In The

Supreme Court of New Jersey

No. A-41-24 (090275)

STATE OF NEW JERSEY, *Plaintiff–Appellant*, v. TYBEAR MILES, *Defendant–Respondent*.	CRIMINAL ACTION ON APPEAL FROM AN ORDER ON A MOTION OF THE SUPERIOR COURT OF NEW JERSEY, APPELLATE DIVISION DOCKET NO. AM-000216-24T1 *Before*: Hon. Jessica Mayer, P.J.A.D. and Hon. Patrick DeAlmeida, J.A.D.

BRIEF OF AMICI CURIAE THE AMERICAN CIVIL LIBERTIES UNION, THE AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY, THE INNOCENCE PROJECT, AND THE COLLABORATIVE RESEARCH CENTER FOR RESILIENCE

Dillon Reisman (374142021)
Ezra Rosenberg (012671974)
Jeanne LoCicero (024052000)
AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY FOUNDATION
[redacted]
P.O. Box 32159
Newark, NJ 07102
(973) 854-1718
dreisman@aclu-nj.org

Nathan Freed Wessler*
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Fl.
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

Maithreyi Nandagopalan*
INNOCENCE PROJECT, INC.
40 Worth Street, Suite 701
New York, NY 10013
(212) 364-5340
mnandagopalan@innocenceproject.org

**Pro hac vice applications forthcoming*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

Rules

PRELIMINARY STATEMENT

When law enforcement uses facial recognition technology ("FRT") to identify suspects, it must disclose evidence related to its operation under New Jersey's broad, automatic discovery rules. That simple proposition flows naturally from *R.* 3:13-3 and *Brady*. The Appellate Division's decision in *State v. Arteaga*, 476 N.J. Super. 36 (App. Div. 2023), lays out the clear relevance of FRT-related discovery to a defendant and his ability to mount a defense.

But now the State claims a new prerogative: if the State believes that it has other, independent grounds for identifying a defendant, it asserts that any discovery about the FRT system it used in its investigation becomes "irrelevant" and not subject to disclosure. That rule disregards the importance of FRT-related discovery to the defense and would undermine discovery far beyond this immediate case. Discovery obligations, particularly those involved in the dangerous and sensitive area of eyewitness identification, cannot be predicated on whether the State believes it has enough other evidence to convict.

There must be no room for the State to second-guess its discovery obligations when it has so plainly used the FRT as a component of its investigation. This brief discusses three points highlighting the necessity of a clear, brightline rule governing FRT-related discovery.

First, the flaws inherent to FRT systems, and cognitive biases induced when investigators turn to FRT, create potent risks of misidentification and false accusation. FRT is inherently unreliable and probabilistic by its nature. It depends on the accuracy of opaque algorithms, the size and composition of messy law enforcement databases, and the subjective decisions and judgments of human analysts. FRT systems' ability to identify people is also frequently skewed for people of color—for example, the vast majority of known false arrest cases have been suffered by Black people. And when law enforcement proceeds with an FRT search despite these pitfalls, they frequently fall prey to "tunnel vision" or "automation bias." Already, FRT systems have driven the wrongful arrest and incarceration of innocent people for crimes they had no possible way of committing. (Point I).

Second, any information about an FRT system used in an investigation will undoubtedly be subject to disclosure under our State's broad discovery rules. New Jersey's criminal discovery rules hinge on the low bar of "relevance." FRT-related evidence clears that bar in numerous ways. Defendants can use FRT-related evidence to impeach the quality of the police's investigation, probe potential third-party guilt, undermine the reliability of subsequent eyewitness identifications, and more. Tybear Miles has the right to access FRT evidence to pursue any number of defense theories. But more

important, it was not the State's right to cut off discovery citing a kind of "independent source" or "inevitable discovery" doctrine that does not exist. The State's logic would undermine discovery rights far beyond the limits of this case. (Point II).

Finally, a clear rule is required because law enforcement often uses FRT in ways that escape scrutiny. New Jersey's law enforcement agencies frequently rely on FRT systems that they may claim they do not control, despite their own access to those systems. The strongest example of this is the system operated by the New York/New Jersey High Intensity Drug Trafficking Area ("NY/NJ HIDTA"), relied upon by law enforcement in the instant case, in *Arteaga* itself, and in the prominent false arrest case of Nijeer Parks in Woodbridge. As *Arteaga* held, this kind of "investigative outsourcing" does not save the State from its discovery obligations, since FRT systems used in investigations belong to the State's prosecution team for *R.* 3:13-3 and *Brady* purposes. This is a particularly acute problem in New Jersey and across the country, as law enforcement frequently evades accountability through spurious claims of trade secrecy or ignorance. (Point III).

For the above reasons, amici respectfully urge this Court to adopt the clear reasoning of *Arteaga* and affirm the trial court's discovery order.

STATEMENT OF FACTS AND PROCEDURAL HISTORY

For the purpose of this brief, amici accept the statement of facts and procedural history contained in the New Jersey Office of the Public Defender's amicus brief.

INTERESTS OF AMICI CURIAE

For over 60 years, the American Civil Liberties Union ("ACLU-NJ") has defended liberty and justice guided by the vision of a fair and equitable New Jersey for all. Our mission is to preserve, advance, and extend the individual rights and liberties guaranteed to every New Jerseyan by the State and Federal Constitutions in courts, in legislative bodies, and in our communities. Founded in 1960 and based in Newark, the ACLU-NJ is a non-partisan organization that operates on several fronts—legal, political, cultural—to bring about systemic change and build a more equitable society. The ACLU-NJ is the state affiliate of the American Civil Liberties Union, which was founded in 1920 for identical purposes.

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with more than two million members and supporters dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. Since its founding in 1920, the ACLU has appeared before the Supreme Court and other federal courts in

numerous cases implicating Americans' right to privacy, including as counsel in Carpenter v. United States, 138 S. Ct. 2206 (2018).

