos*, USA TODAY (Oct. 13, 2009), http://www.usatoday.com/tech/news/2009-10-13-fbi-dmv-facial- recognition.htm).

[126] U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 123, at 10.

[127] *Id.* at 16.

[128] *Id.* at 17.

an identity with the naked eye.[129] This suggests that if human analysts compare the algorithm's results, their conclusions will be subjective at best, as it will be up to the individual analyst to agree or disagree with the algorithm's results. This opens FRT up to similar types of error and legal considerations as other types of criminal evidence that rely on expert interpretation.

III. CONCERNS ABOUT FACIAL RECOGNITION TESTING

When the FBI submitted its affidavit to secure an arrest warrant for a suspect from the Capitol riot, they only stated that they used "an open source facial comparison tool, known to provide reliable results in the past."[130] The affidavit failed to identify what facial recognition software was used and further failed to elaborate upon how the software was known to produce reliable results.[131] As a result, an identification from an unnamed and unknown software served as one of the first pieces of evidence in the case against this defendant and ultimately led to his subsequent arrest.[132] Although the affiant claimed that the software had been "known to provide reliable results in the past," the affidavit itself provides no identifying information in order to verify this claim or further investigate the software's reliability.[133] This lack of information raises serious concerns regarding the FRT that federal law enforcement agencies are using and highlights the difficulties inherent in evaluating whether any particular FRT software is reliable enough for use in the legal system. These difficulties speak directly to potential admissibility of FRT under a *Daubert* standard, implicating both ethical and legal considerations.[134] The section that follows elucidates these concerns, explaining how the proprietary nature of FRT uniquely exacerbates these concerns.

---

[129] Heather Kleider-Offutt et al., *Who is the Best Eyewitness? A Comparison of Identification Accuracy Between Human Eyewitnesses and Face Recognition Software* (2022) (unpublished manuscript) (on file with author).

[130] Jones Aff., *supra* note 1, at 7.

[131] *See id.*

[132] U.S. Attorney's Office D.C., *RANDOLPH, Stephen Chase*, U.S. DEP'T JUST. (July 28, 2021), https://www.justice.gov/usao-dc/defendants/randolph-stephen-chase (providing a list of the charges that Stephen Chase Randolph received).

[133] *See* Jones Aff., *supra* note 1, at 7.

[134] *See e.g.*, Cheng & Yoon, *supra* note 24.

A. *National Institute of Standards and Technology Facial Recognition Vendor Test*

Since 2000, the National Institute of Standards and Technology (NIST) within the Department of Commerce has tested the reliability and accuracy of submitted FRT algorithms in its Facial Recognition Vendor Test (FRVT).[135] The FRVT serves as an independent auditor to evaluate FRT and is widely regarded as the best benchmark for evaluating FRT in a variety of contexts.[136] However, the FRVT exists as a purely voluntary program that only evaluates algorithms that a developer has submitted for testing, allowing developers to opt out of any standardized evaluation for comparison against other algorithms.[137] Further, NIST officials have openly stated that they would oppose any effort to make its current evaluation scheme mandatory as it would "adversely affect the dynamic of their ongoing testing and be inconsistent with NIST's independent nonregulatory mission."[138] Given NIST's statutory requirement to emphasize standards developed by private organizations as opposed to creating any mandatory benchmark standards themselves,[139] it is difficult to imagine the FRVT as a regulatory mechanism that requires commercial FRT to meet certain standards for accuracy and reliability.

Additionally, although the FRVT is viewed as the gold standard for evaluating FRT, the datasets used in its testing fail to represent the variety of situations and contexts in which FRT is used in reality.[140] High accuracy rates

---

[135] The FRVT includes multiple projects that rank algorithms based on their performance in facial identification (1:N) and facial verification (1:1). The FRVT also evaluates the effect of various demographic variables and image quality on an algorithm's performance. Recently, the FRVT has also begun evaluating algorithms' accuracy with face masks following the COVID-19 pandemic. *See generally* Grother et al., *supra* note 102 (highlighting the numerous FRVT tests conducted by NIST).

[136] Business Wire, *NEC's Face Recognition Technology Ranks First in NIST Testing for Third Consecutive Time*, BUSINESS WIRE (June 15, 2014), https://www.businesswire.com/news/home/20140715006057/en/NECs-Face-Recognition-Technology-Ranks-First-in-NIST-Testing-for-Third-Consecutive-Time.

[137] Grother et al., *supra* note 103.

[138] U.S. GOV'T ACCCOUNTABILITY OFF., GAO-20-522, FACIAL RECOGNITION TECHNOLOGY: PRIVACY AND ACCURACY ISSUES RELATED TO COMMERCIAL USES (2020); CONG. RSCH. SERV., R46586, FEDERAL LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECHNOLOGY (2020) (noting that "[u]nder the National Technology Transfer and Advancement Act of 1995 (P.L. 104-113) and OMB Circular A-119, NIST is charged with promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities, encouraging and coordinating federal agency use of voluntary consensus standards in lieu of government-unique standards, and coordinating federal agency participation in the development of relevant standards." (internal citations omitted)).

[139] 15 U.S.C. § 272(b).

[140] Daniel E. Ho et al., *Evaluating Facial Recognition Technology: A Protocol For Performance Assessment In New Domains*, 98 DENV. L. REV. 753, 770 (2021).

in FRVT testing tend to reflect the quality of photographs used, and when lower quality images are used, NIST reports that accuracy rates can drop over 20% even in the most accurate algorithms.[141] A report produced by police chiefs in major cities cites this as a concern that law enforcement agencies should consider when determining which FRT to purchase for their departments, noting that the FRVT's test images are only minimally comparable to what is used during an investigation, and that the most similar comparison does not allow for accurate testing of demographic variation.[142] The FRVT accuracy rates also fail to consider where law enforcement agents may manipulate the process in any way, such as using an artist's forensic sketch or replacing specific facial features in a probe photograph with features of an entirely different person to more closely resemble the structure of mugshot pictures.[143] Despite NIST explicitly stating that sketch images yield poor results and multiple police departments themselves finding that the composite or edited photographs produced "unsuccessful results," these departments still allow officers to utilize manipulated images when using FRT to attempt to identify a suspect.[144]

Because the FRVT involves multiple ongoing projects that publish several updates each year, there is also an increased difficulty in interpreting what exactly it means when a developer markets its algorithm as having received a top ranking.[145] The reports themselves frequently include hundreds of pages of graphs and charts and speak in complicated, technical language, and NIST itself specifically notes that these reports are intended for individuals "who have some familiarity with biometric applications."[146]

---

[141] Grother et al., *supra* note 103, at 6.

