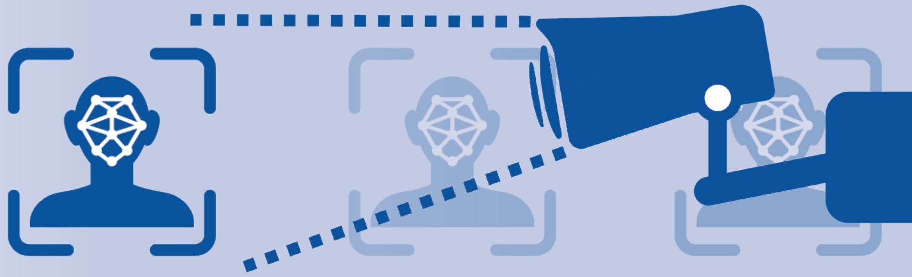
NACDL
FOURTH
AMENDMENT
CENTER



Advisory:
Defense Use of Facial Recognition Technology

Summary

Facial recognition technology, an identification tool that is widely used by law enforcement, is also sometimes promoted as a tool to exonerate the innocent or otherwise support criminal defense.[1] This advisory provides a brief overview of the issues arising from law enforcement use of facial recognition and identifies various concerns that defense attorneys should take into consideration before using facial recognition tools.

For more information on facial recognition and ways to challenge its use, see NACDL's Facial Recognition Resource Page.

Facial recognition overview

Facial recognition is an identification method based on the presumption that faces are unique biometric indicators. Facial recognition algorithms compare two images to determine whether they depict the same person (sometimes called face verification) or compare an image or video of an unknown person against a database of known images to generate a possible identification.[2] Most systems also include a "human in the loop" who reviews the possible match candidates produced by the facial recognition algorithm.[3]

Law enforcement agencies around the country use facial recognition in attempts to identify persons of interest in an investigation including suspects, victims, and witnesses. This use raises several concerns.

- A facial recognition search is a forensic investigative method that lacks scientific validity. Its reliability, as currently used in the policing context, has never been established, and the conditions under which many searches are run suggest the results may suffer from error and bias.[4] And while it is largely considered to generate investigative leads only — not positive identifications — in investigations across multiple jurisdictions officers have relied primarily or entirely on a facial recognition "match" to make arrests.[5] At least six people, all of whom are Black, have been wrongfully arrested because of a facial recognition misidentification.[6]
- Lack of transparency and oversight is systemic, and the government routinely fails to disclose information about facial recognition searches to the defense. This failure violates the government's discovery obligations as well as a defendant's right to exculpatory material under *Brady v. Maryland,* 37 U.S. 83 (1963).[7]
- Facial recognition can be used as a powerful surveillance tool. Since faces can be captured remotely and in secret through a network of surveillance cameras, the technology could be used to track an individual's past and real-time movement in violation of the Fourth Amendment.[8] This may also serve to chill participation in activities protected by the First Amendment.[9]

Facial recognition as a defense tool?

Defense attorneys will typically encounter facial recognition as an element of the government's case against their client and should be prepared to file motions to uncover and challenge its use.[10] There also may be limited circumstances where facial recognition appears useful to a given defense. For example, an attorney could use facial recognition to compare images of the suspect and the defendant to demonstrate that there is no match, and that the defendant is innocent.[11] Or facial recognition could identify other exculpatory information — in a recent vehicular homicide case in Fort Myers, Florida, a defense attorney used facial recognition to track down a witness who was able to exonerate his client.[12]

These cases will be rare, however, and may be more indicative of fundamental weaknesses in the government's case than of the need for a new technology. In the Fort Myers case, defendant Andrew Conlyn was charged with homicide for a fatal car crash despite a witness statement — recorded by an officer's body camera at the scene of the crash — that Conlyn "was the passenger" the witness had helped from the vehicle.[13] Police failed to record the witness' name or other information, or request he provide a statement to investigators, though they did make some limited, unsuccessful attempts to locate him in the following years.[14] This blatant contradiction notwithstanding, the State pursued a case against Conlyn based on an alternate interpretation of evidence from the crash site. Conlyn and his defense team were left to do the State's job of identifying and tracking down the eyewitness.