The Innocence Project, Inc. ("IP") is a nonprofit organization whose principal mission is to free the innocent, prevent wrongful convictions, and create fair, compassionate, and equitable systems of justice for everyone. The Innocence Project performs research and advocates—in individual cases and through legislative and administrative initiatives—for changes in laws and procedures to reduce the risk of wrongful convictions. Its research demonstrates the threat that unreliable or exaggerated forensic evidence poses to the truth-seeking function of criminal trials. To improve the integrity of convictions and reduce the risk of an innocent person being found guilty, the Innocence Project urges courts to afford accused individuals meaningful access to potentially exculpatory evidence, especially when it concerns the reliability of scientific or technical forensic evidence.

The Collaborative Research Center for Resilience ("CRCR") is a non-profit project fiscally sponsored by the Fund for the City of New York. CRCR nurtures futures that build towards a vibrant democracy and a world where everyone can thrive. The CRCR brings together collaborators across issue areas—locally and transnationally—to research technologies that shape the governance of our day-to-day lives. CRCR focuses on how to increase

participatory engagement and design in government implementation of technologies. CRCR is specifically interested in preserving avenues for democratic participation, transparency, and accountability when privatization and corporate contracting of public goods impacts fundamental rights.

ARGUMENT

I. Using facial recognition technology is inherently subjective and error-prone, and has led to misidentifications.

Facial recognition technology ("FRT") searches are not objective, deterministic processes; they are inherently subjective. Unlike investigative methods such as DNA analysis, "facial recognition is not a science."[1] As one FRT manufacturer puts it, it is more like "the 21st-century evolution of the sketch artist."[2] Search results depend on subjective human decisions at every step, from the selection of a probe photo and database to the choice of which candidate result among dozens or even hundreds to pursue.[3] FRT algorithms

[1] Roger Rodriguez, *Facial Recognition: Art or Science?*, Vigilant Solutions (Apr. 4, 2016), https://perma.cc/3J2T-U448.
[2] *Id.* at 2.
[3] *See* Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Geo. L. Ctr. on Privacy & Tech. 9-12 (Dec. 6, 2022), https://perma.cc/7S69-ATML (describing steps in a facial recognition search); Laura S. Moy, *Facing Injustice: How Face Recognition Technology May Increase the Incidence of Misidentifications and Wrongful Convictions*, 30 Wm. & Mary Bill Rts. J. 337, 342 (2021) (noting that New York Police Department's FRT system returns two hundred candidates for each search).

are not designed to, and do not, return a single definitive "match."[4] Rather, they are probabilistic systems that return several potential candidates based on an "algorithmic best guess."[5] As discussed in Point II *infra*, this means that most—sometimes all—candidates an FRT search yields are people who are *not* the person in the probe photo. By design, the algorithm produces lookalikes, and humans often err when trying to select the correct match from a candidate pool. Despite this, police have placed great weight on FRT search results, even to the point of ignoring clear exculpatory evidence. As a result, FRT has contributed to misidentifications and wrongful arrests, including in New Jersey.

A. FRT "matches" are the result of subjective human judgment applied to unreliable and often untested technology.

1. FRT searches involve several subjective human decisions.

FRT searches are not objective processes. Rather, human decisions are central to nearly every part of a search. As fellow amici explain in greater depth, each of these human decisions affects the reliability of the search and

[4] Garvie, *supra* note 3, at 11; Rodriguez, *supra* note 1, at 4.
[5] Eyal Press, *Does A.I. Lead Police to Ignore Contradictory Evidence*, The New Yorker (Nov. 13, 2023), https://perma.cc/RQ48-FZNZ; *see also* Patrick Grother, Mei Ngan & Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, Nat'l Inst. of Standards & Tech. 5 (Dec. 19, 2019), https://perma.cc/6UBY-H8YC.

the accuracy of the results. Yet without transparency about the human decisions behind the search, the algorithms used to conduct it, and the interactions between the software and the human users, it is impossible to assess a search's reliability and accuracy.

First, to conduct a search, a human user must choose a "probe" photo of the unidentified subject for the algorithm to try to "match." The quality of the probe—lighting, contrast, angle, resolution, facial expression, and partial covering of the face—heavily impacts the results.[6] Testing by the National Institute of Standards and Technology ("NIST") found that while some FRT algorithms performed well with high-quality probes taken in controlled settings, they did much worse with low-quality probes.[7] For low-quality images, like the grainy surveillance stills or low-resolution social media screenshots often used in real investigations, "recognition error rates are much higher, *often in excess of 20%* even with the more accurate algorithms."[8] On top of this, human users may edit the probe photo, adding pixels to blur or

---

[6] Garvie, *supra* note 3, at 9-10; Nat'l Acads. of Scis., Eng'g, & Med., *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance* 43, 46 (2024), https://perma.cc/NGM8-VHKK.
[7] Patrick Grother, Mei Ngan & Kayee Hanaoka, Nat'l Inst. of Standards & Tech., *NISTIR 8271 Draft Supplement: Face Recognition Technology Evaluation (FRTE) Part 2: Identification* 10 (Apr. 25, 2025), https://perma.cc/E9VH-V3EA.
[8] *Id.* (emphasis added).

sharpen parts of an image, combining elements from multiple images, or even artificially visualizing features not present in the original probe.[9] Yet "few agencies engage in a robust analysis of probe photo quality or prescribe . . . minimum photo quality standards," or impose limitations on photo editing.[10]

Human operators must also select a similarity threshold for the search. To run a search, a facial recognition system compares the "faceprint" extracted from the probe image to a database of faceprints from images of known individuals, such as arrest photos or driver's license photos.[11] The system then generates similarity scores for each comparison and outputs a list of possible matches, typically ordered by similarity score.[12] Because databases often contain millions or even billions of images, systems are programmed either with a similarity threshold that displays only possible matches exceeding that threshold, or with a numerical cutoff for the number of results to display (e.g., the top 20, 50, or 100 results).[13] Police agencies or vendors select the similarity threshold or cutoff number, and their choices can have a significant

