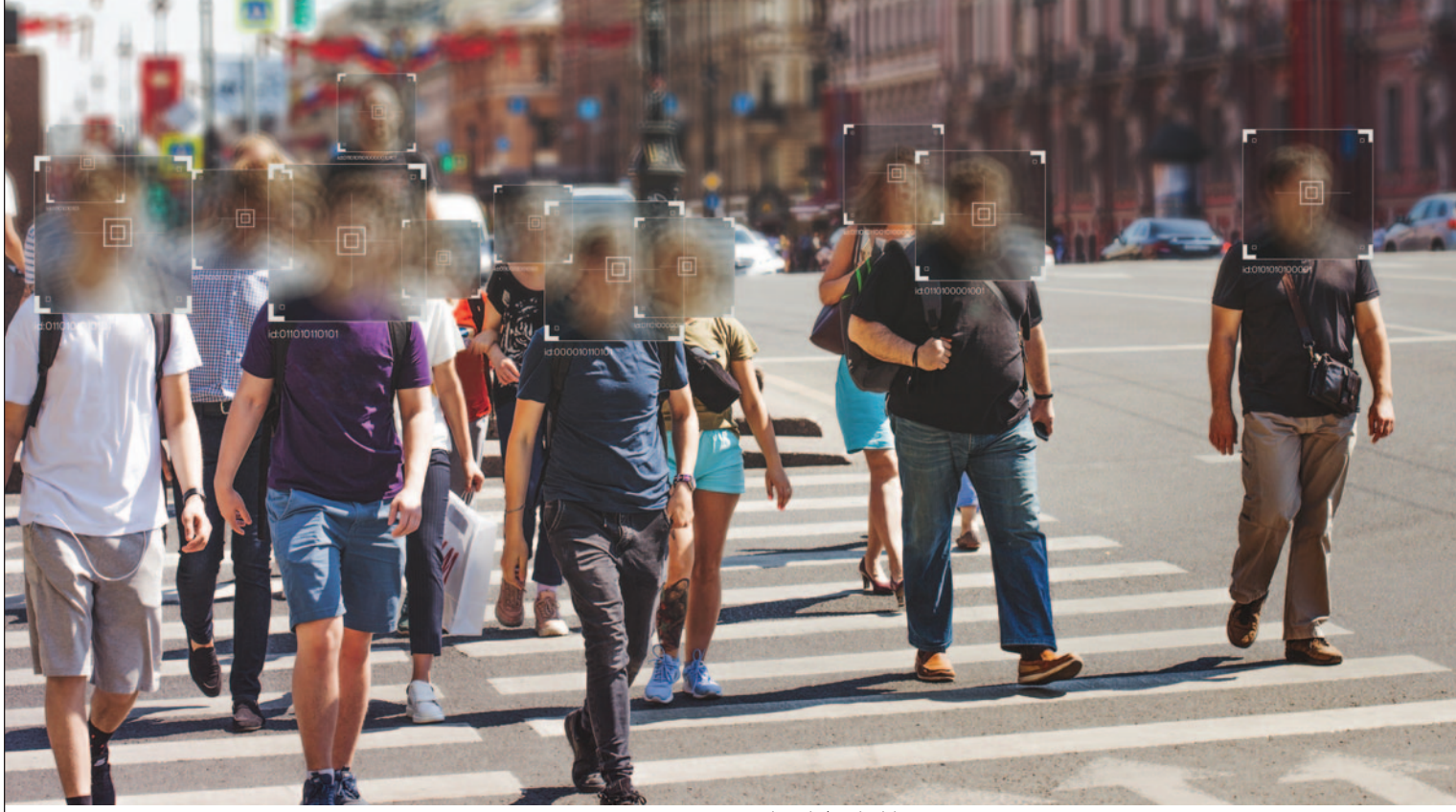

© Alexander | stock.adobe.com

What Defense Counsel Should Know About Facial Recognition Technology

More than 3,200 people have been exonerated since 1989, each serving an average of 8.75 years — or a combined 28,770 years — in prison for crimes they did not commit.[1] These numbers reflect those who have been cleared of wrongdoing; while the true wrongful conviction rate is almost impossible to know, recent studies estimate that somewhere between two and 10 percent of people behind bars are innocent.[2]

Facial recognition technology is not yet listed among the known causes of these miscarriages of justice. But there are several reasons to believe it already has, or will in the near future, become a contributing factor to a wrongful conviction.

