SUPREME COURT OF NEW JERSEY
DOCKET NO. 090275

STATE OF NEW JERSEY,	:
	: CRIMINAL ACTION
Plaintiff-Respondent,	:
	: On Leave to Appeal Granted From
v.	: an Interlocutory Order of the
	Superior Court of New Jersey,
TYBEAR MILES,	: Appellate Division
	:
Defendant-Appellant.	: Sat Below:
	:
	: Jessica R. Mayer, P.J.A.D.
	Patrick DeAlmeida, J.A.D.
	:

PROPOSED BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER, ELECTRONIC FRONTIER FOUNDATION, AND NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS

On the brief:
Christopher J. Frascella
Abigail Kunkler
Hannah Zhao
Michael Price
Shreya Tewari
Daniella Gordon

Christopher J. Frascella
(SBN 410442022)
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave NW
Washington, DC 20036
(202) 483-1140
frascella@epic.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

INTEREST OF *AMICI CURIAE*

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC routinely participates as amicus curiae in privacy cases throughout the country, including in New Jersey. See, e.g., Brief for EPIC, EFF, and NACDL as Amici Curiae Supporting Appellant, State v. Arteaga, 476 N.J. Super. 36 (App. Div. 2023) (No. A-3078-21); Brief for CDT, EPIC, and EFF as Amici Curiae Supporting Appellant, Facebook v. State, 254 N.J. 329 (2023) (No. A-000119-21, A-003350-20) (arguing that a wiretap order is required before law enforcement may demand prospective access to user communications); Brief for EPIC as Amicus Curiae Supporting Appellant, Bozzi v. Jersey City, 434 N.J. 326 (2021) (No. 084392) (arguing that disclosure of personal information held in a government record presents a colorable privacy claim that is not outweighed when that record is requested for commercial purposes); Brief for EPIC as Amicus Curiae Supporting Appellant, State v. Andrews, 243 N.J. 447 (2020) (No. 82209) (arguing that the Fifth Amendment protects privacy interests in cellphone passcodes); Brief for EPIC as Amicus Curiae EPIC Supporting Appellant, State v. Earls, 214 N.J. 564 (2013) (No. 68765) (arguing that

1

individuals have a reasonable expectation of privacy in the current location of their cell phones). EPIC has subject-area expertise in government use of face recognition technology. EPIC has testified on law enforcement use of face recognition technology in Congress and at state legislatures.

The Electronic Frontier Foundation (EFF) is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for over 30 years. With over 30,000 active donors, EFF represents the interests of people impacted by new technologies in court cases and broader policy debates surrounding the application of law in the digital age. EFF has special familiarity with and interest in constitutional issues that arise with new forensic technologies and the use of algorithms in criminal investigations and specifically with facial recognition. See State v. Arteaga, 476 N.J. Super. 36 (App. Div. 2023); State v. Pickett, 466 N.J. Super. 270 (App. Div. 2021); Lynch v. State, 260 So.3d 1166 260 (Fla. Dist. Ct. App. 2018). EFF also participated in the GAO's inquiry regarding forensic technology, which was prompted by concerns from elected officials about the use of these technologies in criminal proceedings, U.S. Gov't Accountability Office, GAO-20-279SP, Forensic Technology: Algorithms Used in Federal Law Enforcement (2020). And EFF has testified on law enforcement use of facial recognition in both the U.S. Senate and the

House of Representatives, as well as submitted comments to the Commission on Civil Rights. Hannah Zhao, <u>EFF Submits Comments on FRT to Commission on Civil Rights</u>, EFF (Apr. 13, 2024).[1]

The National Association of Criminal Defense Lawyers (NACDL) is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. Founded in 1958, NACDL has a nationwide membership of many thousands of direct members, and up to 40,000 with affiliates. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL has a particular interest in cases that involve surveillance technologies and programs that pose new challenges to personal privacy. The NACDL Fourth Amendment Center offers training and direct assistance to defense lawyers handling such cases in order to help safeguard privacy rights in the digital age. NACDL has filed numerous amicus briefs in the U.S. Supreme Court and New Jersey state courts on issues involving digital privacy rights, including: <u>Carpenter v. United States</u>, 585 U.S. 296 (2018); <u>Riley v. California</u>, 573 U.S. 373 (2014);

---

[1] https://www.eff. org/deeplinks/2024/04/eff-submits-comments-frt-commission-civil-rights

United States v. Jones, 565 U.S. 400 (2012); State v. Andrews, 243 N.J. 447 (2020); State v. Arteaga, 476 N.J. Super. 36 (App. Div. 2023); State v. Van Salter, No. A–3963–23, 2025 WL 1442687 (App. Div. 2025).

SUMMARY OF THE ARGUMENT

Facial recognition searches involve multiple components and steps that each introduce a significant possibility of misidentification. As a police identification technique, facial recognition searches are increasingly used as the sole or primary means of identifying a suspect. Indeed, every facial recognition search carries a serious risk of error that is often compounded by subsequent investigative steps. Moreover, no standardized protocols currently exist surrounding the use of face recognition technology by law enforcement agencies. This has resulted in numerous wrongful arrests of innocent individuals.

This Court should affirm the decision below granting Defendant's motion to compel discovery of information about the facial recognition search process. This is the only way to correct the risk of error and protect an individual's constitutional right under Brady v. Maryland, 373 U.S. 83 (1963). Without that information, Mr. Miles cannot truly understand the evidence against him or how law enforcement's use of face recognition technology may have influenced the identification in this case. Thus, denying discovery would

violate constitutional guarantees of due process. See id. at 87 ("suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment…").

The public's right to access criminal court proceedings found in the First Amendment and its corollary under the New Jersey Constitution further support discovery in this case. New Jersey's exceptional tradition favoring open court proceedings requires that information regarding forensic tools used in pretrial proceedings, like the face recognition search in this case, be disclosed as part of this right. Allowing the public to examine the details of the technology and process employed by the State will ensure fairness in the criminal system and reliability in the outcome of the proceedings.