---

[9] Garvie, *supra* note 3, at 11.
[10] *Id.* at 10.
[11] *See, e.g.*, Adam Schwartz et al., *Face Recognition Technology: Commonly Used Terms*, Electronic Frontier Foundation (Oct. 7, 2021), https://perma.cc/LNS8-KZ3C.
[12] Garvie, *supra* note 3, at 11.
[13] *Id.*

impact on the number and quality of potential matches displayed, and the likelihood that the search results will contain only false matches.[14]

The choice of database matters as well. Whether an accused appears in search results may depend on nothing more than whether their state happens to share driver's license or arrest photos with other states, or whether they have previously been arrested in a particular jurisdiction. "If the subject of an investigation is not enrolled in the searched database, any match that the system returns is necessarily a 'false positive' and may result in a misidentification."[15] Smaller databases may thus be more likely to omit the true "match" entirely, producing entire candidate lists of innocent lookalikes. Similarly, databases with limited inclusion criteria will necessarily miss a true "match" who does not meet those criteria: for instance, a mugshot database will always omit a true perpetrator with no prior arrest history. Yet increasing database size does not guarantee better identifications; larger databases may be more likely to contain the correct match, but they also contain more lookalikes, and thus may contribute to misidentifications even when the correct "match" is in the candidate list.[16] Older photos can also increase errors because of the

---

[14] *Id.*
[15] *Id.* at 10.
[16] Garvie, *supra* note 3, at 1; K.S. Krishnapriya et al., *Issues Related to Face Recognition Accuracy Varying Based on Race and Skin Tone*, 1 IEEE Transactions on Tech. & Soc'y 8, 17 (2020).

ways aging changes facial appearance.[17] Uncovering these errors is often impossible unless both the fact of the FRT search and information about its parameters and results are disclosed.

2. FRT algorithms are known to produce biased and erroneous results, which can feed into racial disparities in how they are used.

Even if human subjectivity and potential human error were not part of every FRT search, the algorithms themselves can be biased and error prone. Much depends on the algorithm used because different FRT systems built by different developers can have very different error rates. As recent testing by NIST found, "[r]ecognition accuracy is very strongly dependent on the algorithm and, more generally, on the developer of the algorithm."[18] In one instance, different algorithms tested on the same scenario exhibited error rates ranging "from a few tenths of one percent to *beyond fifty percent*."[19]

The developer of the FRT system in this case, DataWorks Plus, has already been implicated in multiple high-profile misidentifications, most notably in Detroit, where false matches generated by searches using DataWorks have led to three known wrongful arrests.[20] Following the first of

---

[17] Grother et al., *Identification*, *supra* note 7, at 12.
[18] *Id.* at 10-11.
[19] *Id.* at 11 (emphasis added).
[20] Kashmir Hill, *Facial Recognition Led to Wrongful Arrests. So Detroit Is Making Changes.*, N.Y. Times (June 29, 2024),

these, the Detroit Police Chief himself acknowledged, "If we were just to use the technology by itself, to identify someone, I would say 96 percent of the time it would misidentify."[21] Yet without access to the discovery sought, Mr. Miles and his counsel cannot probe the algorithms' reliability, ascertain if the algorithms used here are the same ones that led to misidentifications in Detroit, or determine what uses are most likely to cause errors.

FRT performance also varies by demographic. For instance, NIST found that many algorithms' error rates varied based on gender, age, and race: higher false positives occurred for women, people of color, children, and the elderly.[22] Some algorithms had false positive rates "between 2 and 5 times higher in women than men."[23] Several also exhibited "elevated false positives in the elderly and in children."[24] As to race, NIST found overall false positive rates to be "highest in West and East African people and East Asian people" and lowest

---

https://www.nytimes.com/2024/06/29/technology/detroit-facial-recognition-false-arrests.html. For documentation that the New York/New Jersey High Intensity Drug Trafficking Area program, which hosts the FRT platform in this case, uses DataWorks Plus, *see* New York City Dep't of Investigation, Off. of the Inspector Gen., *An Assessment of NYPD's Response to the POST Act* 23 (Nov. 2022), https://perma.cc/7PMB-N4VG.

[21] Jason Koebler, *Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time*, Vice (June 29, 2020), https://perma.cc/859M-CD88/.

[22] Grother et al., *Demographic Effects*, *supra* note 5, at 7-8.

[23] *Id.* at 7.

[24] *Id.* at 8.

among East Europeans for algorithms developed in the United States; for East Africans in particular, false positive rates with some algorithms were on the order of *100 times greater* than for white men.[25]

Finally, even if the algorithms were wholly unbiased, that would not undo biases in how FRT is deployed. As it is, disparities and errors inherent to the algorithms can feed into disparities in databases and police search practices. For instance, often as a result of historical over-policing, "Black people are overrepresented in many image repositories (e.g., mugshots)."[26] As such, Black people face greater risks of being erroneously included in search results and misidentified when those databases are searched.[27] Law enforcement choices as to whom to search likely compound this effect: while few agencies disclose data on FRT searches, available data suggest those searches disproportionately target people of color.[28] In Detroit, for instance,

---

[25] *Id.* at 7-8, 41.

[26] Thaddeus L. Johnson et al., *Facial Recognition Systems in Policing and Racial Disparities in Arrests*, 39 Gov't Information Quarterly, at 2 (Aug. 2022); *see also* Colleen O'Dea, *State Police Arrest, Charge More Black, Hispanic Drivers Than White*, N.J. Spotlight News (July 9, 2021), https://perma.cc/ML5Q-DSSN (documenting data from 2018 to 2020 showing that, although New Jersey state troopers stopped nearly three times as many white drivers as Black drivers, they physically searched and arrested more Black drivers than white).

[27] Johnson et al., *supra* note 26, at 2.