[142] Major Cities Chiefs Ass'n, *Facial Recognition Technology in Modern Policing: Recommendations and Considerations* (2021), https://majorcitieschiefs.com/wp-content/uploads/2021/10/MCCA-FRT-in-Modern-Policing-Final.pdf.

[143] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. L. CTR. ON PRIV. & TECH. (May 16, 2019), https://www.flawedfacedata.com/ (detailing how NYPD officers used a variety of techniques to replace facial features in probe photos, including combining the photographs of two different people to create a single probe image "to locate a match to one of the people in the combined photograph").

[144] Patrick Grother & Mei Ngan, *Face Recognition Vendor Test (FRVT): Performance of Face Identification Algorithms,* NAT'L INST. STANDARDS & TECH. 4 (May 26, 2014), https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8009.pdf (noting that the accuracy rates from FRVT testing of sketch images was much higher than those found in a study by Michigan State University, likely because the FRVT sketch images were drawn by an artist viewing the mugshot, while the sketches used in the Michigan State University study were created based on an eyewitness description of the subject, which is much more similar to actual use by law enforcement during an investigation).

[145] *See id.* at 6.

[146] Grother et al., *supra* note 103, at 12 (specifically, the FRVT notes that its report "is intended for developers, integrators, end users, policy makers, and others who have some familiarity with biometrics

Law enforcement agencies are encouraged to conduct "market research" on the algorithm's accuracy prior to purchasing any FRT, but even minimal research requires a baseline knowledge of how FRT works and how to properly evaluate an algorithm's accuracy within FRVT reports, according to NIST's own reports.[147] Further, because the FRVT publishes so many reports each year that include multiple areas of rankings, several developers can claim a top ranking if their algorithm scores highly in any single test, even if this test condition does not relate to their product's marketed use.[148] For example, Clearview AI, one of the best-known FRT companies in the United States, boasted its top ranking as an "unmistakable validation of [its] industry leading facial recognition platform," despite the fact that this ranking stemmed from a testing of its 1:1 algorithm and not the 1:N algorithm that it marketed to law enforcement for use in identifying suspects.[149]

---

applications. The methods and metrics documented here will be of interest to organizations engaged in tests of face recognition algorithms").

[147] Major Cities Chiefs Ass'n, *supra* note 142, at 16.

[148] NEC Corp., *NEC Face Recognition Technology Ranks First in NIST Accuracy Testing*, NEC (Aug. 23, 2021), https://www.nec.com/en/press/202108/global_20210823_01.html ("NEC Corporation today announced that its face recognition technology ranked first in the world in the most recent face recognition technology benchmarking test conducted by the globally authoritative U.S. National Institute of Standards and Technology"); *see also* IDEMIA Nat'l Sec. Solutions, *IDEMIA's Facial Recognition Algorithm Maintains #1 Ranking in NIST's FRVT Test*, PR NEWSWIRE (Aug. 2, 2021), https://www.prnewswire.com/news-releases/idemias-facial-recognition-algorithm-maintains-1-ranking-in-nists-frvt-test-301345105.html ("IDEMIA National Security Solutions (NSS), an affiliate of IDEMIA, the world's leading biometric and identity solutions provider, announced today that the company's facial recognition algorithm 1:N has maintained the top spot on the National Institute of Standards and Technology's (NIST) Face Recognition Vender Test (FRVT) . . ."); *see also* Paravision, *Paravision's Face Recognition Ranks as the Most Accurate in the World in Latest NIST FRVT 1:N Report*, GLOBENEWSWIRE (Jan. 21, 2022), https://www.globenewswire.com/news-release/2022/01/21/2371047/0/en/Paravision-s-Face-Recognition-Ranks-as-the-Most-Accurate-in-the-World-in-Latest-NIST-FRVT-1-N-Report.html ("Paravision, the U.S.-based leader in mission-critical computer vision, today announced that it has ranked as the most accurate face recognition vendor in the world in NIST's January 2022 1:N FRVT Report"); *see also Rank One Stands Alone with Top-Tier Performance in NIST FRVT Ongoing Benchmark*, RANK ONE COMPUTING (Aug. 26, 2020), https://rankone.io/2020/08/26/rank-one-stands-alone-with-top-tier-performance-in-nist-frvt-ongoing-benchmark/; *see also Consecutive NIST Tests Confirm Superiority of Clearview AI's Facial Recognition Platform*, CLEARVIEW.AI (Nov. 24, 2021), https://www.clearview.ai/press-release-consecutive-nist-tests-confirm-superiority-of-clearview-ai-facial-recognition ("After ranking No. 1 in the U.S. across all categories in an October 2021 one-to-one (1:1) Facial Recognition Vendor Test (FRVT), Clearview AI again achieved top ranks on the crucial one-to-many (1:N) test").

[149] Kashmir Hill, *Clearview AI Finally Takes Part in a Federal Accuracy Test*, N.Y. TIMES (Oct. 28, 2021), https://www.nytimes.com/2021/10/28/technology/clearview-ai-test.html ("the test that Clearview took reveals how accurate its algorithm is at correctly matching two different photos of the same person, not how accurate it is at finding a match for an unknown face in a database of 10 billion of them"); *see also* Business Wire, *Clearview AI's Facial Recognition Platform Achieves Superior Accuracy and Reliability Across All Demographics in NIST Testing*, BUSINESS WIRE (Nov. 1, 2021, 6:00 AM),

B. *Proprietary Algorithms and Data*

However, because the FRVT operates as purely voluntary, numerous FRT developers have never submitted their algorithms for testing despite selling them to law enforcement for use.[150] Clearview AI submitted its 1:N algorithm for testing for the first time in November 2021, after it had already been selling its software to both state and federal law enforcement agencies since 2017.[151] Similarly, Amazon sold its FRT "Rekognition" software to law enforcement agencies before ever submitting it for FRVT analysis to compare its reliability to its competitors.[152] With no third-party auditing, the majority of information available regarding an algorithm's accuracy comes from the developers themselves, who have an inherent interest in marketing the algorithm to sound as accurate as possible to entice consumers to purchase it.[153] Although there have been independent research studies comparing the accuracy and reliability of various FRT algorithms, most of these studies do not identify which companies they are evaluating, increasing the difficulty in learning about algorithms that are not submitted for FRVT testing.[154]

---

https://www.businesswire.com/news/home/20211101005283/en/Clearview-AI's-Facial-Recognition-Platform-Achieves-Superior-Accuracy-and-Reliability-Across-All-Demographics-in-NIST-Testing.