BACKGROUND

Face recognition technology (FRT) is a tool for identifying an unknown person in a photograph or video by comparing that image against a database of images whose identities are known.[2] Face recognition searches conducted by

---

[2] This brief focuses on the definition and use of face recognition for identification, also known as 1:N (one-to-many face recognition). Other applications of face recognition include verification, or the comparison of two photos to determine whether they are the same individual, and face analysis, an attempt to label or classify individuals based on facial characteristics such as age, race, sex, emotional state, and more.

law enforcement as an investigative technique typically relies on algorithms and subjective human judgment to compare facial features and generate identification leads. The underlying presumption is that, as measured by both algorithms and humans, faces are biometrics unique to each individual and stable across time. A search process will include most or all of the following five steps: 1) probe photo selection; 2) database selection; 3) photo editing; 4) algorithmic search; and 5) human review. See Clare Garvie, A Forensic Without the Science: Face Recognition In U.S. Criminal Investigations, Geo. L. Ctr. on Priv. & Tech. 9-12 (2022) [hereinafter Forensic Without the Science].[3]

New Jersey police can run facial recognition searches against a variety of databases, including against the collaborative High Intensity Drug Trafficking Area (HIDTA) program.[4] The HIDTA draws law enforcement collaborators nationwide, including New Jersey and New York. Detectives in

_____

[3] https://mcusercontent. com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf.
[4] Information about the NYPD's program comes primarily from public records disclosed to the Center on Privacy & Technology at Georgetown Law. Clare Garvie, Garbage In, Garbage Out: Face Recognition on Flawed Data, Geo. L. Ctr. On Priv. & Tech. (2019), https://www.flawedfacedata. com/.

6

this case uploaded a social media photograph to the New Jersey/New York

HIDTA Facial Recognition database and then used both NEC and RankOne

("ROC") matching algorithms. See State Appx. Ex. A, 21-25. These are the

same algorithms that were used in State v. Arteaga, 476 N.J. Super. 36 (App.

Div. 2023), where the Appellate Division affirmed the very same discovery

requests being made in this case.[5]

ARGUMENT

I. **Each facial recognition search presents a unique risk of error that requires robust discovery to be assessed.**

Every facial recognition search is different. The number of components

required to make up each facial recognition search vary drastically from

agency to agency and case to case. The likelihood that any single facial

recognition search produces an error depends on several factors. These include

the face recognition system or software used and its specific version, the

quality and integrity of the image inserted into the system, the capabilities of

the analyst evaluating the matches, and more.

---

[5] Additionally, both NEC and ROC were used to wrongfully arrest Robert Williams in Detroit, who was falsely identified via the Detroit Police Department's facial recognition system. See Nicolás Rivero, The little-known AI firms whose facial recognition tech led to a false arrest, Quartz (Jun. 26, 2020), https://qz. com/1873731/the-unknown-firms-whose-facial-recognition-led-to-a-false-arrest.

Moreover, the disproportionate and discriminatory effects of facial recognition misidentifications are cause enough to evaluate facial recognition evidence skeptically. Facial recognition systems, which are the computer programs that conducts the matching process, are deficient at identifying people of color, women, elders, and children. One survey study even found that Black people were 100 times more likely to be misidentified than white people. Marcus Smith & Monique Mann, Facial Recognition Technology & Potential for Bias and Discrimination in The Cambridge Handbook of Facial Recognition in the Modern State 87, 91 (Rita Matulionyte & Monika Zalnieriute, eds., 2024). There have been at least eight known wrongful arrests in the United States due to inaccurate facial recognition search results and the majority of the individuals misidentified were Black.[6]

A. The accuracy of facial recognition systems utilized by law enforcement differs substantially.

---

[6] Douglas MacMillan, David Ovalle, and Aaron Schaffer, Arrested by AI: Police ignore standards after facial recognition matches, Wash. Post (Jan. 13, 2025), https://www.washingtonpost. com/business/interactive/2025/police-artificial-intelligence-facial-recognition/; *see also* Nathan Freed Wessler, Police Say a Simple Warning Will Prevent Face Recognition Wrongful Arrests. That's Just Not True, ACLU (Apr. 30, 2024), https://www.aclu. org/news/privacy-technology/police-say-a-simple-warning-will-prevent-face-recognition-wrongful-arrests-thats-just-not-true.

Every facial recognition search is comprised of a unique combination of a photograph, database, specific algorithm, and an individual analyst. The number of steps involved, and the variance within each one, creates a unique risk of bias and misidentification for each facial recognition search. See Clare Garvie, A Forensic Without the Science: Face recognition in U.S. Criminal Investigations, Geo. L. Ctr. On Priv. & Tech, 9-12 (2022). Currently, there is no way to uniformly address these errors. There are no statutory requirements, state or federal usage certifications, or consensus for the standards of an acceptable program.[7] Moreover, each step of the search creates a new risk of misidentification, which also affects the next step in the search.

1. **Probe Photo Selection**

The first step of facial recognition requires an officer or analyst to choose the photo, video still, or other image to run through the facial

---

[7] To date, the New Jersey Attorney General's Office has outlined a few guiding principles for facial recognition use by law enforcement and has banned the use of private database, Clearview AI, but no formal policy has been adopted; see Dana Difilippo, A.G. mulls statewide policy on facial recognition technology, NJ Monitor (Feb. 25, 2022), https://newjerseymonitor. com/2022/02/25/a-g-mulls-statewide-policy-on-facial-recognition-technology/; see also Richard Cowen, This N.J. town just said 'no' to facial recognition cameras on its streets, NJ.com (Jan. 3, 2023), https://www.nj. com/essex/2023/01/this-nj-town-just-said-no-to-facial-recognition-cameras-on- its-streets.html.

recognition system, called the "probe photo." The characteristics of the chosen image significantly impact the accuracy of the entire search. However, there is no minimum quality requirement for probe photos used in any law enforcement facial recognition search.