[28] *See, e.g.*, Alfred Ng, *'Wholly Ineffective and Pretty Obviously Racist': Inside New Orleans' Struggle with Facial-Recognition Policing*, Politico (Oct. 31,

the fact that nearly all of the Detroit Police Department's FRT searches target Black people made it virtually inevitable that Black people would bear the brunt of errors—and in fact, all three known FRT misidentifications in Detroit impacted Black people.[29]

3. FRT can contribute to cognitive errors in human investigators and to suggestive witness identifications.

Once an FRT search is completed, the biases, errors, and unconstrained subjective choices inherent in the search process can infect the entire subsequent investigation.

First, humans tend not to be very reliable at determining whether FRT search results contain a correct "match" or at selecting the correct candidate when they do. FRT systems are, by their very nature, "doppelganger" or "lookalike" finders, since they have a propensity to locate "[u]nrelated people" who "can sometimes resemble each other extremely closely."[30] Eyewitness misidentifications are a leading cause of wrongful convictions, responsible for the convictions in more than 60% of the Innocence Project's DNA

2023), https://www.politico.com/news/2023/10/31/new-orleans-police-facial-recognition-00121427.

[29] Detroit Police Dept., *Weekly Report on Facial Recognition* (Dec.18, 2023), https://perma.cc/DSZ5-L525.

[30] Moy, *supra* note 3, at 350.

exonerations.[31] This Court has taken extraordinary care to protect against unreliable eyewitness identifications. *See generally State v. Henderson*, 208 N.J. 208 (2011). FRT threatens to undermine those safeguards, as research shows that people perform poorly at identifying the correct match from FRT-generated candidate lists; critically, one study showed that when the true target was absent from the FRT-generated array, laypeople nonetheless selected a candidate over 50% of the time and even trained examiners still made a false selection nearly a third of the time.[32] *Cf. Henderson*, 208 N.J. at 234 (discussing common error by witnesses of identifying innocent people as suspects when photo array does not contain true perpetrator).

Second, despite such a high risk of error, automation bias and tunnel vision make users overly confident in "matches" they selected from FRT results.[33] Automation bias "occurs when a human decision maker disregards or does not search for contradictory information in light of a computer-generated solution which is accepted as correct," erroneously assuming the computer results are objective, unbiased, and accurate simply because they are machine-

---

[31] *Eyewitness Misidentification*, Innocence Project, 2025, https://perma.cc/W9SE-FK7H.
[32] David White et al., *Error Rates in Users of Automatic Face Recognition Software*, PLoS ONE 7-8 (Oct. 14, 2015), https://perma.cc/PHJ7-J3EP.
[33] *Cf.* Mary Cummings, *Automation Bias in Intelligent Time Critical Decision Support Systems*, Amer. Inst. Aeronautics & Astronautics 1st Intelligent Syst. Tech. Conf., at 2 (Sept. 2004) (explaining phenomenon of automation bias).

generated.[34] This can result in "decisions that are not based on a thorough analysis of all available information but that are strongly biased by the automatically generated advice."[35] For example, in the FRT context, one study asked subjects to determine whether two photos depicted the same person. Subjects were more confident that faces were similar when told that either a human or a computer had determined they were the same person, even if the prior determination was wrong; moreover, they said they "distrust[ed] human identification ability more than computer identification ability"—automation bias at work.[36]

Tunnel vision, meanwhile, is the tendency of "actors in the criminal justice system to single-mindedly focus on a suspect and build a case for conviction while ignoring evidence that points away from guilt."[37] With FRT, this means that police may proceed with an arrest based on an FRT hit even in the face of alibi evidence or other exculpatory information—or may not even bother to take basic investigative steps that could eliminate the FRT-generated

---

[34] *Id.*
[35] Raja Parasuraman & Dietrich Manzey, *Complacency and Bias in Human Use of Automation: An Attentional Integration*, 52 Hum. Factors 381, 391 (2010).
[36] John J. Howard et al., *Human-Algorithm Teaming in Face Recognition: How Algorithm Outcomes Cognitively Bias Human Decision-Making*, PLoS ONE, at 1 (Aug. 21, 2020).
[37] Brian Reichart, *Tunnel Vision: Causes, Effects, and Mitigation Strategies*, 45 Hofstra L. Rev. 451, 451 (2016).

candidate as a suspect. Officers have ignored obvious physical differences between crime-scene footage or witness descriptions of perpetrators and individuals identified through FRT, or failed to seek or confirm readily available proof of an alibi prior to making an arrest.[38] While most law enforcement agencies and FRT vendors that have spoken publicly on FRT caution against using it as the sole justification for an arrest, documented cases of misidentification (discussed *infra*) show that some police officers nonetheless do exactly that.[39]

B. Unfettered use of FRT has produced numerous misidentifications.

In recent years, several misidentifications resulting from FRT searches have revealed the recklessness of the technology and how police use it. In at least eight cases, police are known or alleged to have arrested innocent people they identified through FRT. Given that law enforcement agencies routinely fail to document or disclose their use of FRT, these are likely a fraction of the

---

[38] *See infra* Point I.B.

[39] Douglas MacMillan et al., *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/ (finding that, out of 23 police departments that maintained and produced detailed FRT-related records, "15 departments spanning 12 states" relied on facial recognition matches to arrest suspects without independent corroborating evidence, in spite of their own stated policies).

true number of FRT-based misidentifications.[40] Many of the known misidentifications—some resulting in prolonged pretrial incarceration or guilty pleas by individuals with strong evidence of innocence—exemplify the exact risk factors discussed *supra*, with algorithmic errors feeding into human cognitive bias. Nearly all known misidentifications have been of Black people.