[150] Khari Johnson, *Amazon Imposes One-Year Moratorium on Police Use of Its Facial Recognition Technology*, VENTUREBEAT (June 10, 2020, 3:12 PM), https://venturebeat.com/2020/06/10/amazon-imposes-one-year-moratorium-on-police-use-of-its-facial-recognition-technology/.

[151] Grother et al., *supra* note 103, at 2; *see also* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[152] Johnson, *supra* note 150.

[153] Amazon Web Services, *Amazon Rekognition Improves Accuracy of Real-Time Face Recognition and Verification*, AMAZON (Apr. 2, 2018), https://aws.amazon.com/about-aws/whats-new/2018/04/amazon-rekognition-improves-accuracy-of-real-time-face-recognition-and-verification/ ("With Amazon Rekognition, you can also perform real-time search against tens of millions of faces. With this update, Amazon Rekognition is now up to 25% more accurate in picking out the right face from a digital gallery containing millions of faces." This provides no insight into the software's overall accuracy ratings).

[154] *See* John Howard et al., *An Investigation of High-Throughput Biometric Systems: Results of the 2018 Department of Homeland Security Biometric Technology Rally*, 2018 IEEE 9TH INT'L CONF. ON BIOMETRICS THEORY (2018), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8698547; *see also* Jacqueline Cavazos et al., *Accuracy Comparison Across Face Recognition Algorithms: Where Are We on Measuring Race Bias?,* 3 IEEE TRANS. BIOM, BEHAV. IDENTITY SCI. 101 (2020), https://www.semanticscholar.org/reader/75a409677a7f6b5cac9fe237e32cc3d3e2efd031; *see also* Krishnapriya K.S. et al., *Characterizing the Variability in Face Recognition Accuracy Relative to Race*, PROC. IEEE/CVF CONF. ON COMPUT. VISION & PATTERN RECOGNITION WORKSHOPS (2019), https://openaccess.thecvf.com/content_CVPRW_2019/papers/BEFA/S_Characterizing_the_Variability_in_Face_Recognition_Accuracy_Relative_to_Race_CVPRW_2019_paper.pdf.

As a result of the difficulties in determining an algorithm's accuracy, much of the recent outcry over FRT use has come from outside of law enforcement use. Various companies have come under fire recently related to the reliability of their FRT and allegations of racism in their underlying algorithms.[155] In 2015, Google issued an apology after an African American user found that his Google Photos app had tagged a picture of himself and a friend with the word "Gorillas."[156] Despite its earlier insistence that minorities would not be disproportionately impacted by the use of FRT, in June 2020, Microsoft enacted a ban on the sale of its FRT software to U.S. police departments.[157] This occurred during the aftermath of the death of George Floyd, following an outpouring of concerns that FRT might be used unfairly against protestors and further exacerbated by criticisms related to the accuracy of FRT when used on minorities.[158]

IV. COMPARING FACIAL RECOGNITION TECHNOLOGY TO EYEWITNESS IDENTIFICATIONS

FRT has been suggested as being advantageous over human eyewitnesses in "identify[ing] the guilty with greater accuracy and exonerate[ing] the innocent."[159] However, this Article argues that such a statement is an optimistic oversimplification that does not fully account for the ethical and legal concerns inherent in FRT use. Here, it is useful to engage in an extended analysis, further differentiating FRT from other types of evidence technologies that operate more similarly to traditional policework, by actually comparing FRT to the traditional alternative of eyewitness identification on multiple vectors including bias and recall issues, how both tools are utilized by law enforcement, and by conducting empirical tests of both methods of identification. Such a comparison is not entirely without precedent, as scholars have put eyewitness identification and FRT in

---

[155] Cade Metz & Natasha Singer, *A. I. Experts Question Amazon's Facial-Recognition Technology*, N.Y. TIMES (Apr. 3, 2019), https://www.nytimes.com/2019/04/03/technology/amazon-facial-recognition-technology.html?searchResultPosition=31.

[156] Jethro Mullen, *Google Rushes to Fix Software that Tagged Photo with Racial Slur*, CNN (July 2, 2015), https://www.cnn.com/2015/07/02/tech/google-image-recognition-gorillas-tag/index.html.

[157] Jay Greene, *Microsoft Won't Sell Police its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM*, WASH. POST (June 11, 2020), https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/.

[158] *Id.*

[159] William J. Bratton, *Face Recognition is Not the Enemy*, N.Y. DAILY NEWS (Jan. 26, 2020, 5:00 AM), https://www.nydailynews.com/opinion/ny-oped-face-recognition-is-not-the-enemy-20200126-pjz4z367bvgfhaws465je5o52m-story.html.

conversation before in an effort to analyze the likelihood of increased incidence of wrongful convictions through a pairing of both technologies.[160] Here, we do not focus our analysis necessarily on a co-use of the evidentiary tools; rather, we consider how they compare with each other.

A. *Bias and Recall in Facial Recognition Technology and Eyewitness Identifications*

Problems with eyewitness identification are well documented, prompting experts to argue that eyewitness identifications justify more scrutiny even than other types of eyewitness evidence.[161] The Supreme Court established a reliability test for eyewitness identification in *Manson v. Braithwaite* in 1977, which remains substantially unchanged today, but it has not been sufficient to prevent wrongful convictions related to eyewitness misidentifications.[162] The availability of DNA testing has led to over 375 overturned convictions, 69% of them involving eyewitness misidentification, making mistaken identifications the leading cause of wrongful convictions.[163]

Scientists find that mistaken eyewitness identifications are caused by numerous factors, among them lighting, viewing distance, fear, distress, recall, cross-race identification, and other internal states including personal biases.[164] These variables have been classified broadly as estimator variables or system variables, the former characterizing environmental conditions and internal states of the observer and the latter referring to the process by which the identification lineup is conducted.[165] Additionally, studies find that both worsening witnessing and testing (police lineup) conditions can lower the standards used by individuals to make an affirmative identification.[166] In

---

[160] *See generally* Moy, *supra* note 73, at 365–66.

[161] Suedabeh Walker, *Drawing on Daubert: Bringing Reliability to the Forefront in the Admissibility of Eyewitness Identification Testimony*, 62 EMORY L.J. 1205, 1224 (2013).

[162] *See generally* Manson v. Braithwaite, 432 U.S. 98 (1977); *see also* Gary Wells & Deah Quinlivan, *Suggestive Eyewitness Identification Procedures and the Supreme Court's Reliability Test in Light of Eyewitness Science*: *30 Years Later*, 33 LAW HUM. BEHAV. 1, 1 (2009).

[163] Innocence Project, *Eyewitness Identification Reform*, CARDOZO SCH. L., YESHIVA UNIV. (last visited Oct. 3, 2022), https://innocenceproject.org/eyewitness-identification-reform/.