This case has been used as a "success story" to promote the idea that facial recognition can provide defense attorneys with an efficient and affordable way to identify potential witnesses, correct misidentification, and identify exculpatory evidence.[15] This ignores the fact that the defense turned to facial recognition not for its inherent value but instead to compensate for numerous police and prosecutorial failings in the case. This unusual and mischaracterized anecdote does not override the larger issues that facial recognition introduces into the criminal legal system that defense attorneys should be aware of.

Legal and ethical concerns

1. Threats to constitutional rights.

Use of facial recognition by the defense may increase the perceived legitimacy of this tool in the hands of law enforcement. This in turn can perpetuate the ongoing harms posed by routine police use of facial recognition, which include possible constitutional violations. It may also make it difficult to challenge the validity or reliability of the technology when used in the government's case against a defendant.

Due process. Facial recognition has rarely been disclosed to defendants despite being used in hundreds of thousands of cases since 2001, sometimes as the sole means of identification. This is a due process failure — particularly, the withholding of evidence that should be considered *Brady* material. Given the persistent risk of misidentification present in a facial recognition search, its use undermines confidence in the identification process.[16]

Privacy and free speech. If used as a real-time biometric surveillance tool, police could use facial recognition to track someone's movements across time and public spaces, which may amount to a Fourth Amendment violation under the Supreme Court's holding in *Carpenter v. United States*, 138 U.S. 2206 (2018).[17] When directed at public gatherings, this type of surveillance could chill participation in First Amendment-protected activities of free speech, assembly, and association.[18]

Equal protection. A study conducted by the National Institute of Standards and Technology (NIST) in 2019 found that many facial recognition algorithms examined performed differently depending on the race, sex, and age of the person being searched.[19] Some algorithms have been found to misidentify women, Black faces, and young and old faces at higher rates than other faces.[20] Police use of a tool that performs differently depending on a person's demographics may violate the Equal Protection Clause of the Fourteenth Amendment.

2. Accuracy and bias problems.

Facial recognition suffers from accuracy and bias issues that will impact defense attorney use of the technology as it does with law enforcement applications. Facial recognition searches involve several different components, each of which impacts the accuracy of the search and can lead to misidentification. The quality of the searched-for and database photos, the accuracy of the algorithm, and the training and competence of the person running the search will all determine whether the search is reliable. How an algorithm was developed will also determine whether it exhibits race, sex, or age-based bias in its results, placing certain people at a higher risk of misidentification based on their demographics.

3. Jurisdiction-specific restrictions and professional liability risks.

Various state or local laws may constrain a defense attorney's use of facial recognition technology in different ways. The facial recognition ban in San Francisco, for example, prohibits most uses of the technology by any City official or department, which includes the Public Defender's Office.[21] Biometric privacy laws in Illinois and Texas govern a private or commercial entity's collection and use of biometric templates.[22] While these laws will primarily govern the actions of facial recognition companies and other commercial entities, they may impact certain actions of private attorneys as well. Illinois' Biometric Information Privacy Act (BIPA), for example, applies to all "private entities," defined as "any individual, partnership, corporation, limited liability company, association, or other group, however organized."[23]

In addition, the American Bar Association (ABA) Model Rules of Professional Conduct may apply to a defense attorney's use of various facial recognition tools.[24] Under ABA Rule 5.3, a lawyer is responsible for the conduct — and misconduct — of a non-lawyer, including third-party providers, if the lawyer orders or "ratifies" the conduct or could have prevented or mitigated its effects.[25] This could include a facial recognition company's actions that run afoul of state privacy or consumer protection laws. It may also apply to the performance of a facial recognition system itself, if used by an attorney or under their supervision in a manner similar to other non-lawyer assistance.[26]

Questions to Ask:

1. **What is the potential cost of using facial recognition technology?** Adoption of facial recognition by the defense could serve to legitimize its law enforcement use.

    - Defense use of facial recognition technology may help legitimize a harmful law enforcement practice and undermine future efforts to challenge police use of the technology. Police use of facial recognition, and a widespread failure of the prosecution to disclose its use to the defense, constitutes systematic violations of the due process rights of the accused. Your use of facial recognition could undermine legitimate arguments that facial recognition is unreliable, racially biased, or otherwise deficient, and may compromise your ability to successfully challenge the validity of police use of facial recognition in subsequent cases.

2. **Are there legal or other barriers to using facial recognition?** Using various facial recognition tools may violate your state's laws, executive or office policies, or rules of professional conduct.