Furthermore, the few attempts at testing the accuracy of these systems have proven inadequate. The National Institute of Standards and Technology (NIST) conducts ongoing Face Recognition Vendor Tests (FRVTs), which evaluate the performance of the vendor-submitted facial recognition algorithms in a variety of different conditions. See Patrick Grother et al., Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NIST (Apr. 25, 2025).[8] The longest running tests are based on clear, high-quality frontal images. Id. at 10. Even then, NIST found a false negative rate of anywhere from .1% to 50%. Id. at 11. Error rates uniformly rose to at least 20% when low-quality or indirect probe photos were tested. Id. System accuracy has yet to be tested using probe photos more common in law enforcement investigations, such as surveillance camera stills or social media images where the subject is blurry, looking away from the camera, in poor light, partially obscured, or edited. See Garvie, A Forensic Without the Science, supra at 16.

---

[8] https://pages.nist. gov/frvt/reports/1N/frvt_1N_report.pdf.

Every subsequent step in the search is materially affected by the quality of the chosen image. The only redress to the materiality and potential inaccuracies of the probe photo selected is adequate discovery.

2. Probe Photo Editing

Law enforcement analysts may edit the probe photos prior to a search, casting further doubt on the accuracy of the facial recognition match. Companies such as Data Works Plus, used in other facial recognition cases, commonly provide photo editing software and tools with these capabilities. These tools allow significant changes to be made to an image. For example, the NYPD Facial Identification Section (FIS), has used its editing tools to 1) perform the "removal of facial expression" or "insertion of eyes" (which amounts to cutting and pasting a different person's facial features, and entirely different set of eyes, into the probe photo); 2) "creating a virtual probe," or combining face photographs of two different people to try and identify one of them; 3) using the "blur effect" to add pixels into a low quality image; 4) using the "clone stamp tool" to "create a left cheek and the entire chin area" for a subject whose face was not completely visible; and 5) using 3D modeling software to generate missing parts of a face turned away from the camera in a

probe photo. See Clare Garvie, Garbage In, Garbage Out, Geo. L. Ctr. on Priv. & Tech. (2019).[9]

In a prior case, the NYPD FIS ran a poor-quality probe photo through a facial recognition search which did not yield any usable results and so ran a photo of the actor Woody Harrelson into the system instead, because the analyst thought that the suspect looked similar to the actor. See ibid. This illustrates the ability—and willingness—of agencies to submit garbage data into their systems that would undermine the reliability and accuracy of the system.

3. Database and System Selection

The probe photo is then compared to photographs from a database, the choice of which can further amplify the risk of error and compound potential bias.

Many mugshot databases historically over-include minorities, reflecting the history of over-policing poor communities and persons of color. In New Jersey, for example, Black people are over 12 times more likely than whites to be incarcerated — the highest disparity of any state. See Ashley Nellis, The Color of Justice: Racial and Ethnic Disparity in State Prisons, The Sentencing

---

[9] https://www.flawedfacedata. com.

Project 10 (2021).[10] Given this, using facial recognition on mugshot databases will over-expose minorities to the risk of wrongful identification. Because demographic risks compound the baseline risks of misidentification from inaccurate systems and poor-quality probe images, discovery would allow individuals to meaningfully assess the risks unique to their demographics in relation to the database used.

4. Algorithmic Search

Next, law enforcement feed the probe photo into the chosen FR system, which compares the probe photo to those in the chosen database. This, again, creates conditions for material error. These systems are "black box" technologies created and controlled by private companies. While it is impossible to know exactly how the systems reach their conclusions without looking at their source code, each system can produce different results based on how the matching is conducted and how its algorithm is designed and trained.

The system's output is a "candidate list" of possible matches of photographs ordered according to the system's assessed confidence score in

---

[10] https://www.sentencingproject. org/wp-content/uploads/2016/06/The-Color-of-Justice-Racial-and-Ethnic-Disparity-in-State-Prisons.pdf.

descending order. Groundbreaking research in 2018 on facial classification

systems—which are closely related to facial recognition systems— showed

that people of color, and in particular Black women, were far more likely to be

incorrectly classified. See Joy Buolamwini & Timnit Gebru, Gender Shades:

Intersectional Accuracy Disparities in Commercial Gender Classification, 81

Proc. Machine Learning R. 1-15 (2018).[11] Because each system performs

differently under different conditions due to its algorithmic design, individuals

need detailed discovery on how the search was performed to establish the

likelihood that they were misidentified.

5. **Human Review**

The final stage of a facial recognition search involves a human analyst,

usually someone from the law enforcement agency involved in conducting the

search, who will review the probe photo and the candidate list produced by the

system for matches.

The human analyst in a facial recognition search is performing nothing

more or less than standard eyewitness identification, with all its well-known

flaws and biases. This Court has stated clearly that "eyewitness identifications

bear directly on guilt or innocence." See State v. Henderson, 208 N.J. 208, 219

---

[11] https://proceedings.mlr. press/v81/buolamwini18a/buolamwini18a.pdf.

(2011). Following a review of the scientific literature, the Court concluded that "a number of system and estimator variables can affect the reliability of eyewitness identifications" and that the State must offer proof to support the reliability of eyewitness identifications. Id. at 285, 289. This Court recently extended its guidance from Henderson to pre-trial eyewitness identifications. See State v. Washington, 256 N.J. 136, 163 (2024). All of this Court's findings concerning human memory, undue suggestiveness, racial or gender-based bias, confirmation bias, or other factors that affect eyewitness identification apply squarely to this aspect of facial recognition matching as well.

Any assumption that a "human in the loop" will correct and compensate for errors by a facial recognition algorithm is erroneous. Humans are prone to misidentifying unfamiliar faces and are subject to the same biases present in facial recognition systems. Numerous studies show that overall facial recognition search accuracy is highly dependent on the training the analyst receives for this task.