[164] SHARI R. BERKOWITZ, & ELISABETH F. LOFTUS, FINDING THE TRUTH IN THE COURTROOM: DEALING WITH DECEPTION, LIES, AND MEMORIES 11–20 (Henry Otgaar & Mark L. Howe eds., 2018); s*ee* John T. Wixted et al., *Models of Lineup Memory*, 105 COGNITIVE PSYCH. 81 (2018); s*ee generally* Smith et al., *supra* note 105*; see generally* John T. Wixted et al., *Rethinking the Reliability of Eyewitness Memory*, 13 PERSP. ON PSYCH. SCI. 324 (2018) (discussing the importance of cross-race identification, viewing distance, clarity, and lighting).

[165] *See* Gary L. Wells, *Applied Eyewitness-Testimony Research: System Variables and Estimator Variables*, 36 J. PERS. SOC. PSYCH. 1546 (1978).

[166] Smith et al., *supra* note 105, at 367.

2014, the National Academy of Sciences convened an expert panel to study eyewitness identification, producing a best practices report.[167] Since then, 19 states have passed reforms to eyewitness identification procedures, though 31 states have yet to undertake major reforms.[168] The result is a cornerstone of criminal prosecution that we know is plagued by bias and inaccuracy precisely when the stakes are the highest.

In contrast to the seemingly humanly fallible eyewitness identification, FRT software machine learns through internal tests, adapts, and corrects itself.[169] The machine tests itself against previously uploaded and labeled images, observing whether it identifies the correct subject during comparison.[170] Despite this mechanization, FRT is unfortunately no more insulated against bias than eyewitness identification.[171] The problem with machine learning is that when the algorithm corrects itself based only on the controlled database filled with previously uploaded pictures, it becomes dependent on certain facial landmarks shown in those pictures.[172] For example, research has noted that FRT algorithms are consistently less accurate on women, African Americans and younger people because they were trained with databases that were disproportionately white males.[173]

Scholars assert that racial differences and differing facial structures create this inconsistency.[174] A white person's face may have different distinguishing characteristics than an African American person's face, yet the algorithm will try to create a face print on the African American male's face using the same unique identifying features of a white male's face.[175] Two researchers noted the maximum error rate when comparing photos of white males under prime conditions using three commercial FRT products was 0.8%.[176] This maximum error rate rose to 8% when shown white females and up to 12% for darker-skinned males.[177] Distressingly, the algorithm's error

---

[167] Thomas D. Albright & Jed S. Rakoff, *The Impact of the National Academy of Sciences Report on Eyewitness Identification*, 104 JUDICATURE 20, 21 (2020), https://judicature.duke.edu/wp-content/uploads/2020/04/RAKOFF-NEW.pdf.

[168] *Id.* at 26–27.

[169] Karnow, *supra* note 75, at 145–46.

[170] *Id.*

[171] *Id.*

[172] *Id.*

[173] Brendan Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 IEEE TRANSACTIONS ON INFO. FORENSICS & SEC. 1789, 1797–98 (2012).

[174] *Id.*

[175] *Id*.; *see also* Buolamwini & Gebru, *supra* note 115.

[176] Buolamwini & Gebru, *supra* note 115, at 1, 8.

[177] *Id.* at 8.

rate rises to nearly 35% when comparing images of darker-skinned women.[178]

Microsoft recently announced that they have made marked improvements in FRT error rates for women and minorities by making three changes to their specific FRT software: Microsoft's team stated that they expanded and revised algorithm training and benchmark datasets to include more minorities; launched new data collection efforts to further improve the training data by focusing specifically on skin tone, gender, and age; and improved the classifier to produce higher precision results.[179] These changes would appear to address the lack of minorities and women in the control database that the algorithm trains itself with, and allegedly reduce error rates for darker-skinned men and women by twenty times and reduce error rates for all women by nine times.[180]

Reduction in error rates has high stakes implications for the use of FRT in criminal prosecutions.[181] The legal community should pay special attention to Microsoft's alleged reduction of error rates for minorities, considering their contract with the U.S. Immigration and Customs Enforcement (ICE) to provide FRT software to help investigate travelers at the U.S. border and airports.[182] Despite the earlier insistence that minorities would not be disproportionately impacted by the use of FRT, in June 2020, Microsoft enacted a ban on the sale of its FRT software to U.S. police departments.[183] This occurred during the aftermath of the death of George Floyd in police custody and the ensuing protests, following an outpouring of concerns that FRT might be used unfairly against protestors, exacerbated by criticisms related to the accuracy of FRT when used on minorities.[184]

---

[178] *Id.* at 1, 8.

[179] John Roach, *Microsoft Improves Facial Recognition Technology to Perform Well Across All Skin Tones, Genders*, MICROSOFT (June 26, 2018), https://blogs.microsoft.com/ai/gender-skin-tone-facial-recognition-improvement/?utm_source=social-share.

[180] *Id.*

[181] Drew Harwell, *Facial Recognition Technology is Finally More Accurate in Identifying People of Color. Could That Be Used Against Immigrants?,* WASH. POST (June 28, 2018, 9:56 AM), https://www.washingtonpost.com/technology/2018/06/28/facial-recognition-technology-is-finally-more-accurate-identifying-people-color-could-that-be-used-against-immigrants/?noredirect=on&utm_term=.aa163f24f8da.

[182] *Id.*

[183] Jeffrey Dastin & Munsif Vengattil, *Microsoft Bans Face-Recognition Sales to Police as Big Tech Reacts to Protests*, REUTERS (June 11, 2020, 1:26 PM), https://www.reuters.com/article/us-microsoft-facial-recognition/microsoft-bans-face-recognition-sales-to-police-as-big-tech-reacts-to-protests-idUSKBN23I2T6.

[184] *Id*.

B. *Law Enforcement Use of Eyewitness Identifications vs. Facial Recognition Technologies*

Many factors contribute to whether a witness will accurately remember or misremember event information, including perpetrators, and these factors can influence memory both during event/crime encoding and event retrieval (e.g., police questioning and lineup procedures).[185] Studies focused on defining factors that contribute to eyewitness memory error find that the context of the event and whether the witness accurately recorded event details into memory is unchangeable (i.e., estimator variables); however, procedures to query the witness subsequent to the event are within the purview of law enforcement (i.e., systems variables) and thus influence the reliability of identification evidence.[186]

Human memory has well-established vulnerabilities, such as fading over time, incorporation of misinformation, confusion over source of information, and memory loss due to distraction, to name a few.[187] However, memory also processes efficiently and updates with new information; additionally, typically important central facts are remembered while peripheral details are forgotten, and people will often know that information is familiar.[188] Although human memory performs well for everyday functioning and remembering important information, its updatable nature fails to be advantageous for recalling specific details or people from a crime scene, especially when stress and emotions are high.[189] Thus, the requirements of an eyewitness stretch this system outside of its normal demands. Recognizing this difficulty, scientific research has culminated in a set of recommendations for best practices in attempts to preserve the integrity of an eyewitness' memory, focusing primarily on law enforcement procedures.[190] Eyewitnesses do correctly identify perpetrators, but memory is not infallible. The questions become: how much error is tolerable and where does that leave law enforcement when trying to identify a perpetrator?