Porcha Woodruff's case in Detroit is emblematic of the kind of tunnel vision that can lead police to proceed with getting a warrant and making an arrest despite obvious evidence of innocence. Ms. Woodruff was eight months pregnant when she was arrested on a warrant for an alleged carjacking.[41] Yet no witness statements or descriptions of the perpetrator suggested that the perpetrator had been pregnant; in fact, the perpetrator was not visibly pregnant on the surveillance video footage used to run the FRT search.[42] Despite this,

---

[40] *See* Garvie, *supra* note 3, at 9 (finding that fewer than one in five agencies who responded to records requests on FRT had ever conducted an audit on their use of FRT, and discussing exemptions to public records laws that allow many agencies not to disclose FRT-related documents); Douglas MacMillan et al., *Police Seldom Disclose Use of Facial Recognition Despite False Arrests*, Wash. Post (Oct. 6, 2024), https://www.washingtonpost.com/business/2024/10/06/police-facial-recognition-secret-false-arrest/ ("Most police departments are not required to report that they use facial recognition, and few keep records of their use of the technology.").

[41] Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, N.Y. Times (Aug. 6, 2023), https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.

[42] *Id.*

law enforcement held Ms. Woodruff in custody for 11 hours following her arrest, questioned her extensively, and seized her phone as potential evidence; her case was dismissed roughly a month later.[43]

Other cases illustrate how FRT search results can bias subsequent witness identifications. For example, in Nijeer Parks's case—the subject of recent litigation and a $300,000 settlement here in New Jersey—police used FRT to purportedly "match" Mr. Parks with a fake driver's license left behind by a shoplifting suspect.[44] The investigating detective then directly compared Mr. Parks' New Jersey state ID against the fake driver's license "and agreed it was the same person."[45] Along with an eyewitness confirming that the fake driver's license photo depicted the shoplifter (but decidedly not identifying Mr. Parks), that was enough for police to issue a warrant for Mr. Parks' arrest. Mr. Parks had an alibi capable of investigation—he had been thirty miles away making a money transfer during the crime, with a receipt to prove it—and DNA and handprint evidence from the scene would have quickly ruled him out as the suspect, but confirmation bias likely influenced the detective's

---

[43] *Id.*

[44] Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. Times (Dec. 29, 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html; *see also* Douglas MacMillan et al., *supra* note 39 (noting Mr. Parks' settlement with the township of Woodbridge).

[45] Hill, *supra* note 44.

identification and decision to seek a warrant without further investigation.[46] Mr. Parks spent ten days in jail for the police's reliance on an erroneous FRT match.[47]

In Robert Williams' case, Detroit police followed an FRT "match" with an identification procedure that was perhaps even more suspect: the witness they had "identify" Mr. Williams was not even an eyewitness to the crime.[48] Police first used a blurry still from a store surveillance video to run an FRT search for a suspected shoplifter.[49] An off-site loss prevention contractor then picked Mr. Williams from a photo lineup, but she was not an eyewitness: she had only seen the shoplifter on the same blurry surveillance video used to generate the FRT "match." When Mr. Williams was arrested and brought in for questioning, he held the surveillance still up next to his face to highlight obvious differences between his features and the shoplifter's and told police he was not the person in the image. The detectives questioning him agreed—but he was nonetheless held for 30 hours before being released on a bond. His case

---

[46] *See* MacMillan et al., *Arrested by AI*, *supra* note 39 (noting the available exculpatory evidence); Second Am. Compl. ¶ 95, *Parks v. McCormac*, No. 21-cv-4021 (D.N.J.) (ECF No. 72) (discussing alibi evidence).
[47] Hill, *Another Arrest*, *supra* note 44.
[48] MacMillan et al., *Arrested by AI*, *supra* note 39.
[49] Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. Times (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; Khari Johnson, *Face Recognition Software Led to His Arrest. It Was Dead Wrong*, Wired (Feb. 28, 2023), https://perma.cc/M95N-LEDS.

remained pending until two weeks later, when he took time off work to appear at an arraignment, only for the prosecutor to move to dismiss it.[50]

These cases illustrate the risks of permitting unfettered law enforcement use of inadequately vetted, opaque, and often unreliable technology. Without guardrails, follow-up investigation or—perhaps most critically—a minimum degree of transparency about the technology and how it is used, misidentifications and the wrongful incarcerations they produce are inevitable. Recognizing these risks, the Appellate Division in *State v. Arteaga* correctly required disclosure of the kind of FRT-related information sought here when law enforcement uses FRT to pursue an individual as a suspect. *State v. Arteaga*, 476 N.J. Super. 36, 59 (App. Div. 2022). The State now seeks to evade its obligations, although *Arteaga* made its responsibilities clear. Amici therefore urge this Court to adopt *Arteaga*'s reasoning and require that, whenever FRT is used in an investigation—whether it is the sole evidence of identification or not—information about it must be disclosed.

II. Information about the facial recognition technology must be disclosed to the defense under *Brady* and *Rule* 3:13-3.

Criminal discovery is governed in New Jersey by *Rule* 3:13-3 and the constitutional precepts flowing from *Brady v. Maryland*, 373 U.S. 83 (1963).

[50] Hill, *Wrongfully Accused*, *supra* note 49.

Under any fair understanding of those rules, information about FRT used in the course of a criminal investigation must be disclosed to defendants. The State's view to the contrary would undermine the well-reasoned holding of *Arteaga*, in which the Appellate Division explained how FRT evidence may be used to probe "the accuracy of [subsequent] eyewitness identifications, the thoroughness of the State's investigation, and the ability to prove the existence of other viable suspects." *Arteaga*, 476 N.J. Super. at 59.

Arteaga notwithstanding, the State attempts to dispose of its discovery obligations under the theory that, despite its clear use of FRT in an investigation, basic information concerning the FRT is somehow not relevant or useful to the defense and thus not subject to disclosure. But the prosecution cannot decide, unilaterally and preemptively, that its own investigative tools and tactics are "irrelevant"; nor can it pick and choose which cases require disclosure based on its own untested claims about the strength of its case. This notion is squarely false and a dereliction of the State's disclosure obligations, as a matter of both constitutional due process and court rule.