People are substantially worse at correctly identifying or distinguishing between strangers' faces than faces of those they know.[12] These errors are

---

[12] Vicki Bruce et al., Matching Identities of Familiar and Unfamiliar Faces Caught on CCTV Images, 7(3) J. of Experimental Psych.. Applied 3, 207 (2001).

magnified when variations like image quality, pose, age between photographs, or similar-looking imposters are introduced—compounding the same errors occurring at the prior stages of the search.[13] In one study testing individuals' ability to identify subjects in low-quality surveillance images, participants made correct identifications at a rate only marginally better than chance. See Garvie, Forensic Without the Science, supra at 23. Further, human analysts are prone to confirmation bias. Id. at 30. Therefore, if the algorithm involved produces a misidentification, human analysts are unlikely to disagree with it.

Worse still, experience with identifications does not improve performance. Separate studies on law enforcement and immigration agents found that individuals with years on the job performed just as poorly as non-professional participants. See Garvie, Forensic Without the Science, supra, at 23-24. And while training may help performance, available forensic facial identification training is inconsistent and lacks an evaluation scheme of effectiveness. Rather than providing a check against the deficiencies of algorithms, the "human in the loop" introduces additional vector for error in identification.

----

[13] See Garvie, A Forensic Without the Science, supra at 22; Vicki Bruce, et al., Verification of Face Identities From Images Captured on Video, 5 J. Experimental Psych. Applied 4, 349 (1999).

B. Fourth Amendment Precedent and Recent Caselaw Support Mr. Miles' Argument

Notably, the Appellate Division evaluated several of the arguments in this brief in <u>Arteaga</u>. <u>Arteaga</u> involved a similar use of the New Jersey/New York HIDTA Facial Recognition Module to identify a criminal suspect. The discovery requests in Mr. Miles' case include the same items that were explicitly affirmed in <u>Arteaga</u> as necessary discovery. <u>Arteaga,</u> 476 N.J. Super. at 61. The court found that the "evidence sought here is directly tied to the defense's ability to test the reliability of the [FRT]. As such, it is vital to impeach the witnesses' identification, challenge the State's investigation, create reasonable doubt, and demonstrate third-party guilt." <u>Id.</u> at 57.

<u>Arteaga</u> is consistent with the U.S. Supreme Court's decision in <u>Florida v. Harris</u>, 568 U.S. 237 (2013), affirming an individual's right to challenge the reliability of a narcotics-detection dog, "Aldo," used by law enforcement in their investigation. The Court emphasized that an individual "must have an opportunity to challenge such evidence of a dog's reliability," including by "contest[ing] the adequacy of a certification or training program." <u>See id.</u> at 247.

When the Court decided <u>Harris</u>, the use of narcotics-detection dogs was by no means a "new" identification system, having been regularly incorporated

in United States law enforcement investigations since at least the 1950-60s.[14]

Moreover, Florida had a "strict evidentiary checklist" to "assess the reliability

of a drug-detection dog" and required the State to "introduce[] comprehensive

documentation of the dog's prior 'hits' and 'misses' in the field." Id. at 244-

45. Yet, the Supreme Court still found these requirements lacking. It noted that

even Aldo's past field performance and satisfaction of independent evidentiary

requirements still left too large a possibility for error, as opposed to "evidence

of a dog's satisfactory performance in a certification or training program..." Id.

at 245-46.

The Court's reasoning in Harris supports discovery in this case. Unlike

narcotics-detecting dogs, facial recognition, is an emerging and evolving

technology. The New Jersey Appellate Division memorably described FRT as

"novel and untested" in Arteaga. Arteaga, 476 N.J. Supr. at 57. Neither New

Jersey nor any other entity has imposed any independent requirements for use

or required that law enforcement produce any evidence of reliable performance

and no such thing as a formal certification or evaluation exists that assesses

systems for any uniformity or measures of accuracy. Aldo and his canine

---

[14] Kevin W. Bliss, A Brief History of K-9 Units in Law Enforcement, Crim. Legal News (Apr. 15, 2023), https://www.criminallegalnews. org/news/2023/apr/15/brief-history-k-9-units-law-enforcement/.

colleagues were more strictly monitored over a decade ago, than a current technology that has already left behind a litany of grave errors in its short societal tenure to date.

Further, there are remarkable similarities between algorithmic decision-making and other investigative techniques previously evaluated in the courts, such as narcotics-detection dogs. "Without saying so explicitly, [Florida v. Harris] recognizes that finding a black box reliable requires external and independent evidence supporting reliability. A drug-sniffing dog cannot explain its decision-making, nor can a judge assess it, necessitating a reliability proxy that is trustworthy on its own." See Maneka Sinha, The Automated Fourth Amendment, 73 Emory L. J. 589, 647 (2024). Just like Aldo needed a training certification for his abilities, facial recognition algorithms should be required to prove adherence to, at the bare minimum, a certain threshold of accuracy. The instant litigation, like Arteaga, in the absence of such a standard, merely requests that the State properly disclose information about how this technology was used to identify Mr. Miles. See Brady, 373 U.S. at 87.

In another recent example, Minnesota v. Archambault, No. 62-CR-20-5866 (D. Minn. Sept. 13, 2024), the District Court of Minnesota evaluated a facial

recognition match challenge under the Frye-Mack[15] standard for scientific

reliability and determined that the technology, as used in the case, did not

"consistently and reliably produce accurate results as is required by law." See

Archambault, slip op. at 11. Furthermore, the court identified the use of facial

recognition algorithms in court as "novel" and a system that "[i]nstead of being

designed to produce accurate results, it is designed to produce possibilities." Id. at

13-14. The facial recognition "possibilities" produced in Archambault included

several extremely "low-confidence" scored matches with absolutely "nothing

preclude[ing] an analyst from using a probe photo to generate a run result of

individuals who 'match' the probe with a confidence score of less than 60%." Id. at

17-18. The fact that law enforcement is not required to seek a certain minimum

confidence score is a major source of error. It means that the algorithms can and

will return a match 100% percent of the time, even if a person is not in the

database at all. As described in Archambault, such a system "produces this cascade

of inaccurate, false positives by design." Id. at 18.