    - Does your state or local jurisdiction have a law against government use of facial recognition or private collection of biometric or other personal data without notice to and consent of the affected person? Has a relevant agency barred the use of facial recognition by government employees?

    - Has your office adopted a policy or taken a public position against the use of facial recognition technology?[27]

    - Could using a particular tool open you up to liability under your state's rules of professional conduct?

3. **Would you actually use facial recognition?** The duty you have to your client is paramount, and that may mean considering the use of facial recognition technology in some circumstances. These cases will be rare, however, and you should also consider whether using a tool that lacks scientific validity will be persuasive.

    - Hypothetically, facial recognition could be of use if a fact pattern matches that of the Conlyn case, or to demonstrate a misidentification. These cases are likely to be rare, however, and the long-term harms of legitimizing the technology remain serious.

    - Facial recognition has not yet been established as a forensically sound method of identification, suffering from unaddressed accuracy and bias concerns. Using facial recognition to find a witness or exonerate your client, for example, may be subject to challenge based on a lack of established reliability and risk of error.

For the reasons outlined above, NACDL urges careful consideration of the non-monetary costs and potential liabilities that may arise from the use of facial recognition tools in your defense. If your office is considering a contract for a facial recognition product or using it in a specific case, NACDL can help. Contact cgarvie@nacdl.org.

Notes

[1] *See, e.g.,* Daily News Editorial Board, *Facing facts: Google's facial recognition goof*, NY Daily News (Oct. 5, 2019), https://www.nydailynews.com/opinion/ny-edit-facing-facts-20191005-waqzue2ugna7hlf3ye7h7qjsdu-story.html (arguing that "if refined, the technology holds tremendous promise both to find individuals guilty of serious crimes and to exonerate the innocent"); *see* Kashmir Hill, *Clearview AI, Used by Police to Find Criminals, Is Now in Public Defenders' Hands*, NYTimes (Sept. 18, 2022), https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html (describing the use of facial recognition by a defense attorney to find an eyewitness with information material to his client's case).

[2] For a more in-depth overview of how facial recognition works, *see* Brief of Amici Curiae Electronic Privacy Information Center, Electronic Frontier Foundation, and National Association of Criminal Defense Lawyers in Support of Defendant-Appellant, New Jersey v. Arteaga, No. A-3078-21T1 (NJ Sup. Ct. 2021), *available at* https://www.nacdl.org/brief/New-Jersey-v-Arteaga.

[3] National Institute of Standards & Technology (NIST), *Face Recognition Vendor Test Part 2: Identification*, 13 (Dec. 18, 2022), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

[4] For a more in-depth description of this issue, *see* Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Center on Privacy & Technology at Georgetown Law (Dec. 6, 2022), http://forensicwithoutscience.org/.

[5] *Id*. at 6–8.

[6] *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.

[7] Brady v. Maryland, 37 U.S. 83 (1963). *See* Brief of Amici Curiae Electronic Privacy Information Center, Electronic Frontier Foundation, and National Association of Criminal Defense Lawyers in Support of Defendant-Appellant, New Jersey v. Arteaga, No. A-3078-21T1 (NJ Sup. Ct. 2021), *available at* https://www.nacdl.org/brief/New-Jersey-v-Arteaga.

[8] *See* Carpenter v. United States, 138 U.S. 2206 (2018).

[9] *See, e.g., Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field*, Int'l Justice and Public Safety Network (June 30, 2011), *available at* https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf ("The mere possibility of [facial recognition] surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition. These potential consequences of routine surveillance are often referred to as 'chilling effects.'").

[10] For more information, *see* Kaitlin Jackson, *Challenging Facial Recognition Software in Criminal Court,* The Champion (July 2019), *available at* https://www.nacdl.org/getattachment/548c697c-fd8e-4b8d-b4c3-2540336fad94/challenging-facial-recognition-software-in-criminal-court_july-2019.pdf.

[11] Amazon Rekognition, for example, is a tool developed by AWS that performs several different functions including 1:1 photo comparison to determine whether two images depict the same person. *See Amazon Rekognition Developer Guide*, AWS, 153, https://docs.aws.amazon.com/pdfs/rekognition/latest/dg/rekognition-dg.pdf#face-feature-differences. (last accessed June 22, 2023). AWS used to market this tool to law enforcement; in June 2020, the company halted law enforcement facial recognition sales, although its 1:1 facial comparison capabilities are still available to any public user. *See* Jeffrey Dastin, *Amazon extends moratorium on police use of facial recognition software*, Reuters (May 18, 2021), https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/.