For the below reasons, amici urge the Court to adopt *Arteaga*'s reasoning and clarify it with a bright-line rule: when law enforcement uses FRT in the actual process of identifying a defendant as a suspect, information about that FRT must always be disclosed to the defense. Such a rule would recognize the

utility of FRT-related discovery and vindicate defendants' constitutional rights to a "complete defense." It would also safeguard those rights against efforts to circumvent discovery by laundering FRT searches with other witness identifications.

A. *Arteaga* properly held that FRT information is subject to discovery under *Brady*'s and *Rule* 3:13-3's requirements that a prosecutor disclose steps taken in a criminal investigation.

Pretrial discovery promotes "the search for truth" and a "just and fair trial." *State v. Scoles*, 214 N.J. 236, 251 (2013). For that reason, our state has always followed a broad, "open file" approach to pretrial discovery in criminal cases. *Id.* at 252; *see also State v. Ramirez*, 252 N.J. 277, 295 (2022). The mandate for comprehensive pretrial disclosure flows from two sources: *Rule* 3:13-3 and the *Brady* doctrine. Our discovery rules are guided by the recognition that "[a] criminal trial where the defendant does not have 'access to the raw materials integral to the building of an effective defense' is fundamentally unfair." *State in Int. of A.B.*, 219 N.J. 542, 556 (2014) (quoting *Ake v. Oklahoma*, 470 U.S. 68, 77 (1985)).

Rule 3:13-3 implements our broad approach to disclosure: it requires that any material "relevant to the issues in the case" is subject to disclosure to the defense. *Ramirez*, 252 N.J. at 296. "Relevant" materials are those that have "a tendency in reason to prove or disprove [a] fact of consequence to the

determination of the action." *State v. Desir*, 245 N.J. 179, 193 (2021). This rule, while not unlimited, captures a broad array of material. Relevance is not a high bar. *See State v. Cole*, 229 N.J. 430, 465 (2017) (Rabner, C.J., concurring); *State v. Buckley*, 216 N.J. 249, 261 (2013) ("Evidence need not be dispositive or even strongly probative in order to clear the relevancy bar."). There need only be a "logical connection between the [evidence] and a fact in issue." *State v. Bakka*, 176 N.J. 533, 545 (2003) (quoting *State v. Darby*, 174 N.J. 509, 519 (2002)).

The denial of criminal discovery is of constitutional dimension. Our federal and state constitutions guarantee criminal defendants "a meaningful opportunity to present a complete defense." *State v. Pickett*, 466 N.J. Super. 270, 302 (App. Div. 2021) (quoting *State v. Garron*, 177 N.J. 147, 168 (2003)). The State's obligations under *Brady v. Maryland*, 373 U.S. 83 (1963), are an integral part of that guarantee. The State must disclose to a defendant any evidence in its possession that is favorable to the defense and material to a determination of guilt. *Brady*, 373 U.S. at 87; *see also State v. Carter*, 69 N.J. 420, 433 (1976) (citing *Giglio v. United States*, 405 U.S. 150 (1972)).

Both impeachment evidence and exculpatory evidence "fall[ ] within the *Brady* rule." *United States v. Bagley*, 473 U.S. 667, 676 (1985). The *Brady* rule is premised on the fundamental principle that "[s]ociety wins not only when

the guilty are convicted but when criminal trials are fair; our system of the administration of justice suffers when any accused is treated unfairly." *Brady*, 373 U.S. at 87.[51] As such, the withholding constitutes constitutional error when, in its absence, someone accused of a crime cannot receive a "fair trial, understood as a trial resulting in a verdict worthy of confidence," or when the failure to disclose, "considered collectively" in the context of the other evidence, "undermines confidence in the outcome of the trial." *Kyles v. Whitley*, 514 U.S. 419, 434, 436 (1995) (citing *Bagley*, 473 U.S. at 678).[52] It is incumbent upon the prosecution to locate and disclose this information. *Id.* at 437 ("[T]he individual prosecutor has a duty to learn of any favorable evidence known to the others acting on the government's behalf in the case, including the police."). Prosecutors are exhorted to err on the side of disclosure. *See United States v. Agurs*, 427 U.S. 97, 108 (1976) ("[T]he prudent prosecutor

---

[51] A prosecutor's obligation to disclose favorable, material evidence is not limited to evidence that is admissible at trial. Inadmissible evidence that could lead to admissible evidence is encompassed under the *Brady* rule. *See, e.g.*, *United States v. Gil*, 297 F.3d 93, 104 (2d Cir. 2002) ("[I]nadmissible evidence may be material under *Brady*.") (quoting *Spence v. Johnson*, 80 F.3d 989, 1005 n.14 (5th Cir. 1996)).

[52] Some courts have held that *Brady* requires prosecutors to disclose favorable evidence to the defense irrespective of how that evidence might impact the defendant's trial. *See, e.g.*, *United States v. Bundy*, 968 F.3d 1019, 1033 (9th Cir. 2020) (quoting *United States v. Olsen*, 704 F.3d 1172, 1183 n.3 (9th Cir. 2013)) ("[T]rial prosecutors must disclose favorable information without attempting to predict whether its disclosure might affect the outcome of the trial.").

will resolve doubtful questions in favor of disclosure."); *Kyles*, 514 U.S. at 439 ("[A] prosecutor anxious about tacking too close to the wind will disclose a favorable piece of evidence. This is as it should be.") (internal citation omitted).

In *Arteaga*, the Appellate Division correctly recognized that *Brady* and *Rule* 3:13-3 require disclosure of information about FRT when it is used in an investigation or contributes to law enforcement's decision to pursue the defendant as a suspect. *Arteaga*, 476 N.J. Super. at 57. The Appellate Division reasoned that the evidence sought was "directly tied to the defense's ability to test the reliability of the FRT," and therefore had to be disclosed—even if there were "eyewitnesses who have already identified the perpetrator, and the identification found admissible under *Wade*." *Id.* (citing *United States v. Wade*, 388 U.S. 218 (1967)). The existence of witness identifications did not foreclose the possibility that FRT-related evidence could be used not only to impeach those identifications but also to "challenge the State's investigation, create reasonable doubt, and demonstrate third-party guilt." *Id. Arteaga*'s reasoning was sound, and amici urge its adoption here.