First, facial recognition has become a widespread and routine forensic investigative technique and has been used in tens if not hundreds of thousands of cases. The first law enforcement system was established in 2001 by the Pinellas County Sheriff's Office in Florida. By 2016, this system alone was searched on average 8,000 times per month by more than 240 different agencies across the state. Also, by 2016, over one quarter of the 15,000 police departments across the United States had access to facial recognition databases, by conservative estimates, which include the faces of over half of all American adults.[3] This use appears to be expanding as well. In 2020, 20 federal agencies reported using facial recognition specifically for law enforcement purposes, with many looking to expand.[4] One company, Clearview AI, has created a database of more than 30 billion facial recognition templates, with plans to increase that number to 100 billion by the end of 2023.[5]

Second, facial recognition has already led to wrongful arrests. Five people — all Black men — in four different jurisdictions have spent time in jail for crimes they did not commit because of a facial recognition misidentification.[6] At least one of these men, Nijeer Parks, considered pleading guilty for fear of being convicted and sentenced to 20 years in prison by a court.[7]

Third, according to the National Registry of Exonerations, two of the leading factors contributing to wrongful convictions are mistaken eyewitness identification and the use of false or misleading forensic evidence at some stage in the investigation or adjudication.[8] Facial recognition searches reflect the most problematic elements of both of these techniques. It is a forensic investigative method that has never been established as scientifically valid — its reliability as an identification method as used in criminal investigations remains unknown. It requires both the facial recognition algorithm and the officer running the search to perform a function similar to what an eyewitness does — selecting a match out of a photo array — under conditions ripe for error and cognitive bias.

Unreliable Investigative Lead, or Probable Cause to Arrest?

Facial recognition is a forensic investigative technique based on the presumption that faces are unique

BY CLARE GARVIE

biometric identifiers.[9] Law enforcement agencies use facial recognition algorithms to compare a photo or video of an unknown person of interest, often called a "probe photo," to a database of known photographs, for example booking or driver's license photos.[10] The algorithm creates a "template" or a mathematical representation of the face in the probe photo and compares it to the templates on file in the database. It then generates a list of possible matches from the database, called a "candidate list," typically displayed in rank order starting with the photo that the algorithm has determined is the closest match. The candidate list can range from zero photos — the algorithm found no likely match — to hundreds of possible matches depending on several factors, including the quality of the probe image and the system configuration. It is then the task of the officer who ran the search to determine which photo, if any, in the candidate list is a likely match.[11] The individual steps in a search — and the risks of error each of them pose — are outlined in detail later on.

Most agencies consider the match produced by a facial recognition search to be an investigative lead only, not probable cause to arrest. For example, the Michigan State Police Facial Recognition Investigative Lead Report states at the top, in all capital letters: "This document is not a positive identification. It is an *investigative lead only* and is not probable cause to arrest. Further investigation is needed to develop probable cause to arrest."[12] The New York Police Department (NYPD) Patrol Guide states that "determination of a possible match candidate alone does not constitute probable cause to effect an arrest, or obtain an arrest or search warrant, and that further investigation is needed to establish probable cause."[13]

Investigative techniques produce evidence of varying reliability. An anonymous tip provided to a hotline, for example, may be given different weight than a high-quality latent print found at a crime scene. Indeed, police officers collect investigative leads from all manner of reliable or unreliable sources — some police departments have even been known to use psychics[14] — as long as the lead is corroborated by additional, credible evidence. While investigative leads are not held to the same rigorous standard as evidence introduced in court, it is nonetheless important to have a baseline understanding of how reliable or unreliable a method is.[15] Without this, it is quite simply impossible to know how much it can be relied upon, or in other words how much additional investigation should be required before the probable cause threshold is met. In the words of the authors of a 2016 government-sponsored review of the forensic science field: "Without appropriate estimates of accuracy, an examiner's statement that two samples are similar … is scientifically meaningless: it has no probative value, and considerable potential for prejudicial impact."[16]