Just this year, in Ohio v. Tolbert, No. CR-24-689572-A (Cuyahoga Cty. Ct.

of Common Pleas, Jan. 9, 2025), appeal pending, the trial court granted a motion to

---

[15] See Frye v. United States, 293 F. 1013 (D.C. Cir. 1923); State v. Mack, 292
N.W.2d 764 (Minn. 1980).

suppress on the defense's challenge to a search warrant pursuant to <u>Franks v.</u>
<u>Delaware</u>, 438 U.S. 154 (1978) (regarding affidavits containing material false
statements or omissions). The search warrant in <u>Tolbert</u> relied on a facial
recognition search that yielded multiple other possible matches besides Mr.
Tolbert. It also utilized a database maintained by a private company, Clearview AI,
which disclaimed any accuracy in its matching system for purposes of courts of
law. The state omitted all of these facts from the search warrant affidavit and the
court excluded all evidence resulting from the execution of the warrant.

In sum, multiple courts have considered challenges to FRT and agree that
the possibilities of error and misleading information resulting from facial
recognition searches are unacceptable in criminal cases. Amici urge this Court to
affirm the ruling below in line with other courts in New Jersey and nationwide.

C. **Facial recognition searches routinely determine the course of
investigation and errors have resulted in numerous wrongful arrests.**

Because law enforcement uses facial recognition searches early in the
investigation, the results tend to guide the course of a case. Errors from these
facial recognition searches have already resulted in numerous wrongful arrests,
including in New Jersey. And the risk is especially high when police treat the
results as a de-facto identification of a suspect, even if officers are instructed
otherwise. <u>See</u> Garvie, <u>A Forensic Without the Science</u>, <u>supra</u>, at 3, 15. The

wrongful identification is not easily cured by further investigation, resulting in derailing human lives and wasting judicial resources.

New Jersey is no stranger to facial recognition misidentifications. The Woodbridge Police Department arrested Nijeer Parks in 2019 for a shoplifting crime after a facial recognition system incorrectly flagged him as the perpetrator. Mr. Parks was wrongly "identified" from a photo on a fake ID left at the scene by the suspect. See Kashmir Hill, Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match, N.Y. Times (Dec. 29, 2020).[16] The photo was cropped, altered, and uploaded to the facial recognition system which erroneously identified Mr. Parks as a "match." The investigating detective, compounding the many errors, wrongly confirmed that Mr. Parks was a match. Id.; see also Dillon Reisman, How Face Recognition Technology Landed One Innocent Man In New Jersey Jail For Ten Days, ACLU N.J. (May 29, 2024); Aff. of Probable Cause, State v. Parks, Police Case No. 19010123 (Woodbridge Mun. Ct. 2019); Compl. and Demand for Trial by Jury, Parks v. McCormack, No. 2:21-CV-03021 (Sup. Ct. N.J. 2020).[17] The devastating

---

[16] https://www.nytimes. com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[17] https://int.nyt. com/data/documenttools/new-jersey-facial-recognition-lawsuit-nijeer-parks-v/38ff3e74088a95a9/full.pdf.

impact of these errors cannot be overstated. Mr. Parks was jailed for 10 days

and experienced harsh treatment in custody. Moreover, his charges were

pending for nearly a year before they were finally dropped. Mr. Parks even

considered taking a plea deal despite knowing he was innocent. Khari Johnson,

How Wrongful Arrests Based on AI Derailed 3 Men's Lives, Wired (Mar. 7,

2022).[18]

These devastating consequences are not limited to the face recognition

system used by New Jersey law enforcement. Detroit police, ignominious for

wrongful arrests, conducted a face recognition much like the one in Arteaga,

476 N.J. Super. 36, while investigating the alleged grabbing and smashing of a

smartphone. That face recognition system there returned Mr. Oliver as a

supposed "match" based on a single surveillance screen-grab image. See

Elaisha Stokes, Wrongful Arrest Exposes Racial Bias in Facial Recognition

Technology, CBS News (Nov. 19, 2020).[19] Officers then presented an

eyewitness with a photo array containing Mr. Oliver's photo, along with five

other fillers, and the eyewitness *confirmed*, rather than *corrected* for, the

mistake. See Henderson, 208 N.J. at 285. Mr. Oliver was driving to work when

---

[18] https://www.wired. com/story/wrongful-arrests-ai-derailed-3-mens-lives/.
[19] https://www.cbsnews. com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/.

he was pulled over and arrested in handcuffs. Stokes, <u>supra</u>. His charges were pending for 4 months, but the detrimental impact on his life continued long after. As a result of the wrongful arrest, Mr. Oliver lost his job, home, and vehicle. <u>Ibid.</u> Even more alarmingly, there were significant visual differences between Mr. Oliver's appearance and that of the suspect from the screen-grab, including that the suspect lacked Mr. Oliver's visible tattoos. <u>Ibid.</u> Mr. Oliver's case illustrates that, in practice, human involvement is not a sufficient check against FRT errors.

