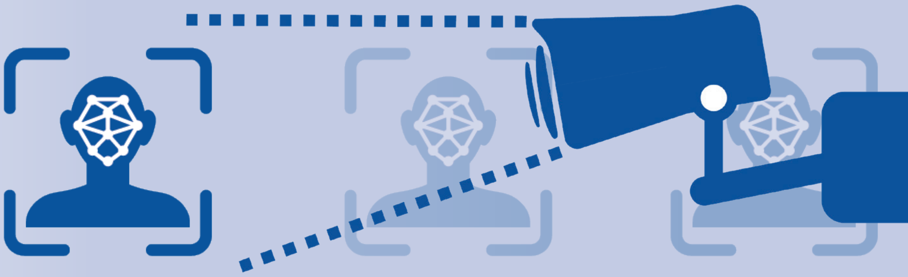
NACDL
FOURTH
AMENDMENT
CENTER



Facial Recognition Primer

What is facial recognition technology?

Law enforcement agencies use facial recognition technology (FRT) to assist in identifying unknown people — suspects, victims, witnesses, and others — captured on video or in photos.[1] These systems employ pattern recognition algorithms, computer programs that are trained to analyze and evaluate the similarity of features present in facial photographs.[2] When fed a "probe" photo or video, the system first detects whether there is a face in the frame. Next, it creates a "face template" or feature vector, a mathematical representation of that face. Finally, it compares that template to facial templates on file in the database(s) it is paired with, which may be booking photos, driver's licenses, visa and passport photos, or databases compiled by private companies from other sources such as the internet.[3] When used in criminal investigations, this technology is paired with a number of steps conducted by an officer or analyst which may include: selecting a video still to search; choosing the database to be searched; editing the probe image; and reviewing the "candidate list" produced by the algorithm.[4]

What does police facial recognition look like?

It is a widespread investigative tool. Facial recognition has become a routine investigative technique, used in hundreds of thousands of cases.[5] The earliest systems were implemented in 2001; by 2016 more than one quarter of the 15,000 U.S. police departments had access to a FRT system.[6] At least thirty-one states allow police officers to run or request facial recognition searches of driver's license photos, and many more systems run against mugshot databases.[7] FRT company Clearview AI has additionally amassed a database of more than thirty billion images from various internet sources, with the goal of reaching 100 billion images by the end of 2023.[8]

Its reliability has not been established. As used in criminal investigations, facial recognition is a "subjective feature comparison method" — a series of steps used to determine whether an evidentiary sample (in this case a face photo or video) can be associated with a particular source (i.e., a specific person) based on similarities between the sample and the source.[9] To be considered scientifically valid, this type of method must be subject to empirical testing that a) establishes estimated error rates for the technique and b) reflects how it is used in real-world investigations.[10] To date, no study has yet evaluated and established error rates for how a typical or representative sample of investigative facial recognition searches are run.[11]

It is a series of subjective, unconstrained steps. As used in criminal investigations, facial recognition searches comprise a series of human and machine steps, each of which introduces variability in quality and the possibility of error. These include:[12]

- **Sourcing the probe image.** The quality of the probe image or video will affect the reliability of the search. There are currently no national requirements prescribing minimum photo quality standards.[13]
- **Selecting the database.** Facial recognition can only identify faces in its database — if the search subject is not enrolled, the resulting "matches" will all be misidentifications. Database size impacts accuracy as well; larger databases mean more possible correct matches enrolled but also a higher likelihood of the "doppelgänger" effect leading to the wrong person ultimately selected as a match.[14]
- **Photo editing.** Many systems allow officers to edit the probe image, ranging from simple cropping and color correction to more invasive Photoshopping. Photo editing will impact the reliability of the search in unpredictable ways.[15]
- **Algorithmic search.** Facial recognition algorithms vary by quality; the make and model of the algorithm used will impact the accuracy of the search. Many algorithms also

perform differently depending on the age, race, and sex of the person being searched, with some algorithms performing worse on young faces, women, and darker skin tones.[16]