This is where facial recognition has fallen into a procedural, scientific, and legal gray area. Despite being an investigative lead only on paper, in many cases facial recognition has provided the primary, if not only, piece of identity evidence. For example, in the case that resulted in the wrongful arrest of Nijeer Parks, the only additional investigative steps taken by the detective, who was not a witness to the crime, was to visually compare the photo of the suspect with Mr. Parks' mugshot.[17] In other cases, facial recognition has been paired with impermissible or otherwise deficient investigative steps. In a separate misidentification case, detectives asked a non-witness civilian to view video footage of the crime in question and then perform a photo array. The man she selected, Robert Williams, was subsequently jailed for a crime he did not commit.[18] In still other cases, the facial recognition investigative lead has been presented to an eyewitness but in a highly suggestive manner. When using facial recognition to investigate a sock theft, NYPD detectives texted the eyewitness the "possible match" with the accompanying text: "Is this the guy you know from going into your store many times before?"[19]

Despite providing the foundation for probable cause in these and other cases, the reliability of facial recognition as it is used in criminal investigations has never been established. While numerous studies published over the past few decades have evaluated the accuracy rates of facial recognition algorithms, and many studies have examined the reliability — or unreliability — of human facial identification, no study has yet comprehensively evaluated the unique combination of facial recognition algorithms and subjective human decision-making that makes up a typical criminal investigative search.[20]

Five Steps in a Search, and the Risk of Error

Facial recognition searches are composed of a series of human and machine steps — each of which introduces the possibility of error.[21]

1. Sourcing a probe photo. In many facial recognition searches, an officer will have the opportunity to select which probe image to submit to the facial recognition system, such as when there is CCTV footage or a social media account containing numerous photos of the subject. What this image looks like will affect the accuracy of the search. The less information is available about the face in the image, due to pixelation, blurriness, over- or underexposure, angle of the face, or attire such as hats or surgical masks, the lower the reliability of the resulting match will be. This is intuitive — lower quality images provide less information for both the algorithm and person making the identification to rely on when making a comparison.

There is no universally applied minimum photo quality standard in the United States, meaning that many facial recognition searches are run on low-quality images. In fact, some jurisdictions allow officers to run searches on non-photos such as forensic sketches, despite research that demonstrates this will overwhelmingly fail to produce an accurate identification.[22] At least one agency — the NYPD — has additionally submitted celebrity photographs in place of the subject they were looking for, on the faulty assumption that similar-looking people's facial biometrics can be substituted for one another.[23]

2. Selecting the database. An officer may have the opportunity to select which database against which to run the search. Since a facial recognition program can only make matches to faces in the database, which database is selected and who is enrolled will have an impact on accuracy as well. For example, if the correct match is not in the database searched, the resulting "matches" will all be misidentifications.

The size of the database matters. Larger databases contain more possible matches but also more people who look similar to each other, increasing the risk of the "doppelgänger" effect — a misidentification who nonetheless looks much like the search subject. Accuracy is also affected by the age of

the enrolled photos, with larger time spans between photos being harder for both humans and facial recognition algorithms to reliably compare.

While most facial recognition systems run on government-verified identity databases, some systems compare probe photos to images collected from the internet. This adds another aspect of uncertainty to any "match" — whether the internet-sourced image is tied to an accurate identity or an alias or fake account.[24]

3. Photo "preprocessing." Many facial recognition systems allow users to edit the probe photo before it is submitted to the algorithm, ranging from cropping the photo and other minor adjustments to wholesale creation of part of the face. Edits in real-world investigations have included the following:

- Cutting and pasting another person's eyes over the subject's closed eyes.
- Cropping out a subject's open mouth and chin and replacing it with the lower half of a face from an internet image search.
- Combining low quality images of two different people to search for a match to one of those people.
- Using 3D modeling software to change the orientation of a face.[25]

Photo editing will affect the accuracy of the facial recognition search in unpredictable ways. Facial recognition is considered a biometric identification process; editing at the pre-search stage may amount to the intentional contamination of the biometric sample. Since the algorithm has no way to tell what information is from the original photo and what has been added in by software programs or from other photographs, the resulting match may be more a reflection of the edits made than what the subject of the search actually looks like.