---

[185] Wixted et al., *supra* note 164 (discussing the importance of cross-race identification, viewing distance, clarity, and lighting); Berkowitz & Loftus, *supra* note 164, at 11–20; *see generally* Smith et al., *supra* note 104.

[186] *See* Smith et al., *supra* note 105.

[187] Kleider-Offutt et al., *supra* note 129, at 3.

[188] *Id.*

[189] *Id.*

[190] Gary Wells et al., *Policy and Procedure Recommendations for the Collection and Preservation of Eyewitness Identification Evidence,* 44 L. & HUM. BEHAV. 3 (2020).

C. *Is FRT Better than Eyewitness Identification?*

Amidst the uncertainty surrounding reliability in FRT systems, are these systems superior to human eyewitnesses for correct identification? If so, is FRT superior in all situations, or are there contexts where FRT identifications remain susceptible to the same errors that present themselves in human eyewitness performance? Unlike human eyewitnesses, the post-event factors (e.g., poor law enforcement interviewing) that contaminate memory will not influence computer-based identification systems, suggesting that FRT could potentially avoid some foibles of the human memory system.[191] However, what about the errors that occur as a result of poor encoding of an event? The difficulties human eyewitnesses encounter, such as lighting, time of day, distance from the perpetrator, and ethnicity of the perpetrator, remain relevant factors for FRT systems.[192] As with variability in human eyewitness abilities (i.e., age, cognitive abilities, response to stress), FRT systems will vary by algorithm as well.[193] Law enforcement agencies currently use a variety of systems, although the reliability of the software is oftentimes proprietary and unreported, resulting in the potential use of algorithms with questionable accuracy rates.[194] In a real criminal case, the ground truth of who committed the crime remains unknown, making it impossible to verify the accuracy of a system's identification, and highlighting the complexities of using FRT in real time.

1. An Empirical Test of FRT vs. Eyewitnesses Identification

To directly test FRT compared to eyewitness performance, the Authors conducted a research study using several crime videos with videos of varying quality and with perpetrators of different ethnicities.[195] 121 participants of a diverse population served as eyewitnesses to watch the crime videos and try to identify the perpetrator from a six-pack line up.[196] In addition, the same task was performed using a highly rated, but proprietary, FRT software using still-frames from the crime videos of the suspect as the probe image to

---

[191] *Id.*

[192] Kleider-Offutt et al., *supra* note 129.

[193] *Id.* at 5.

[194] Rachel S. Fleischer, *Bias in, Bias out: Why Legislation Placing Requirements on the Procurement of Commercialized Facial Recognition Technology Must Be Passed to Protect People of Color*, 50 PUB. CONT. L.J. 63 (2020).

[195] Kleider-Offutt et al., *supra* note 129.

[196] *Id.* at 10.

compare to the lineup faces.[197] When comparing the probe image to the lineup faces, the software provides a "similarity score" for each of the lineup faces.[198]

This score indicates how similar the lineup face is to the probe image.[199] A "perfect" score of 1.0 is the closest to what might be termed a "match" (setting aside that such a finding is not a legal term).[200] A score of 0.2 means that two faces are just as much alike as they are unalike.[201] Every 0.1 increase above 0.2 is 1 standard deviation closer to that perfect score.[202] It is important to note that after the software provides the similarity scores for a series' faces, it is then up to a facial recognition examiner (i.e., the person conducting the search), to determine which–if any–faces are a match to the perpetrator, which, of course, injects the prospect of human error (and associated biases) into the equation.[203]

Results from the study showed that the FRT system was superior to the eyewitness in all but two crime scenarios wherein the videos' quality was poor.[204] In a follow-up study, the probe images from the original videos were compared to a larger, publicly available database of 100,000 faces.[205] The FRT system made similar perpetrator identifications in all but one video condition–an unclear video condition.[206] In this single condition, the software returned seven faces that were considered a better match to the probe image than the actual perpetrator.[207] This indicates that the FRT software is superior to human eyewitnesses, but when presented with a larger database of faces and varying video quality, the software has limitations. Moreover, the decision of whether one of the eight matches is the perpetrator, is left to the recognition examiner (i.e., the person conducting the search).[208]

---

[197] *Id.* at 12–13.
[198] *Id.* at 16.
[199] *Id.*
[200] *Id.*
[201] *Id.* at 19.
[202] *Id.*
[203] *Id.* at 30.
[204] *Id.* at 21.
[205] *Id.* at 27–28.
[206] *Id.* at 28.
[207] *Id.*
[208] *Id*.

V. FACIAL RECOGNITION TECHNOLOGY AND EYEWITNESS TESTIMONY IN COURTS

A. Comparing Eyewitness Identification and Facial Recognition Technologies

The experiment conducted by Authors Kleider-Offutt, Stevens, and Cino suggests that FRT performs better than eyewitness identifications in most cases, though it is measurably imperfect.[209] However, simply substituting FRT for eyewitness identifications is not scientifically or legally straightforward.[210] The sections that follow expand on this comparison while emphasizing the novel legal considerations of FRT. Mirroring the legal considerations examined at the opening of this Article, FRT and eyewitness identifications are discussed specifically in four key domains: *Daubert* and admissibility issues, Fourth Amendment considerations, Sixth Amendment considerations, and potential *Brady* violations. In doing so, this Article not only analyzes potential evidentiary issues with FRT, but also places them in conversation with a current evidentiary standard for identification—identifying relative strengths or weaknesses of FRT by comparison.[211]

1. *Daubert* and Admissibility Issues in Eyewitness Identification vs. FRT

Some jurisdictions allow expert witnesses to testify about the unreliability of eyewitness identification, but others do not, arguing that eyewitness identification is within the purview of jury understanding.[212] However, studies show that juries are generally overly inclined to trust eyewitnesses and consequently ascribe more certainty to their identifications ultimately leading to wrongful convictions.[213] Scholar Peter Cohen argues that this reality is precisely why expert testimony should be allowed regarding eyewitness identification, writing, "it is not unreasonable,

---

[209] *Id.* at 29.