- **Candidate review.** The system produces a list of possible matches for a person to review. This "human in the loop" is supposed to provide a check against any misidentification risk introduced by the algorithm. However, there are no nationally required training standards or guardrails against poor performance, cognitive bias, or other sources of human error.[17]

It is an "investigative lead" that leads to arrests. Most agencies consider FRT matches investigative leads only, not positive identification or probable cause to make an arrest. How much additional evidence needs to be collected, however, and the quality and independence of that evidence, is rarely defined. In fact, there have been many cases where an FRT match was the sole, or primary, piece of identification evidence. A "possible match" might be paired with a non-witness officer review of the match, a confirmatory ID by another officer, or a single-photo array presented to an eyewitness. The witness might additionally know that FRT was used, influencing their belief in the reliability of the possible match.[18]

At least six people have been wrongfully arrested because of an FRT misidentification.[19] Others may have taken plea deals or been convicted of crimes they did not commit without ever being informed FRT was an element of the case against them.

Potential legal arguments. FRT is not typically introduced as identity evidence in court by the government but has nonetheless led to an unknown number of people arrested and charged through its use as an investigative lead. Defense attorneys should consider the following ways to gather more information and challenge the use of FRT in their case:

1. **Discovery.** If facial recognition is referenced as part of an investigation, defense counsel should consider requesting detailed discovery about how the search was conducted, looking for indicia of unreliability in each of the search process steps such as low-quality images, editing, or lack of training.[20] Even if FRT isn't expressly mentioned, if a) identity is at issue, b) there is a photo or video of the suspect, and c) there isn't a clear explanation of how the identification occurred, consider filing an FRT discovery motion to shift the burden of explaining an otherwise unclear identification process onto the government.
2. **Brady.** Because of the risk of error present in a given facial recognition search, defense counsel should argue that information pertaining to the search is *Brady* material under the theory of negating guilt. FRT is also information relevant to impeaching a witness — both the facial recognition algorithm and the system operator perform functions analogous to that of an eyewitness or a forensic expert, producing material that should be disclosed under *Brady* regardless of whether it is requested.[21]
    a. In 2023, a New Jersey appellate court held that the defendant was entitled to discovery, finding that the defense provided "convincing evidence of FRT's novelty, the human agency involved in generating images, and the fact FRT's veracity has not been tested or found reliable on an evidential basis by any New Jersey court."[22]
3. **Reliability and suppression.** Defense counsel should consider filing motions for a reliability hearing and to suppress an FRT identification procedure on the grounds that it is unreliable, unduly suggestive, or otherwise prone to misidentification. This is particularly true if the facial recognition search provided the sole, or primary, basis for probable cause despite what the arrest or search warrant affidavit states, or if the witness had reason to know that FRT was used, such as when the witness is an officer.[23]

Additional Resources

- *New Jersey v. Arteaga*, No. A-3078-21T1 (Sup. Ct. N.J. 2023), https://www.nacdl.org/Document/New-Jersey-v-Arteaga-Appellate-Decision; Brief of Amici Curiae EPIC, EFF, and NACDL in *New Jersey v. Arteaga*, https://www.nacdl.org/brief/New-Jersey-v-Arteaga.
- Clare Garvie, *What Defense Counsel Should Know About Facial Recognition Technology*, The Champion (June 2023), https://www.nacdl.org/Document/What-Defense-Counsel-Should-Know-About-Facial-Reco.
- Kaitlin Jackson, *Challenging Facial Recognition Software in Criminal Court*, The Champion (July 2019), https://www.nacdl.org/getattachment/548c697c-fd8e-4b8d-b4c3-2540336fad94/.
- Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Georgetown Law Center on Privacy & Technology (Dec. 2022), http://forensicwithoutscience.org/.