4. Algorithmic search. Facial recognition algorithms have improved dramatically over the past decade but are far from perfect, with many different factors affecting performance. First, ongoing tests conducted by the National Institute of Standards and Technology have shown that "accuracy is very strongly dependent on the algorithm and, more generally, on the developer of the algorithm."[26] In other words, not only does the age of the algorithm matter, but what company an agency chooses to purchase the algorithm from will influence the reliability of the search. Second, accuracy is influenced by the demographics — the age, sex, and race — of the person being searched. Some algorithms perform more poorly on darker skin tones, women, and both young and older faces.[27]

Facial recognition is considered a biometric identification process; editing at the pre-search stage may amount to the intentional contamination of the biometric sample.

Third, and related, demographics influence the confidence scores that algorithms return. Many algorithms will produce higher confidence scores for misidentifications if the person being misidentified is of the same race, sex, and age of the subject of the search.[28] This is similar to the type of error a person is likely to make — confusing two people who share demographic characteristics. The "human in the loop" may therefore compound, rather than be able to correct for, any algorithmic errors.[29] And finally, while algorithms have been subject to rigorous testing, these testing conditions do not necessarily reflect real-world use cases. Law enforcement agencies have run facial recognition searches on a wider range of lower quality and edited photos than has been tested to date.[30]

5. Candidate review. The final stage in any facial recognition search is the candidate review, also sometimes referred to as the "human in the loop." Facial recognition algorithms do not generate one "match" — they produce a list of possible matches, often accompanied by confidence scores and other information, for the officer to review. This review entails comparing the original probe image or video to each of the "candidate" photos to determine if there is a match.

While often framed as a valuable check against misidentification, this step in particular may introduce the highest risk of error. It assumes that people are good at comparing and identifying unfamiliar faces from photographs. Yet numerous studies show people perform remarkably poorly at this task, with even experienced officers performing no better at it than the average person.[31] In most jurisdictions, however, there is no training or certification requirement for the officers or analysts who perform this task, and no requirements that notes be taken on what procedure or method is used to form a conclusion that two faces are of the same person.

The conditions under which the facial comparison is conducted is additionally challenging — the algorithm has narrowed the field of "possible matches" down to very similar looking people, likely all within the same age range, racial group, and gender expression. The candidate lists may contain hundreds of photos, each representing a risk of a misidentification. Each photo may be presented with associated criminal arrest and other information, which may introduce bias — an officer may find a "match" between patterns in the crime being investigated and a person's criminal arrest history rather than in the two faces. Other cognitive biases that may be present at this stage include motivation to find a match and make an arrest; confirmation of a prior hypothesis of who committed the crime; illusory superiority, or the officer's belief that he or she is good at making facial identifications; context that increases pressure on finding a match even if there isn't one; and more.[32]

Taken as a whole, the facial recognition search process contains numerous opportunities for error, depending on the particulars of a given case. While widely considered an investigative lead only, evidence suggests that facial recognition searches are often relied upon as the primary, if not only, piece of evidence tying a defendant to the crime. In light of this, defendants should be given the opportunity to challenge the facial recognition search process.

Defense Counsel's Options and Opportunities

The on-paper status of facial recognition as an investigative lead has largely shielded it from court scrutiny for over 20 years, and the limited case law that does exist on the discoverability, reliability, or admissibility of facial recognition is inconsistent at best. However, based on the risk of misidentification outlined

above, there are several steps defense counsel should consider pursuing in facial recognition cases.

Discovery

If facial recognition is referenced as part of the investigation, defense counsel should request detailed discovery to uncover how the search was conducted. Some courts have been willing to entertain discovery, particularly of the facial recognition search results or candidate list. An article published in *The Champion* in July 2019, titled *Challenging Facial Recognition Software in Criminal Court*, provides a list of specific items defense counsel should consider requesting.[33]

One of the challenges facing defense counsel is that facial recognition is often not explicitly mentioned in an arrest warrant application or other disclosed information. Sometimes, the search process may be referred to by the facial recognition company's name or the name of the database searched. In other cases, reference to the facial recognition search may be omitted altogether, and there is an absence of any clear connection between a photo or video of the suspect and the defendant's identity. A motivated attorney or defense office could consider filing a facial recognition discovery motion in every case where (a) identity is at issue and (b) there is a photograph or video of the subject of the investigation. This places the burden on the State to either deny facial recognition was used or produce the discovery requested without requiring the defense counsel to intuit whether the technology was used.