[210] *Id*.

[211] Note that this comparison is in no way intended to serve as a comprehensive analysis of evidentiary concerns facing eyewitness identification. The comparison here should be understood as motivated uni-directionally to compare the salient challenges facing FRT to eyewitness identification, rather than the other way around.

[212] Walker, *supra* note 161, at 1223.

[213] Jennifer L. Overbeck, *Beyond Admissibility: A Practical Look at the Use of Eyewitness Expert Testimony in the Federal Courts*, 80 N.Y.U. L. REV. 1895, 1895 (2005).

therefore, to allow expert testimony regarding eyewitness identification just as would occur were the evidence a 'novel' and impersonal DNA match rather than the witness's classic declaration: 'That's the one!'"[214] This view is endorsed by studies that find that expert testimony of eyewitness identification does not confuse or prejudice the jury against the evidence, sometimes even finding the opposite with benefits to the prosecution.[215] Importantly, comparing eyewitness identification and FRT on *Daubert* is comparing two slightly different issues. As it concerns eyewitness identification, the issue is whether or not expert testimony on the reliability of eyewitness identification should be allowed, not whether eyewitness identification itself as a category is admissible.[216] FRT, in contrast, is itself a technological tool that may or not clear *Daubert* factors.[217]

As it presently stands, there is conflict among legal scholars regarding FRT's admissibility under *Daubert.*[218] On an analysis of *Daubert* factors (which are notably factors, rather than elements), FRT may have difficultly passing some of them, not because it theoretically could not, but rather because it has not yet.[219] An example is testability, which is theoretically perfectly possible for FRT, but which has not yet been systematized with rigor.[220] Similarly, peer review and publication is a reality for FRT, but with limits on transparency due to proprietary algorithms, there are questions about the level of academic scrutiny actually applied to FRT en masse.[221] Both error rates and standards are difficult to quantify with FRT, as error rates are opaque and standards are not developed.[222] The final *Daubert* factor, general acceptance, is more nebulous. FRT evidence has been included in criminal investigations and in court, but it has also been party to substantial criticism throughout its brief tenure.[223] One reading of the culmination of these factors is that they likely prevent admissibility under *Daubert*.[224] However, other readings of those same factors conclude exactly

---

[214] Peter J. Cohen, *How Shall They Be Known? Daubert v. Merrell Dow Pharmaceuticals and Eyewitness Identification*, 16 PACE L. REV. 237, 280 (1996).

[215] Steven D. Penrod et al., *Expert Psychological Testimony on Eyewitness Reliability Before and After* Daubert*: The State of the Law and the Science*, 13 BEHAV. SCI. & L. 229, 254 (1995).

[216] *Id.* at 244.

[217] *See* Haddad, *supra* note 53, at 908.

[218] *Id.* (arguing that FRT does not meet *Daubert* muster to be admitted as evidence); Nawara, *supra* note 110, at 621 (concluding that FRT is acceptable under both *Frye* and *Daubert* due to its reliability, relevancy, and general acceptance in the scientific community).

[219] Haddad, *supra* note 53, at 902.

[220] *Id.* at 905.

[221] *Id.* at 906.

[222] *Id.* at 906–07.

[223] *Id.* at 897, 904–05.

[224] *Id.* at 908.

the opposite, noting that every factor need not be entirely satisfied.[225] For purposes of highlighting potential legal issues, FRT is unlikely to consistently pass *Daubert* factor scrutiny, though inconsistent application of *Daubert* standards across courts pose a threat to this assertion.[226]

2. Fourth Amendment Digital Search Surveillance in Eyewitness Identifications vs. Facial Recognition Technology

In general, the Fourth Amendment has fewer eyewitness identification applications, particularly applications relevant to the core issue of digital surveillance discussed here.[227] The applications that do exist generally focus on analysis of identification line-ups.[228] In *U.S. v. Dionisio*, the Supreme Court held that viewing a face in a lineup is not a search as defined by the Fourth Amendment.[229] However, courts have found that the police need to have at least reasonable suspicion that an individual is involved in a crime to bring a non-distractor into a lineup, here invoking Fourth Amendment protections against seizure of individuals by law enforcement.[230] Even so, scholars have argued that Fourth Amendment analyses of lineups fill gaps left by insufficient due process analyses such that suggestive lineups could be removed as unreasonable seizures, regardless of their correctness.[231]

The Fourth Amendment concern is perhaps where FRT seems most significantly more perilous compared to current methodologies of eyewitness identification. Scholars are generally pessimistic about the lack of protections for individuals against biometric and digital surveillance under the Fourth Amendment, despite what they see as clear constitutional grounds to reject such searches.[232] That is not to say that there are no possible pathways for limits on FRT via the Fourth Amendment. Scholars distinguish between types of FRT available to law enforcement in analyzing possible Fourth Amendment protections.[233] Face surveillance is mass surveillance of people

---

[225] Nawara, *supra* note 110, at 606.

[226] *See generally* Fradella et al., *supra* note 27 (discussing various inconsistencies in *Daubert* applications).

[227] Sarah Anne Mourer, *Reforming Eyewitness Identification Procedures Under the Fourth Amendment,* 3 DUKE J. CON. L. & PUB. POL. 49, 51 (2008).

[228] *Id.*

[229] U.S. v. Dionisio, 410 U.S. 1, 14 (1973).

[230] *See* Hayes v. Florida, 470 U.S. 811, 816 (1985); Davis v. Mississippi, 394 U.S. 721, 724 (1969).

[231] Mourer, *supra* note 227, at 88.

[232] *See* Matthew Doktor, *Facial Recognition and the Fourth Amendment in the Wake of* Carpenter v. United States, 89 U. CIN. L. REV. 552, 573 (2021) (where the Author writes that "there is not a single viable basis for monitoring unconstitutional biometric searches of individuals through facial recognition technology").