[12] *See* Kashmir Hill, *supra* note 1. Other facial recognition companies, such as PimEyes, offer related capabilities. *See* Drew Harwell, *This*

facial recognition website can turn anyone into a cop — or a stalker, Washington Post (May 14, 2021), https://www.washingtonpost.com/technology/2021/05/14/pimeyes-facial-recognition-search-secrecy/.

[13] *Id.*

[14] Interestingly, officers did collect information from the three other witnesses interviewed at the scene, though none could offer details about who was driving the car. *See* Peter Fleischer, *Search is on for Good Samaritan, witness of deadly 2017 Fort Myers crash*, WINK (May 11, 2022), https://www.winknews.com/2022/05/11/search-is-on-for-good-samaritan-witness-of-deadly-2017-fort-myers-crash/.

[15] *See* JusticeClearview, Clearview AI, https://www.clearview.ai/public-defenders (last accessed June 20, 2023).

[16] *See supra* note 4.

[17] *Supra* note 8.

[18] Police agencies themselves have recognized this. *See, supra,* note 9.

[19] Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NIST (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf.

[20] *Id.*

[21] San Francisco, CA Administrative Code § 19B.2(d) prohibits any City Department from obtaining, retaining, accessing, or using facial recognition software or information. The San Francisco Public Defender's Office is an agency of the Government of San Francisco. *See Departments*, SF.gov, https://sf.gov/departments (last accessed June 22, 2023).

[22] Illinois Biometric Information Privacy Act (BIPA), 740 ILCS 14; Texas Business and Commerce Code § 503.

[23] 740 ILCS 14. The Tex. Bus. and Comm. Code § 503 applies to all persons collecting biometric identifiers "for a commercial purpose."

[24] American Bar Association (ABA), Model Rules of Professional Conduct Rule 8.4(a) states: "It is professional misconduct for a lawyer to violate or attempt to violate the Rules of Professional Conduct … or do so through the acts of another."

[25] ABA, Model Rules of Professional Conduct Rule 5.3(c). *See* Anthony E. Davis, *The Future of Law Firms (and Lawyers) in the Age of Artificial Intelligence*, The Professional Lawyer Vol. 27, No. 1 (Oct. 02, 2020), *available at* https://www.americanbar.org/groups/professional_responsibility/publications/professional_lawyer/27/1/the-future-law-firms-and-lawyers-the-age-artificial-intelligence/.

[26] *See* Michael A. Patterson & Rachel P. Dunaway, *Understanding the Ethical Obligations of Using Artificial Intelligence*, LA Bar Ass'n Seminar (May 2019), *available at* https://fluxconsole.com/files/item/128/46566/AI-CLE-2019.pdf (examining how the use of artificial intelligence tools in the legal profession may fall within a lawyer's ethical obligations under state rules of professional conduct, including ABA Rule 5.3(c)); *see* Roy D. Simon, *Artificial Intelligence, Real Ethics*, NY SBA Journal (Apr. 2018), *available at* https://www.iadclaw.org/assets/1/7/10.5-_Simon_(Roy)-_Artificial_Intelligence_Real_Ethics.pdf (arguing that AI products "are effectively non-human nonlawyers" for the purposes of Rule 5.3 and that the rule places an obligation on lawyers to understand the limitations of a given tool and to double check the work of an AI system).

[27] *See, e.g.*, Timothy Young, *Memorandum on Ohio's Use of Facial Recognition Software*, Office of the Ohio Public Defender (Jan. 26, 2020), *available at* https://www.ohioattorneygeneral.gov/Files/Briefing-Room/News-Releases/AG-Facial-Recognition-Task-Force-Report-FINAL.aspx (stating that the state "should consider a recommendation that bans the use of facial recognition technology until the legislature expressly authorizes its use").

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**.

How to Support Our Work

You can support our mission and enhance your career by becoming a member of the NACDL. Learn more by visiting **https://www.nacdl.org/Landing/JoinNow**.

NACDL FOURTH
AMENDMENT CENTER

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