Another challenge is that few, if any, agencies have applied data retention requirements to the facial recognition search process. Even when a court grants discovery, there is no guarantee that the information, such as the notes taken by the officer who ran the search or the search results themselves, still exists. This may benefit the defense in some cases; the State's failure to be able to comply with a court order or to otherwise retain discoverable information may result in the case being dropped or a favorable plea deal offered.

Brady Disclosure

Facial recognition searches produce *Brady* material — evidence that is potentially exculpatory and material — under at least two theories.[34] The first is negating guilt. Anything that suggests that the identification process was unreliable, tainted by subjectivity or cognitive bias of the officer who ran the search, or that someone besides the defendant may have been responsible for the crime such as the other photos in the candidate list, will be material. Relevant information might include the quality of the original probe image, any edits made, information about whether multiple databases were searched with different results, all possible match photos returned by the algorithm and their associated information, proficiency testing for the officer who ran the search, procedures followed, and so on.[35]

The second theory is impeachment of a witness. In searching a database for likely matches, the facial recognition algorithms perform a task analogous to an eyewitness selecting a match from a photo array or lineup. The confidence score that the system produces, such as a 75% "match," has been described as "the equivalent of an eyewitness saying they are 75% sure that the image depicts the person they observed at the crime scene."[36] Similarly, the officer reviewing the candidate list selects what he or she believes to be the most likely match from an array of photographs. This is particularly true given the absence of training in most jurisdictions; the officer running the search relies on his or her innate ability (or inability) to recognize faces rather than any specialized forensic knowledge. Information about how the algorithm came to its conclusion of similarity, and the conditions under which the officer selected the defendant from the candidate list, are analogous to information about conditions that might affect an eyewitness's memory and selection, which would be discoverable by the defense.[37]

Alternatively, a court may view the facial recognition search process as a forensic investigative technique, analogous less to an eyewitness process and more to another forensic method such as latent fingerprint examination.[38] Under this theory, the conditions under which the search was run, the information it produced, and the qualifications of the officer who ran the search should still be discoverable for impeachment purposes.

Reliability Hearings and Suppression

Defense counsel should consider filing motions for a reliability hearing as well as to suppress the facial recognition identification procedure on grounds that it is unreliable, unduly suggestive, or otherwise prone to misidentification.[39] If facial recognition provided the sole, or substantial, basis for probable cause, this amounts to reliance on an identification procedure that has never been established as scientifically valid. Another argument could focus on the investigative follow-up and subsequent identification. If the facial recognition lead was confirmed by an eyewitness, defense attorneys should consider whether the witness had reason to know that a facial recognition search had been conducted and was influenced by that fact. If the eyewitness is an officer, for example, it is likely the officer was aware that a facial recognition search took place. If the eyewitness is presented with a single image to identify — some jurisdictions allow this for officers or eyewitnesses to whom the defendant is "known" — the suggestiveness argument may be particularly compelling.

In a recent New York case, *People v. Gomez*, law enforcement used a facial recognition search to generate an investigative lead and "not as the basis for the defendant's arrest," according to the court. Nonetheless, the court granted a *Wade* hearing to determine whether the subsequent investigative step — sending the video of the crime to an officer who had previously arrested the person identified as the "possible match" — was unduly suggestive.[40] Similarly in a 2022 case in New Jersey, *United States v. Turner*, the court found the defendant's argument that a facial recognition search involves image editing, cognitive bias, and the possibility of human error persuasive enough to grant the defendant's motion for a reliability hearing on the identification procedure as a whole.[41]

Admissibility

The facial recognition search process overwhelmingly fails to meet the *Frye* or *Daubert* standards of admissibility. In *Frye* jurisdictions, the court asks whether the evidence or testimony in question was obtained using methods that were "sufficiently established to have gained general acceptance in the particular field in which it belongs."[42] The *Daubert* standard asks courts to consider (1) whether the technique in question can be and has been tested; (2) whether it has been subjected to peer review and publication; (3) its known or potential error rate; (4) the existence and maintenance of standards controlling how it is used; and (5) whether it has achieved widespread acceptance within the relevant scientific community.[43]

Having never been the subject of reliability testing in operational conditions, it would be hard to make the argument that facial recognition meets any, much less all, of these requirements.[44] The limited case law on the admissibility of facial recognition in court is largely in agreement. Most cases take for granted that facial recognition has not been accepted as reliable within the relevant scientific community.[45]

Facial recognition appears to have been presented as an element of the identification procedure for consideration by the court in at least a few cases, however, coming in through an officer's in-court testimony.[46] It is unclear how much weight the court gave the use of a facial recognition search in the resulting ruling, but this suggests defense attorneys should be prepared to argue that facial recognition fails to meet either the *Frye* or *Daubert* standard of admissibility, and that such testimony should not be admitted.