4. **Admissibility.** FRT is rarely, if ever, introduced directly as identity evidence in court, and courts generally assume it has not reached the level of scientific reliability to allow this to happen.[24] However it has been referenced as an element of the identity procedure in officer in-court testimony.[25] Therefore, defense counsel should be prepared to argue that the facial recognition search process as a whole, for the reasons outlined above, is not a reliable identification procedure that meets the standard required for in-court admission of scientific evidence under the *Daubert* or *Frye* standards.[26]

5. **State laws.** Several states have passed laws governing the use of FRT by law enforcement. Check the fact pattern of your case against any relevant state laws for restrictions, inconstancies, required disclosures, and documents that should be discoverable.[27]

Notes

[1] For a detailed examination of facial recognition in criminal investigations, see Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Georgetown Law Center on Privacy & Technology (Dec. 6, 2022), http://forensicwithoutscience.org/ (hereinafter *Forensic*). The term "facial recognition" additionally is used to refer to other face-based comparisons, including: face confirmation (comparing two photos or a live person with their photo to verify they are who they say they are) and face classification or characterization (inferring something about a person such as their demographics or emotional state). When paired with live video footage, FRT also can be used as a surveillance tool, scanning the faces of everyone who passes by a camera to locate and identify certain individuals. Since these use cases are rare in the U.S. policing context, they are not explored in this document. For an in-depth analysis of the surveillance implications, see Clare Garvie & Laura Moy, *America Under Watch: Face Surveillance in the United States*, Georgetown Law Center on Privacy & Technology (May 16, 2019), https://www.americaunderwatch.com/.

[2] For more information on the types of algorithms in a facial recognition system and how they are trained, see Testimony of Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards & Technology (NIST) (Feb. 6, 2020), https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0.

[3] *See What Is Facial Recognition*, AWS, https://aws.amazon.com/what-is/facial-recognition/ (last visited May 10, 2023); *see, e.g.*, Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, NYTimes (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[4] *See generally Forensic*, *supra* note 1.

[5] *See Forensic*, *supra* note 1 at 9.

[6] *See* Clare Garvie, Alvaro Bedoya, Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Center on Privacy & Technology at Georgetown Law, 25 (Oct. 18, 2016), https://www.perpetuallineup.org/.

[7] *See* Clare Garvie, *Statement before the U.S. House of Representatives Committee on Oversight and Reform Hearing on Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties*, 5, (May 22, 2019), *available at* https://www.congress.gov/116/meeting/house/109521/witnesses/HHRG-116-GO00-Wstate-GarvieC-20190522.pdf.

[8] *See* Clearview AI, https://www.clearview.ai/law-enforcement (describing a 30+ billion image database sourced from various Internet sources) (*last viewed* Mar. 14, 2023); *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/.

[9] Other feature comparison methods found in policing include analyses of fingerprint, DNA, hair and fiber, handwriting, firearms and toolmark impressions, bitemarks, and more. *See* Garvie, *supra* note 1, at 13.

[10] *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,* Executive Office of the President, 2 (Sept. 2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf.

[11] *See Forensic*, *supra* note 1 at 15–16.

[12] Not all these steps will be present in each search; this represents the universe of variability that may be introduced in any given search. For complete citations and more details on each of these steps, *see supra* note 1.

[13] *See Forensic*, *supra* note 1 at 10.

[14] *See* C. Rathgeb et al., *Impact of Doppelgängers on Face Recognition: Database and Evaluation,* 2021 International Conference of the Biometrics Special Interest Group (BIOSIG), 1–4 (2021), *doi: 10.1109/BIOSIG52210.2021.9548306.*

[15] *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data* (May 16, 2019), https://www.flawedfacedata.com/.

[16] *See* Patrick Grother, Mei Ngan, and Kayee Hanoaka, *Face Recognition Vender Test part 3: Demographic Effects,* National Institute of Standards and Technology (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[17] *See generally Forensic*, *supra* note 1.

[18] *See Forensic, supra* note 1 at 6–8.

[19] *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* 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* Kashmir Hill, *Wrongful Accused by an Algorithm*, NYTimes (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; *see* 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/; *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; *see* Kashmir Hill, *Eight Months Pregnant and*

Arrested After False Facial Recognition Match, NYTimes (Aug. 6, 2023), https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.

[20] For a list of documents and other information to request in discovery, *see* 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.