B. The FRT system used by the prosecution is unquestionably relevant and material for *Brady* purposes.

The Jersey City Police Department ("JCPD") used FRT to inculpate Mr. Miles as the suspect. The State's assertion that it can now deny access to basic

information about the FRT system as "irrelevant" not only flies in the face of constitutional requirements and court rules, but also defies all logic. Once FRT is employed, basic information about it is unquestionably relevant to the question of the suspect's identification and can serve important purposes for impeaching the State's case.

The primary use of FRT in an investigation is to assemble a list of suspect "candidates" that most resemble the image of the target suspect. The exact steps of how law enforcement uses that candidate list to zero in on a suspect can vary a great deal. In the most egregious cases of FRT misuse and misidentification, investigators hastily conclude that a candidate with a high "score" must be the target suspect and have made arrests on that basis alone.[53] In other cases, law enforcement may seek eyewitness "ratification" of their chosen candidate by presenting eyewitnesses with the candidate's image—sometimes in a photo array, other times as a single image for a "confirmatory" identification.[54]

In any of these cases, information about the FRT used bears on the question of the identification of the suspect and its reliability, as well as the reliability of the State's investigation as a whole. *Cf. Henderson*, 208 N.J. at

[53] *See* Garvie, *supra* note 3, at 7-8, 47-48 & n.353.
[54] *See, e.g.*, MacMillan et al., *Arrested by AI*, *supra* note 39.

303 (highlighting the court's special concern for ensuring the reliability of identifications). This is the conclusion of *Arteaga*, which held that disclosure of information about FRT was required even when otherwise admissible witness identifications had already taken place. *Arteaga*, 476 N.J. Super. at 57. As the Appellate Division recognized, the admissibility of the witness identifications did not preclude the defense from using the FRT evidence to challenge their reliability; nor was that the only possible use of the FRT-related discovery, which the defense could also use to attack the quality of the State's investigation or point to third-party guilt. *Id*. Other courts have also begun to recognize the importance of robust discovery and reliability assessments for FRT when police use it in the course of selecting an investigation's target. *See United States v. Sgt. Michael S. Delisfort U.S. Army*, No. ARMY MISC 20240488, 2025 WL 1305323, at *5 (Army Crim. App. May 5, 2025) (concluding government's failure to disclose FRT information prejudiced defendant);[55] Order at 14, *State v. Archambault*, No 62-CR-20-5866 (Minn.

[55] Per *R.* 1:36-3, amici cite this unpublished opinion to demonstrate other courts' approaches to similar legal and factual circumstances. Amici know of no opinions contrary to this limited proposition.

Dist. Ct. 2d. Jud. Dist. Sept. 13, 2024) (finding FRT unreliable under Minnesota's admissibility standard for scientific or technical evidence).[56]

Practically speaking, FRT-related information can bear on a case in any number of ways. Defense counsel can use the FRT evidence to cast doubt on the thoroughness and accuracy of the police investigation by, for example, showing that law enforcement failed to investigate numerous other individuals on the potential match list who either "scored" higher or better resembled the suspect's photograph, pointing to potential third-party guilt. Further information about the analysis process can shed light on whether analysts overlooked potential candidates for reasons of bias or other unknown reasons or whether a composite or edited photo was improperly used in the analysis.

Alternatively, information about the size and composition of the candidate pool used by the FRT system can be used to challenge the overall reliability and thoroughness of the search. If a candidate pool is small or otherwise skewed in who it covers (e.g. if the candidate pool contains mugshots from one jurisdiction but not another or if parts of the candidate pool are sourced from low-quality images), those can all bear on the likelihood that

[56] Per *R.* 1:36-3, amici cite this unpublished opinion to demonstrate other courts' approaches to similar legal and factual circumstances. Amici know of no opinions contrary to this limited proposition.

the FRT may have missed the target suspect.[57] Even basic information, too often shielded from defendants, about how to interpret similarity scores or rankings and about the underlying algorithm's reliability as measured in validation testing (including testing for racial bias and performance varying on probe image quality) shed important light on the limitations of the FRT system.

Crucially, much of the FRT evidence can be used to probe whether the FRT merely found a doppelganger of the target suspect. Despite the State's contentions, the doppelganger problem does not go away, and FRT evidence does not become irrelevant, just because eyewitnesses or people familiar with the candidate somehow "ratify" the FRT candidate. There can be no true "independent" eyewitness identification once FRT is involved, for the simple reason that FRT searches are designed to find "lookalikes" capable of fooling witnesses and even people familiar with the accused. In other words, FRT can yield a false match that can fool witnesses; those witness identifications can then serve as flawed and circular "confirmations" of an FRT result, providing a parallel and purportedly independent source of the identification despite being influenced by that very result.[58] That is why *Arteaga* recognized that the FRT

---

[57] *See supra* Point I.A.1.

[58] *Cf.* Natasha Babazadeh, *Concealing Evidence: "Parallel Construction," Federal Investigations, and the Constitution*, 22 Va. J. L. & Tech. 1, 8-9 (2018) ("Parallel construction is a law enforcement process of building a separate and

evidence is "relevant to [the] defendant's ability to impeach" an eyewitness's supposed identification. *Arteaga*, 476 N.J. Super at 61.