Shy of the State introducing facial recognition as an element of proof of identification, courts appear reluctant to grant an admissibility hearing if the defense requests it. Nonetheless, defense counsel should consider whether the facts of their case support an argument that facial recognition constituted a significant enough element of probable cause such that an admissibility hearing is required.

A Long but Necessary Road Ahead

Facial recognition continues unabated in police investigations, leading to arrests, charges, plea deals, and convictions — the defendant often unaware that it was even used. Defense counsel has a vital role to play in discovering when and how it is used and pushing back against yet another flawed forensic technique and faulty identification process. The criminal legal system should not wait for an exoneration to happen to discover how facial recognition may be contributing to wrongful convictions.

Notes

1. National Registry of Exonerations, Mich. St. Univ. C. of L., https://www.law.umich.edu/special/exoneration/Pages/about.aspx (last visited Mar. 12, 2023).

2. *See* Staff, *How Many Innocent People Are in Prison*, Innocence Project, Feb. 22, 2023, https://innocenceproject.org/how-many-innocent-people-are-in-prison/; *see* Clare Gilbert, *Beneath the Statistics: The Structural and Systemic Causes of Our Wrongful Conviction Problem*, Ga. Innocence Project, Feb. 1, 2022, https://www.georgiainnocenceproject.org/2022/02/01/beneath-the-statistics-the-structural-and-systemic-causes-of-our-wrongful-conviction-problem/ (estimating that between four and six percent of people currently incarcerated in the United States are innocent).

3. *See* Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Ctr. on Priv. & Tech., Oct. 18, 2016, https://www.perpetuallineup.org/.

4. *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks,* GAO-21-518, 9, U.S. Gov't Acct. Off., June 2021, https://www.gao.gov/assets/gao-21-518.pdf; *Facial Recognition Technology: Current and Planned Uses by Federal Agencies,* GAO-21-526, 25, U.S. Gov't Acct. Off., Aug. 2021, https://www.gao.gov/assets/gao-21-526.pdf.

5. *See* Drew Harwell, *Facial Recognition Firm Clearview AI Tells Investors It's Seeking Massive Expansion Beyond Law Enforcement,* Wash. Post, Feb. 16, 2022, https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/.

6. *See* Kashmir Hill, *Wrongfully Accused by an Algorithm*, NYTimes (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; *see* Elisha Anderson, *Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit*, Detroit Free Press, July 10, 2020, https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/; *see* Anthony G. Attrino, *He Spent 10 Days in Jail After Facial Recognition Software Led to the Arrest of the Wrong Man, Lawsuit Says*, NJ Advance Media, Dec. 29, 2020, https://www.nj.com/middlesex/2020/12/he-spent-10-days-in-jail-after-facial-recognition-software-led-to-the-arrest-of-the-wrong-man-lawsuit-says.html; *see* Thomas Germain, *Innocent Black Man Jailed After Facial Recognition Got It Wrong, His Lawyer Says*, Gizmodo, Jan. 3, 2023, https://gizmodo.com/facial-recognition-randall-reid-black-man-error-jail-1849944231; Khari Johnson, *Face Recognition Software Led to His Arrest. It Was Dead Wrong*, Wired, Feb. 28, 2023, https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/.

7. Anderson Cooper, *Police Departments Adopting Facial Recognition Tech Amid Allegations of Wrongful Arrests*, CBS 60 Minutes, May 16, 2021, https://www.cbsnews.com/news/facial-recognition-60-minutes-2021-05-16/.