Mr. Oliver's wrongful arrests came on the heels of Detroit police wrongfully arresting another innocent man. Based on an erroneous facial recognition-based identification, Robert Williams was arrested in front of his wife and two young daughters and locked up for thirty hours.[20] Tate Ryan-Mosley, <u>The New Lawsuit that Shows Facial Recognition Is Officially a Civil Rights </u>Issue, MIT Press (Apr. 14, 2021).[21] Once again, the "identification" of Mr. Williams was based on feeding a "blurry, low-quality still image from the store's surveillance video" into the Michigan Police facial recognition system. <u>Ibid.</u> And again, that identification was incorrectly confirmed in a photo array

---

[21] https://www.technologyreview. com/2021/04/14/1022676/robert-williams-facial-recognition-lawsuit-aclu-detroit-police/.

by a "witness" who was actually not even present at the time of the crime. Ibid. Mr. Williams' case resulted in a settlement prohibiting the Detroit Police Department from, among other things, relying solely on facial recognition search results to conduct arrests. Civil Rights Advocates Achieve the Nation's Strongest Police Department Policy on Facial Recognition Technology, ACLU (Jun. 28, 2024).[22]

Because FRT usage by law enforcement is a relatively new practice, there is likely an entire body of facial recognition errors that have yet to surface. These are just a few examples of the wrongful arrests that have been clearly linked to FRT errors. And like most of those wrongful arrests, they all involved Black men. The cases that are emerging, as well as the instances that will remain unreported, will likely have a disproportionate impact on and involve misidentifications of persons of color. Discovery provides the best chance to identify and mitigate the immediate and long-term harms of misidentifications by facial recognition systems.

---

[22] https://www.aclu. org/press-releases/civil-rights-advocates-achieve-the-nations-strongest-police-department-policy-on-facial-recognition-technology.

II.   Discovery is necessary in this case to allow the defendant to understand the evidence against him.

The sections above demonstrate why Mr. Miles must have access to discovery of the facial recognition process used to identify him. Any identification procedure based on a facial recognition search process contains substantial risk of error, which is potentially exculpatory. Because the identification of an individual as the suspect in a criminal case is material to guilt or innocence, information about this identification should be considered Brady material.

Because facial recognition 1) risks creating mistaken identity and 2) impacts the resulting identification that is introduced in court, information about a facial recognition search process must be disclosed in order to comply with the requirements of Brady. The state has the responsibility to disclose material information that tends to exculpate the individual accused in a criminal case and/or undermine the credibility of its witnesses. Brady v. Maryland, 373 U.S. 83 (1963); Kyles v. Whitley, 514 U.S. 419 (1995). Information is material if it tends to undermine confidence in the result of the criminal case. United States v. Bagley, 473 U.S. 667 (1985).

Information about a facial recognition search may negate guilt by suggesting someone other than the individual identified as a "match," such as someone else in the candidate list, committed the offense in question. Facial

recognition additionally produces information that may negate guilt or undermine the confidence in the result of a case as it suggests the State's reliance on an investigative process that has not been thoroughly tested and determined to be reliable.

Information about a facial recognition search additionally may be <u>Brady</u> material because the system acts as an impeachable witness. The algorithm performs the task of selecting what it calculates to be the most likely matches, out of a much larger pool of individuals and ranks these matches. The analyst then also performs a task not unlike that of an eyewitness by reviewing the candidate list, likely of similar-looking individuals, and selecting the most likely match. The analyst's competence, the suggestiveness of the candidate list, or other potentially biasing factors impact the reliability of this identification as it would that of an eyewitness reviewing a photo array.

Although neither the algorithm nor the analyst was an eyewitness to the crime, the system components may still be considered impeachable under the expert witness theory — the algorithm and analyst perform a biometric forensic search process. Like any other forensic expert, however, the analyst and algorithm must still be made available to the defense for review for impeachment purposes through cross-examination to ensure that the search process was, in fact, scientifically sound.

Disclosure of information about the facial recognition search process will not just substantially reduce the risk of misidentification but will additionally protect individuals' constitutional right to due process.

III. The public right's right to access criminal court proceedings found in the First Amendment and its corollary under the New Jersey Constitution requires disclosure

This Court should grant Mr. Miles' motion to compel to ensure that the First Amendment qualified public right of access will attach to any discovery materials regarding the face recognition search conducted in this case.

The First Amendment grants "the right to attend criminal trials" and to "'receive information and ideas'" related to those proceedings. Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 556, 576 (1980) (plurality opinion) (quoting Kleindienst v. Mandel, 408 U.S. 753, 762 (1972)). Disclosure is necessary to protect the constitutional right of the public and the press to access criminal judicial proceedings as "a presumption of openness inheres in the very nature of a criminal trial under our system of justice." Richmond Newspapers, 448 U.S. at 573; see also Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 606–07 (1982). Recognizing the important role played by public access, "the rules governing New Jersey courts have endorsed a strong and consistent policy in favor of open judicial proceedings." State v. Williams, 93 N.J. 39, 56 (1983). Allowing public access to information and materials about new technologies like FRT will

help ensure that there is meaningful oversight of the technology's widespread problems, see, supra, Part I. Concerns with the FRT systems can be efficiently audited by independent experts if they have access to these materials.

Under the Supreme Court's prevailing "experience and logic" test, the public's First Amendment right of access attaches to judicial proceedings and records where (a) the type of judicial process or record sought has historically been available to the public, and (b) the public access plays a "significant positive role" in the functioning of the process itself. Press-Enter. Co. v. Superior Court, 478 U.S. 1, 8-9, 11 (1986); see Barber v. Shop-Rite of Englewood & Associates, Inc., 393 N.J. Super. 292, 300-01 (App. Div. 2007).

A. Under the "experience" prong of the Press-Enterprise test, New Jersey's vigorous tradition of open criminal pretrial proceedings supports disclosure.

The U.S. Supreme Court grounded the First Amendment "presumption of openness [that] inheres in the very nature of a criminal trial under our system of justice" in the "unbroken, uncontradicted history" of such access, "supported by reasons as valid today as in centuries past." Richmond Newspapers, 448 U.S. at 573; see also Press-Enter. Co. v. Superior Court, 464 U.S. 501, 505-08 (1984) (discussing history of openness in criminal trials). This Court agreed, ruling that

> "a public right of access to criminal pretrial proceedings under the provisions of Art. I, par. 6 of the State Constitution, comparable to that based upon the First Amendment, can be found by addressing the same substantive concerns and employing the same analytical principles of

constitutional interpretation invoked in <u>Richmond Newspapers</u> and <u>Globe Newspaper</u>."