[233] Ferguson, *supra* note 97.

in public spaces absent suspicion of a crime and has been positioned as possibly protected against by the Fourth Amendment on the grounds that the aggregation, tracking, and permanence of the data might constitute a Fourth Amendment search.[234] Importantly, face surveillance seems more similar to traditional police lineups, which were considered in *Hayes v. Florida* and *Davis v. Mississippi* and require suspicion of involvement in a criminal act.[235] Face identification is less likely to be protected under the Fourth Amendment, since it can be argued that such scans are not substantially differentiable from law enforcement photos and are individualized based on suspicion.[236] Finally, face tracking, the capacity to scan archives and databases of non-law enforcement video footage for faces, is complex under the Fourth Amendment with open questions about what legal requirements exist to bound the purchasing of third-party data acquisition.[237]

3. Sixth Amendment Confrontation Clause Issues in Eyewitness Identification and Facial Recognition Technology

The confrontation clause explicitly protects the right of the accused to confront the witnesses accusing them, making its consideration especially relevant when comparing eyewitness identification and FRT.[238] *Mattox v. United States* establishes the essential purpose of the confrontation clause as allowing the defendant the opportunity for "testing the recollection and sifting the conscience of the witnesses, [and] of compelling him to stand face to face with the jury in order that they may look at him and judge by his demeanor…whether he is worthy of belief."[239] Current interpretations of the confrontation clause are consistent with the principle function of securing an opportunity for the accused to cross-examine their accuser.[240] Out of courtroom identifications are permissible, provided the defendant returns to testify at trial.[241] Ruminating on the issue, the Senate determined that out-of-court identifications are more reliable and so adopted Federal Rule of Evidence 801(d)(c) as an exception to the Hearsay Rule (Federal Rule of

---

[234] *Id.* at 1142–44.

[235] *Hayes*, 470 U.S. at 816; *Davis*, 394 U.S. at 724.

[236] Ferguson, *supra* note 97, at 1151–52.

[237] *Id.* at 1158–59.

[238] U.S. CONST. amend. VI.

[239] Mattox v. U.S., 156 U.S. 237, 242–43 (1895).

[240] Claire L. Seltz, *Sixth Amendment—The Confrontation Clause, Witness Memory Loss and Hearsay Exceptions: What are the Defendant's Constitutional and Evidentiary Guarantees—Procedure or Substance?*, 79 J. CRIM. L. & CRIMINOLOGY 866, 883 (1988).

[241] U.S. v. Owens, 108 S.Ct. 838, 841–43 (1988).

Evidence 802).[242] In its more straightforward application then, the confrontation clause is a check on the power of eyewitness identification and an acknowledgment of its unreliability in that it must be constitutionally protected for it to be specifically interrogated.

How FRT fits into the confrontation clause framework is not obviously clear. Statements by machines are generally not considered to be hearsay "because the hearsay problems of perception, memory, sincerity and ambiguity have either been addressed or eliminated."[243] This suggests that the developer of the underlying algorithm is exempt from *Crawford* requirements, because the developer did not witness the specific events being testified to in creating the algorithm.[244] However, from *Melendez-Diaz* and *Bullcoming*, it seems straightforward to anticipate that whoever actually uploads the probe image into the database and searches for results will be required to testify to that process as opposed to submitting an affidavit or sending a substitute.[245] This would allow for cross-examination on the techniques used in uploading the probe image, such as modifying features or combining two faces.[246]

Opponents attempting to prevent the use of FRT in court may be able to utilize Federal Rule of Evidence 901 to their advantage by requiring the proponent of the evidence to "produce evidence sufficient to support a finding that the item is what the proponent claims it is."[247] Specifically, Rule 901(b)(9) allows for "[e]vidence describing a process or system and showing that it produces an accurate result."[248] Although this is a low bar, requiring only evidence sufficient to suggest a jury might believe the evidence is what it is purported to be, it would require evidence that the FRT used is reliable.[249]

---

[242] *See generally* Seltz, *supra* note 240 (for a more nuanced description of the foundations and current use of the confrontation clause).

[243] Jonathan D. Frieden & Leigh M. Murray, *The Admissibility of Electronic Evidence Under the Federal Rules of Evidence*, 17 RICH. J. L. & TECH. 1, 27 (2011) (quoting PAUL R. RICE, ELECTRONIC EVIDENCE: LAW AND PRACTICE 200 (2nd ed. 2005)); *see* State v. Armstead, 432 So. 2d 837, 840 (La. 1983) (arguing that machine statements are not hearsay because "there is no possibility of a conscious misrepresentation, and the possibility of inaccurate or misleading data only materializes if the machine is not functioning properly").

[244] Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 2045–46 (2017).

[245] *See* Melendez-Diaz v. Massachusetts, 557 U.S. 305 (2009); *see also* Bullcoming v. New Mexico, 564 U.S. 647 (2011).

[246] Garvie, *supra* note 143.

[247] FED. R. EVID. 901(a).

[248] FED. R. EVID. 901(b)(9).

[249] Frieden & Murray, *supra* note 243.

4. *Brady* and Exculpatory Evidence in Eyewitness Identifications and Facial Recognition Technology

Eyewitnesses make honest mistakes; this is well documented.[250] Wrongful convictions based on eyewitness testimony are nothing new to the criminal legal system.[251] Poor perception, bias, and imagination all contribute to potential eyewitness misidentifications.[252] When a perpetrator is misidentified and an innocent person is arrested (or, worse, convicted), the actual perpetrator is left at large. This harms both the liberty of the misidentified individual and the public safety interest of arresting criminals. Because "[s]ociety wins not only when the guilty are convicted but when criminal trials are fair," the Court has imposed upon the government an affirmative obligation to furnish exonerating evidence to defendants, pursuant to *Brady v. Maryland*.[253]

In addition to the vulnerability of eyewitness identifications to honest mistakes of perception, humans are subject to implicit biases, can be motivated by malicious intent, and are able to lie. Without the protections of *Brady*, the testimony of a mistaken eyewitness can easily lead to wrongful convictions.[254] When, however, the government complies with its *Brady* obligations, a defendant is provided with information about the eyewitness and circumstances under which the defendant was identified as the accused perpetrator.[255] Allowing a defendant to have access to potentially exonerating information creates the opportunity to challenge the reliability of the eyewitness' identification.[256] Information about the eyewitness that can be beneficial for the defendant includes if the witness received any benefits for providing the testimony.[257] For example, in *Banks v. Dretke*, a Brady violation was found when the prosecution failed to reveal that the witness was a paid informant.[258] Likewise, in *Giglio v. United States*, the court also recognized a *Brady* violation for failing to disclose a nonprosecution

---

[250] Edward Lasker, *Possible Procedural Safeguards Against Mistaken Identification by Eyewitnesses*, 2 UCLA L. REV. 552, 552 (1955).

[251] *See* Beth Schuster, *Police Lineups: Making Eyewitness Identification More Reliable,* NAT'L INST. JUST. (Oct. 1, 2007), https://nij.ojp.gov/topics/articles/police-lineups-making-eyewitness-identification-more-reliable (discussing a 2007 study that found that faulty eyewitness reports contributed to 75% of the first 183 DNA exonerations for that year).

[252] *See* Brian M. Addison, *Expert Testimony on Eyewitness Perception*, 82 DICK. L. REV. 465 (1978).

[253] Brady v. Maryland., 373 U.S. 83, 87 (1963).