8. *See* Innocence Project, *The Causes of Wrongful Conviction*, https://innocenceproject.org/causes-wrongful-conviction./, (last visited Mar. 12, 2023). The National Registry of Exonerations lists six factors that contribute to wrongful convictions: false or misleading forensic evidence, false confessions, mistaken witness identification, official misconduct, perjury or false accusation, and inadequate legal defense, with most cases having multiple contributing factors. *See* Nat'l Registry of Exonerations, https://www.law.umich.edu/special/exoneration/Pages/detaillist.aspx (last visited Mar. 12, 2023).

9. *See* National Research Council, Biometric Recognition: Challenges and Opportunities, 1 (2010).

10. Other facial recognition databases used by law enforcement include visa and passport photos and the Clearview AI database, composed of images scraped from various internet sources. *See Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy,* U.S. Gov't Acct. Off., May 2016, https://www.gao.gov/assets/gao-16-267.pdf (describing FBI access to the Department of State visa applicant and citizen passport photos). *See* Clearview AI, https://www.clearview.ai/law-enforcement (describing a 30+ billion image database sourced from various internet sources) (last visited Mar. 14, 2023).

11. For a more detailed description of the facial recognition search process, *see* Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Ctr. on Priv. & Tech., Dec. 06, 2022, https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/.

12. *See, e.g.,* Michigan State Police, Investigative Lead Report, Case Number 1810050167, Mar. 11, 2019, *available at* https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig (emphasis in original).

13. New York Police Dep't, Patrol Guide, Facial Recognition Technology, Procedure No: 212-129, 3, Dec. 2, 2022, *available at* https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/public-pguide2.pdf.

14. *See, e.g.,* Myrna Oliver, *Dorothy Allison; Volunteered to Aid Police as 'Psychic,'* L.A. Times, Dec. 7, 1999, latimes.com/archives/la-xpm-1999-dec-07-mn-41451-story.html (describing how police in New Jersey consulted with a self-proclaimed psychic over a period of 30 years on thousands of cases).

15. *See* President's Council of Advisors on

Science and Technology, *Report to the President: Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature Comparison Methods*, Exec. Off. of the Pres., 2, Sept. 2016, *available at* https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf/.

16. *Id.* at 121.

17. Affidavit of Probable Cause, State of New Jersey v. Nijeer Parks, Police Case No. 19010123 (Woodbridge Mun. Ct. 2019). This appears to be a relatively common practice — where a non-witness detective makes a visual comparison between two photographs, one assumed to be that of the suspect and the other returned as a possible match photograph, and presents it as a witness identification in the arrest warrant application. *See, e.g.,* People v. Reyes, 69 Misc.3d 963 (Sup. Ct. NY 2020).

18. *See* Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. Times, June 4, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

19. *See* Garvie, *A Forensic Without the Science, supra* note 11, at 1.

20. *Id.* at 15–16.

21. This characterization of a search process as a series of human and machine steps is adapted from Garvie, *A Forensic Without the Science*, *supra* note 11, at 9–12.

22. *See, e.g.,* Scott Klum, Hu Han, Anil Jain & Brendan Klare, *Sketch Based Face Recognition: Forensic vs. Composite Sketches,* 2013 Int'l. Conf. on Biometrics, 2013.

23. *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Ctr. on Priv. & Tech. May 16, 2019, https://www.flawedfacedata.com/.

24. *See, e.g.,* Clearview AI, https://www.clearview.ai/law-enforcement (last visited Mar. 14, 2023).

25. *See supra* note 22.

26. Patrick J. Grother, Mei L. Ngan & Kayee K. Hanaoka, *Ongoing Face Recognition Vendor Test (FRVT) Part II: Identification*, Natl. Inst. of Stds. & Tech., Sept. 13, 2019, https://www.nist.gov/publications/face-recognition-vendor-test-frvt-part-2-identification.

27. Patrick Grother, Mei Ngan & Kayee Hanaoka, *Face Recognition Vender Test Part 3: Demographic Effects*, Natl. Inst. of Stds. & Tech, Dec. 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

28. Cynthia M. Cook et al., *Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*, IEEE Transactions on Biometrics, Behavior and Identity Science, Feb. 2019, https://mdtf.org/publications/demographic-effects-image-acquisition.pdf; K.S. Krishnapriya et al., *Characterizing the Variability in Face Recognition Accuracy Relative to Race*, 2019 IEEE/CVF Conf. on Comp. Vision and Pattern Recog. Workshops, 2278–2285 (2019), doi:10.1109/CVPRW.2019.00281.