<u>State v. Williams</u>, 93 N.J. 39, 58 (1983).

In New Jersey, there is an "exceptionally vigorous judicial tradition in this State that favors open judicial proceedings." <u>Williams</u>, 93 N.J. at 59; <u>see also</u> <u>State v. Schmid</u>, 84 N.J. 535, 557 (1980) (noting the "exceptional vitality in the New Jersey Constitution" with respect to First Amendment rights). In observance of this tradition, this Court held that the presumption of right of access to criminal trials also applies to criminal pretrial proceedings. <u>Williams</u>, 93 N.J. at 59. This "historic and current practice" demonstrates that disclosure is supported by experience. <u>Williams</u>, 93 N.J. at 53.

The presumption of access applies broadly to all materials essential to that proceeding. <u>See</u> <u>Doe v. Pub. Citizen</u>, 749 F.3d 246, 267 (4th Cir. 2014) ("[T]he First Amendment right of access extends to materials submitted in conjunction with judicial proceedings that themselves would trigger the right to access."); <u>see also</u> <u>In re Application of WFMJ Broad. Co.</u>, 566 F. Supp. 1036, 1040 (N.D. Ohio 1983) ("Just as the Supreme Court's reluctance to embrace a 'narrow, literal conception of the [First] Amendment's terms', <u>Globe Newspaper</u> gave rise to a constitutional right of access to criminal trials, the same view could make a constitutional right to evidence an appropriate adjunct to insure that such proceedings are 'open.'").

As the Ninth Circuit recognized in <u>Woodford</u>, meaningful access to a proceeding means access to its nuts and bolts. <u>Cal. First Amend. Coal. v. Woodford</u>, 299 F.3d 868 (9th Cir. 2002). In <u>Woodford</u>, a lethal injection case, that meant a right to view "executions from the moment the condemned is escorted into the execution chamber." <u>Id.</u> at 870–871, 877. The court explained that, for the right of access to accomplish its goals, "citizens must have reliable information about the 'initial procedures,' which are invasive, possibly painful and may give rise to serious complications." <u>Id.</u> at 876–77. The same must be true for the technology relied on by the prosecution in identifying the defendant in a criminal case that also has the potential for serious complications and inaccuracies. <u>See</u>, <u>supra</u>, Part I. Just as without access to the initial procedures of an execution, "the public will be forced to rely on the same prison officials who are responsible for administering the execution to disclose and provide information about any difficulties with the procedure," without access to information regarding the face recognition system conducted in this case, the public will be forced to rely on the same government representatives who sought to use to the tool to vouch for its reliability. <u>Woodford</u>, 299 F.3d at 883. And much like prison officials, these persons "do not have the same incentives to describe fully the potential shortcomings of" their evidence. <u>Id.</u> at 884. Here, as in

<u>Woodford</u>, the government cannot deny public access to all but the ultimate output of the tool.[23]

Because New Jersey has recognized that the qualified right of public access applies to criminal pretrial proceedings, it applies, by extension, to the materials used during or in support of those proceedings as well.

B. Under the "logic" prong of the <u>Press-Enterprise</u> test, disclosure would allow the public to pay the significant role of meaningfully overseeing the criminal judicial process

Public access to information and materials about FRT has a positive role in overseeing widespread problems, <u>see</u>, <u>supra</u>, Part I, whether in the system's design or the human inputs that affect it. Allowing the public, including academics and other experts, to examine such evidence would markedly improve the reliability and fairness of such evidence in criminal proceedings.

Disclosure would achieve one of the main purposes of the First Amendment right of access, which attaches to criminal trials to allow the public to observe and

---

[23] Courts have held that the public's First Amendment right of access attaches to materials in the record of a criminal case for this reason. See, e.g., <u>In re Globe Newspaper Co.</u>, 729 F.2d 47 (1st Cir. 1984) (right of access attaches to memorandum, affidavits and transcripts in criminal case); <u>In re N.Y. Times Co.</u>, 828 F.2d 110 (2d Cir. 1987) (same for suppression motions and exhibits); <u>In re Wash. Post Co.</u>, 807 F.2d 383 (4th Cir. 1986) (same for plea agreements); <u>United States v. Peters</u>, 754 F.2d 753, 763 (7th Cir. 1985) (same for trial exhibits).

evaluate the workings of the criminal justice system—and to make changes in order to eliminate injustice. See Richmond Newspapers, 448 U.S. at 572. As the U.S. Supreme Court has explained, "the criminal justice system exists in a larger context of a government ultimately of the people, who wish to be informed about happenings in the criminal justice system, and, if sufficiently informed about those happenings, might wish to make changes in the system." Gentile v. State Bar of Nev., 501 U.S. 1030, 1070 (1991). The need for public oversight of government process is strongest in criminal trials, where the state wields its greatest power to affect individual liberty. Public access "enhances the quality and safeguards the integrity" of the judicial process, "heighten[s] public respect" for that process, and "permits the public to participate in and serve as a check upon the judicial process…." Globe Newspaper, 457 U.S. at 606.