[254] *See generally id.*

[255] *Id.*

[256] *Id.*

[257] *Id.*

[258] Banks v. Dretke, 540 U.S. 668, 698, 702–03 (2004).

agreement with the witness provided conditionally to incentivize his testimony.[259]

Even though the need for turning over exculpatory evidence has been found necessary to level the playing field, especially when fallible eyewitness testimony is at issue, the courts have been reluctant to expand those *Brady* protections to the context of FRT.[260] In *Lynch v. State*, the court's reasoning that the defendant could not prove that the other matches resembled him and thus might have been the person captured from the cell phone photo was made possible because the state did not provide the other potential matches to the defendant, quashing any opportunity for arguing misidentification.[261] The court refused to release the other photos to the defendant because they held the other potential match photos were not relevant.[262] The parody of this is that the "FACES" software used by Florida police in the *Lynch* case only provided a one "star" match for the defendant as a match to the provided "target" photo and also returned other potential matches, which the analyst never sent to police.[263] If a human eyewitness had been doing the identification and only identified the defendant with weak confidence while also stating that other persons in the lineup looked like the perpetrator, too, this information would be turned over to the defendant as *Brady* material.[264] When the court found the other potential match photos "not relevant," it held that FRT is more reliable than human eyewitnesses–without any basis for that reasoning.[265] In the *Lynch* case, the crime analyst did not even provide testimony about the procedures used to identify the defendant before sending his photo and rap sheet to officers, and the officer's identification based on the analyst's suggestion was upheld as reliable after applying the *Biggers* factors for reliability.[266]

Lynch stands as the strongest controlling authority on FRT and *Brady* material but other courts have ruled along the same lines.[267] It has been proposed that implementation of "open-file" or "automatic discovery" would serve to alleviate some of the concerns of power imbalance and prevent situations like in *Lynch*, where the defendant is not made aware that he was identified by FRT until the eve of trial and therefore is not able to prepare an

---

[259] Giglio v. United States, 405 U.S. 150, 154–55 (1972).
[260] *See, e.g.*, Lynch v. State, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018).
[261] *Id.*
[262] *Id.* at 1169.
[263] *Id.*
[264] Brady v. Maryland, 373 U.S. 83 (1963).
[265] *Lynch*, 260 So. 3d at 1169.
[266] *Id.* at 1170.
[267] *See* People v. Knight, 130 N.Y.S.3d 919 (N.Y. Sup. Ct. 2020).

adequate defense.[268] But "open-file" discovery still presents problems for defendants.[269] Recently, in *People v. Knight*, the Kings County Supreme Court found that when the state turned over a list of some of the potential matches, but not the entire list, it had satisfied the automatic discovery requirements of the New York Statute.[270]

Earlier this year when a defendant challenged the use of FRT to identify him, a New Jersey district granted an evidentiary hearing according to the standards set out in *United States v. Turner* to determine the admissibility of the photo array and the out of court identification made possible through FRT.[271] The defendant in *Turner* was granted the evidentiary hearing after pointing out to the court that in order for an officer to use FRT, the officer first must "manipulate or normalize" the image through "scaling, rotating and aligning it."[272] The defendant also suggested that officers can manipulate or edit images to increase the likelihood of a match, and that when the FRT returns a list of ranked matches, it is the officers' discretion that determines the best match from those potential matches produced by the software.[273]

V. CONCLUSION

Given FRT's increased use in daily life, its general lack of regulation and oversight is alarming. As the technology continues to find its way into law enforcement agencies across the country, these agencies need to be better prepared in how to thoroughly analyze each developer in order to prevent unreliable software platforms from being used against criminal defendants. Although there are recommendations that any agency using FRT also employ a trained facial examiner, there is limited evidence on who qualifies as a trained forensic examiner and how frequently a trained examiner is involved in FRT's use.[274]

This Article demonstrates that in its current form, there are many legal and ethical concerns about FRT that should caution its use in criminal courtrooms. FRT is plagued by opacity, with little available knowledge about

---

[268] Brian P. Fox, *An Argument Against Open-File Discovery in Criminal Cases*, 89 NOTRE DAVE L. REV. 425 (2013).

[269] *Id.*

[270] *Knight*, 130 N.Y.S.3d at 923.

[271] U.S. v. Turner, No. 19-763 (WJM), 2022 U.S. Dist. LEXIS 17318 (D.N.J. Jan. 31, 2022).

[272] *Id.* at *6.

[273] *Id.* (Defendant asserts that these steps of an officer uploading an image, receiving output and then making a discretionary call as to the best match are not only subject to human error, but also officer cognitive bias, and the software's inherent bias against correctly identifying faces of minorities.)

[274] *See* Kimberly J. Del Greco*, Law Enforcement's Use of Facial Recognition Technology*, FBI (Mar. 22, 2017), https://www.fbi.gov/news/testimony/law-enforcements-use-of-facial-recognition-technology.

its use, reliability, and the proprietary algorithms that undergird it.[275] Moreover, in a comparison with more traditional eyewitness identifications, it is clear that FRT suffers from bias and numerous gaps in legal protections.[276] Compared to eyewitness identifications, the status of FRT admissibility under *Daubert* is tenuous, significant concerns with digital search and surveillance under the Fourth Amendment persist, there is no dispositive guidance on how to conceptualize it within a Sixth Amendment framework, and *Brady* protections have yet to be suitably expanded to FRT. These problems require caution in the use of FRT, not only in courts, but also on the front-end of the process when acquiring FRT technology for later use in criminal cases, as the legal terrain surrounding FRT continues to grow and change.

Any agency looking to purchase FRT should also attempt to uncover whether the software has been submitted to the FRVT, and if so, how to interpret those results. This type of inquiry should include a thorough understanding of the algorithm's testing database, including its gender and racial composition, accuracy ratings, and comparisons against its direct competitors. While such scrutiny is likely to present an initial strain on departments who must then use their time and resources to meticulously evaluate each software, this level of understanding is critical in ensuring that unreliable technology is not inadvertently used against criminal defendants.[277]

---

[275] *See* Won, *supra* note 69.

[276] *See id.*

[277] Facial recognition issues are not just a feature of the legal system. In May 2022, a class action suit was brought against Snapchat for sharing users' unique facial features and voices without first providing required disclosures about how the information will be used and for how long. Coss et al., v. Snap, Inc., No. 1:22-cv-02480 (E.D. Ill. May 11, 2022). According to the lawsuit, Snapchat's proprietary "Lenses" involve the use of technology to create a face scan and "creating, obtaining and storing" a user's unique biometric identifiers that the company can store and use how it sees fit.