[21] Brady v. Maryland, 272 U.S. 284 (1973). *See supra* note 1 at 39–43. Note that at least one court has considered — and rejected — this argument, but the resulting decision fails basic logic. *See* Lynch v. Florida, No. 1D16-3290, 2017 WL 11618201 (Fla. App. 1 Dist. 2017).

[22] New Jersey v. Arteaga, No. A-3078-21 (Sup. Ct. NJ 2023), *available at* https://www.nacdl.org/Document/New-Jersey-v-Arteaga-Appellate-Decision.

[23] A handful of cases have considered this question. *See* People v. Gomez, Ind. No. 70498-2022 (Sup. Ct. NY 2022); *see* United States v. Turner, 2022 WL 279784 (Dist. Ct. NJ 2022).

[24] *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 he 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).

[25] *See, e.g.,* People v. Robinson, 2022 WL 15525821 (Mich. App. Ct. 2022); *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.).

[26] Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579 (1993); Frye v. United States, 293 F. 1013 (D.C. Cir. 1923).

[27] Potentially relevant state statutes include: Ala. Code 1975 § 15-10-111; A.R.S. § 15-109 (Ariz.); C.R.S.A. §§ 24-18-301–309, 2-3-1707, 22-32-150, 22-32-529, 24-33.5-117 (Colo.); F.S.A. §§ 1022.222, 943.05 (Fla.); 740 ILCS § 14/1–99, 105 ILCS §§ 5/10-20.40, 5/34-18.34, 625 ILCS 5/6-110.1 (Ill.); Ky. Rev. Stat. §§ 61.9305, 72-6315; La. Rev. Stat. §§ 32:410, 17:100.8; 29-A M.R.S.A. § 1401, 25 M.R.S.A § 4501, § 6001 (Maine); MD Code § 4-320.1; M.G.L.A. § 220 (Mass.); M.S.A. § 626.19 (Minn.); N.H. Rev. Stat. § 189:68; NY State Tech § 106-b; O.R.S. §§ 133.741, 807.026; 42 Pa.C.S.A. § 67 A07; T.C.A. § 49-1-706 (Tenn.); U.C.A. 1953 §§ 77-23e-101–106 (Utah); 20 V.S.A. § 4633, 23 V.S.A. § 634, 2020 Acts & Resolves No. 166 § 14 (Vt.); VA Code Ann. §§ 52-4.5, 15.2-1723.2, 23.1-815.1; RCW §§ 43.386.010–901, 46.20.037, 40.26.020 (Wa.).

About the National Association of Criminal Defense Lawyers (NACDL)

The National Association of Criminal Defense Lawyers (NACDL) envisions a society where all individuals receive fair, rational, and humane treatment within the criminal legal system.

NACDL's mission is to serve as a leader, alongside diverse coalitions, in identifying and reforming flaws and inequities in the criminal legal system, and redressing systemic racism, and ensuring that its members and others in the criminal defense bar are fully equipped to serve all accused persons at the highest level.

About the Fourth Amendment Center

NACDL's Fourth Amendment Center offers direct assistance to defense lawyers handling cases involving new surveillance tools, technologies and tactics that infringe on the constitutional rights of people in America.

The Center is available to help members of the defense bar in bringing new Fourth Amendment challenges. To request assistance or additional information, contact **4AC@nacdl.org**.

About the NACDL Foundation for Criminal Justice (NFCJ)

NACDL's Fourth Amendment Center is supported by contributions made to the NACDL Foundation for Criminal Justice (NFCJ), a 501(c)(3) charity. The mission of the NFCJ is to preserve and promote the core values of America's justice system guaranteed by the Constitution — among them due process, freedom from unreasonable search and seizure, fair sentencing and effective assistance of counsel — by educating the public and the legal profession to the role of these rights and values in a free society.

How to Support Our Work

You can support our mission and enhance your career by becoming a member of the NACDL or by making a tax-deductible donation to the NFCJ. Learn more by visiting https://www.nacdl.org/Landing/JoinNow or nfcj.org/support.

NACDL FOURTH
AMENDMENT CENTER

For litigation assistance and other resources contact 4AC@nacdl.org