There is immense public value in openness with forensic methodology. There is a long history of junk science employed under the guise of technological advancement in criminal cases—and of public access to and analysis of such evidence as the means to its eventual invalidation. "Since a series of high-profile legal challenges in the 1990s increased scrutiny of forensic evidence, a range of long-standing crime-lab methods have been deflated or outright debunked," including bite-mark analysis, ballistics testing, fingerprinting, and microscopic-hair-

comparison. Matthew Shaer, The False Promise of DNA Testing, Atlantic (Jun. 2016).[24]

Indeed, the U.S. Supreme Court has relied on public scrutiny of forensic processes to inform its interpretation of constitutional protections. See Melendez-Diaz v. Massachusetts, 557 U.S. 305, 319 (2009) ("Serious deficiencies have been found in the forensic evidence used in criminal trials."). And state supreme courts—as well as federal appellate courts—have equally looked to work done by the public, rather than either party or its experts in a criminal case, to determine that evidence based on specific technologies was not sufficiently reliable to be admissible into evidence. See, e.g., Han Tak Lee v. Houtzdale SCI, 798 F.3d 159, 166–67 (3d Cir. 2015) (discussing changes in "fire–science"); People v. Leone, 255 N.E.2d 696 (N.Y. 1969) (relying on commentary of outside experts to hold that evidence derived from polygraph tests was not fit for admission); People v. Davis, 72 N.W.2d 269, 281– 82 (Mich. 1955) (same).

Public scrutiny has had substantial benefits outside of the courtroom as well, leading to important improvements in investigative fields. For example, after a New Yorker article exposed a flawed case based on fire-science evidence, Texas not only

---

[24] https://www.theatlantic. com/magazine/archive/2016/06/a-reasonable-doubt/480747/.

"reconsider[ed] old cases that had been improperly handled by the original investigators," but also "reinvented itself as a leader in arson science and investigation" by "revamp[ing] the state's training and investigative standards." Jeremy Stahl, <u>The Trials of Ed Graf</u>, Slate (Aug. 16, 2015).[25]

Public access would plainly enhance the reliability of the evidence produced by algorithms, especially systems like FRT for which there have been myriad accuracy issues documented. In the context of criminal cases in which defendants and their counsel have limited resources, public access to algorithmic evidence would bolster courts' ability to "ensure that any and all scientific testimony or evidence admitted is not only relevant, but reliable," <u>Daubert v. Merrell Dow Pharm., Inc.</u>, 509 U.S. 579, 589 (1993), by providing the public with an opportunity to evaluate and test evidentiary material.

As one scholar, Erin Murphy, has explained, numerous factors that plague the defense in criminal trials—including "structural asymmetry[,] . . . scarcity of resources, weak discovery practices, and high rate of plea bargaining"—make the "adversarial process[] an inadequate safeguard of the integrity of forensic science." Erin Murphy, <u>The New Forensics: Criminal Justice, False Certainty, and the Second</u>

Generation of Scientific Evidence, 95 Calif. L. Rev. 721, 757 (2007). But experts reviewing publicly disclosed information about algorithms may not be encumbered by these obstacles and could have the time, resources, and expertise to effectively and efficiently audit the algorithm used in these systems. Independent review of documents across cases may catch errors or mistakes that would not be identifiable in one case alone. See Murphy, supra, at 773.

Allowing the public to see and scrutinize information will benefit the criminal justice system including by preventing the jury from giving it undue weight where necessary and increasing the public's confidence in the justice system more generally. Consequently, disclosure is proper considering the "significant governmental benefits, strong public policy, important social values, vigorous tradition and consistent practice of open judicial proceedings." Williams, 93 N.J. at 59.

CONCLUSION

Amici respectfully request that the court affirm the Superior Court's ruling pursuant to State v. Arteaga, and find that Mr. Miles is entitled to discovery on the details of how he was identified using a facial recognition search because the likelihood of a misidentification is a fact-specific determination that can only be made with discovery.

Dated: 05/28/2025

Christopher J. Frascella

Christopher J. Frascella
(SBN 410442022)

ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave NW
Washington, DC 20036
(202) 483-1140
frascella@epic.org

Abigail Kunkler (*PHV Pending)
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave NW
Washington, DC 20036
kunkler@epic.org

Hannah Zhao (*PHV Pending)
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy St.
San Francisco, CA 94109
zhao@eff.org
(415) 436-8333

Michael Price (*PHV Pending)
Shreya Tewari (*PHV Pending)
NATIONAL ASSOCIATION OF
CRIMINAL DEFENSE LAWYERS
1660 L St NW #12
Washington, DC 20036
mprice@nacdl.org
stewari@nacdl.org

Daniella Gordon
(SBN 39372005)
Vice-Chair, NACDL Amicus
Committee

37

McCarter & English, LLP
1600 Market Street, Ste. 3900
Philadelphia, PA 19103
dgordon@McCarter.com
(215) 979-3182

STATE OF NEW JERSEY,	:	<u>CRIMINAL ACTION</u>
Plaintiff-Respondent,	:	On Leave to Appeal Granted From
v.	:	an Interlocutory Order of the Superior Court of New Jersey,
TYBEAR MILES,	:	Appellate Division.
Defendant-Appellant.	:	Sat Below:
	:	
	:	Jessica R. Mayer, P.J.A.D. Patrick DeAlmeida, J.A.D.
	:	

CERTIFICATE OF SERVICE

Christopher J. Frascella
(SBN 410442022)
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave NW
Washington, DC 20036
(202) 483-1140
frascella@epic.org

I certify that true copies of the Proposed Brief of *Amici Curiae*

Electronic Privacy Information Center, Electronic Frontier Foundation, and the

National Association for Criminal Defense Lawyers was served by Electronic

Service or by Overnight UPS service this date upon the following:

Heather Joy Baker
Clerk of the Supreme Court
Supreme Court of New Jersey
Hughes Justice Complex
P.O. 970
25 West Market Street
Trenton, New Jersey 08625

Esther Suarez
Hudson County Prosecutor
Office of the Hudson County Prosecutor
595 Newark Ave.
Jersey City, New Jersey 07306

Colleen Kristan Signorelli
Assistant Hudson County Prosecutor
Office of the Hudson County Prosecutor
595 Newark Ave.
Jersey City, New Jersey 07306

Joel Silberman, Esq.
26 Journal Square, Ste. #300
Jersey City, New Jersey 07306

Dated: May 28, 2025   */s/ Christopher J. Frascella*
                                        Christopher J. Frascella