29. *Id.*

30. *See supra* note 11.

31. For a summary of these studies, *see supra* note 11, at 22–26.

32. *See id.* at 22–33.

33. Kaitlin Jackson, *Challenging Facial Recognition Software in Criminal Court*, The Champion, 14–26, July 2019, *available at* https://www.nacdl.org/getattachment/548c697c-fd8e-4b8d-b4c3-2540336fad94/challenging-facial-recognition-software-in-criminal-court_july-2019.pdf.

34. Note that at least one court has considered — and rejected — this argument, but the resulting decision fails basic logic. In *Lynch v. Florida,* the District Court of Appeal for the First District of Florida denied the appellant's request for the facial recognition search results under *Brady*, arguing that "because he cannot show that the other photos the database returned resembled him, he cannot show that they would have supported his argument that someone in one of those photos was the culprit." In other words, the appellant needed to know what the photos he was requesting looked like before being granted the opportunity to view them. *See* Lynch v. Florida, No. 1D16-3290, 2017 WL 11618201 (Fla. App. 1 Dist. 2017).

35. *See supra* note 11, at 42.

36. *See* Nicole A. Spaun, *Chapter 26: Face Recognition in Forensic Science* in Handbook of Face Recog., 667 (Stan Z. Li & Anil K. Jain, eds., 2d. ed., 2011).

37. *See supra* note 11 at 42–43.

38. There are superficial similarities between these two techniques. Both are subjective feature comparison methods. Both involve a latent print — either a face or fingerprint — retrieved and compared against a database of known prints. When automated, both techniques produce a list of possible matches for an examiner or officer to review.

39. For an in-depth examination of facial recognition and suppression, see Jackson, *Challenging Facial Recognition Software in Criminal Court*, at 21–22.

40. People v. Gomez, Ind. No. 70498-2022 (Sup. Ct. NY 2022).

41. United States v. Turner, 2022 WL 279784 (Dist. Ct. NJ 2022).

42. Frye v. United States, 293 F. 1012, 1014 (D.C. Cir. 1923). The *Frye* standard is followed by California, Illinois, Minnesota, New Jersey, New York, Pennsylvania, and Washington.

43. Daubert v. Merrill Dow Pharmaceuticals Inc., 506 U.S. 579 (1993).

44. For a more in-depth look at this argument, *see supra* note 11, at 43–46.

45. *See, e.g.,* People v. Reyes, 69 Misc.3d 963 (Sup. Ct. NY 2020) ("There is no agreement in a relevant community of technological experts that [facial recognition] matches are sufficiently reliable to be used in court as identification evidence."); *see* People v. Collins, 15 N.Y.S.3d 564 (2015) ("evidence produced by these technologies is not generally accepted as reliable by the relevant scientific communities and so cannot be admitted in trials."); *see* Hutcherson v. State, 2014 Ark. 326 (Ark. Sup. Ct. 2014) (holding that the appellant failed to demonstrate that facial recognition had become an accepted forensic tool in Arkansas); *see* People v. Carrington, 2018 Cal. App. Unpub. LEXIS 796 (finding that facial recognition and video enhancing software is not generally accepted as reliable in the relevant scientific community).

46. *See, e.g.,* People v. Robinson, 2022 WL 15525821 (Mich. App. Ct. 2022) (describing how the detective "provided detailed testimony" including that investigating officers "extracted video from inside the BP gas station, sent certain 'clips' to the media, and attempted to identify the individual through facial recognition software." The court further stated: "Facial recognition software and tips that were reported through Crime Stoppers supported that defendant was the individual in the gas station," suggesting that at least some weight was given the search.); *see* United States v. Lee, 451 F.Supp.3d 1 (Dist. Ct. DC 2020) (describing how the fact that facial recognition software identified the defendant was part of the "weight of the evidence" against him counseling in favor of detention). ■

About the Author

Clare Garvie is the Training & Resource Counsel with NACDL's Fourth Amendment Center. She is the author of *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations* with the Center on Privacy & Technology, the report on which this article is based.

Clare Garvie
NACDL
Washington, DC
202-465-7657
Email cgarvie@nacdl.org
Twitter @clareangelyn