The FRT information is just as relevant to challenging Mr. Miles' identification and the State's investigation as it was in *Arteaga*. *Arteaga* concerned the use of an FRT-generated mugshot in a photo array, where it was subsequently chosen by eyewitnesses. *Id.* Here, the use of FRT bore on two different identification processes undertaken by JCPD, each with the goal of identifying the target suspect seen in a surveillance video. First, after a confidential informant identified the person in the surveillance video as a person he knew by the street name "Fat Daddy," officers used a photo from an Instagram account they believed belonged to "Fat Daddy" in an FRT search. Pb1. They then showed Mr. Miles' mugshot, obtained from the FRT search, to the confidential informant, who identified defendant as "Fat Daddy." Pb1. Second, thanks to the FRT match, JCPD approached Mr. Miles' sister and ex-girlfriend and presented them with the original surveillance video. *Id.*

Is Mr. Miles the person in the surveillance video? This issue may be the heart of this case. It may be that Mr. Miles is not the true identity of "Fat Daddy," whom the CI and one other witness identified in the surveillance

---

parallel evidentiary basis for a criminal investigation to conceal how the investigation actually began . . . .").

video. To make a "complete defense," information about the FRT used will help him contest that the FRT identified the correct person from "Fat Daddy's" Instagram page. He may use the FRT information to argue that FRT produced a doppelganger that misled the CI and the other witness; that the analyst chose him as a match for reasons of bias or FRT inaccuracy; that other viable candidates were overlooked; that the FRT search was not likely to find the true identity of "Fat Daddy" because of a limited candidate pool, an insufficiently clear photo, or inadequate vendor evaluation; or that police biased subsequent identifications by consciously or unconsciously signaling that they already believed the witnesses making those identifications were familiar with the person in the surveillance video.

Regardless, it cannot be the role of the prosecution to unilaterally decide, in advance of trial and in an effort to preempt its discovery obligations, what the defense's use of the FRT information should or should not be. Nor should the defense have to divulge its current theory of the case or planned trial strategy simply to obtain discovery plainly required under *Rule* 3:13-3. *Cf. Delisfort*, No. ARMY MISC 20240488, 2025 WL 1305323, at *5 (upholding dismissal of criminal case as sanction for Government's failure to timely disclose information about FRT search, and crediting trial judge's finding that defense was prejudiced by having "to reveal its trial strategy to the

Government to proffer evidence in support of the Government's alleged discovery violations," thereby "weaken[ing]" its ability to present a full defense).

The subsequent identifications of Mr. Miles' sister and ex-girlfriend do not lessen the relevance of the FRT evidence. Mr. Miles' case, in fact, bears striking similarities to the identification process that led the FBI to arrest Steven Talley, a man wrongfully accused of two bank robberies using both forensic facial analysis and an identification by his estranged wife. Mr. Talley was identified—wrongly—by two anonymous tipsters as the perpetrator of a pair of bank robberies in Denver after police aired clips of the surveillance footage.[59] Subsequently, Mr. Talley's ex-wife also identified him *directly from the video*, as did a forensic analysis unit at the FBI that compared his photograph with the footage. Yet evidence later emerged to show that Mr. Talley had provable alibis during both bank robberies.[60] Neither his ex-wife's longstanding familiarity with Mr. Talley nor the specialized training of the FBI forensic team had prevented them from misidentifying him on the video.

---

[59] Kirk Mitchell, *Man Sues FBI and Denver Police for $10 Million Claiming False Arrest for 2 Bank Robberies and Excessive Force*, Denver Post (Sept. 15, 2016), https://www.denverpost.com/2016/09/15/fbi-denver-police-sued-false-arrest-excessive-force; Moy, *supra* note 3, at 363.
[60] Mitchell, *supra* note 59.

Similarly, the identifications in this case cannot be presumed correct, nor should they foreclose a thorough defense review of the FRT search.

C. The State's attempt to deny the FRT discovery behind the pretext of "irrelevance" denies defendants due process.

The State seeks to withhold evidence on the tool that led its investigation to Mr. Miles—FRT—simply because it has other evidence that it has deemed unassailable. But that (a) is not the logic of discovery and (b) makes a mockery of defendants' due process rights. Once an indictment issues, defendants are entitled to "automatic and broad discovery of the evidence the State has gathered in support of its charges." *Scoles*, 214 N.J. at 252. There is no room for the State to say, in essence, "Yes, but our case is so strong that we have decided there is no use in this evidence to challenge it"; such an approach would short-circuit the discovery process by predicating defendants' due process rights on the State's perception of its own case's strength. And when so many of the ways FRT can bias an investigation are unconscious, *see* Point I.A.3 *supra*, the very party susceptible to that unconscious bias cannot be the arbiter of whether FRT-related information should be disclosed. Rather, evidence bearing on an FRT search should be disclosed whenever FRT is used in an investigation or contributes to the selection of a suspect.

Fortunately, our discovery jurisprudence recognizes that defendants require automatic discovery only limited by the low bar of "relevance," to

ensure that our system's "quest for truth" is served. *Ramirez*, 252 N.J. 277, 295 (2022); *see also State v. Bakka*, 176 N.J. 533, 545 (2003) (quoting *State v. Darby*, 174 N.J. 509, 519 (2002)). Despite the State's suggestions otherwise, "relevance" does not require that evidence prove an alternative theory of the case or even raise a "strong probability" that the State's case is wrong; the touchstone of relevance is that the evidence "need only *tend to* create a reasonable doubt." *State v. Jorgensen*, 241 N.J. Super. 345, 351 (App. Div. 1990) (quoting *Johnson v. Unted States*, 552 A.2d 513, 517 (D.C. 1989)).

These rules demand a clear result when it comes to FRT evidence: no matter how FRT results themselves are subsequently used by the police or prosecution in an investigation, evidence about any FRT system used by the police will *always* bear a logical connection to the defendant's identification. Amici urge the Court to adopt a bright-line rule that FRT-related evidence is always subject to automatic discovery whenever it is used in an investigation.

Any other rule would give space for prosecutors to dodge discovery responsibilities by making unchallengeable assertions about the defense's theory of the case and the outcome of trial, all before the defendant has had any benefit of due process. This is constitutionally intolerable for several reasons. First, the prosecutor "presumably knows very little" about the defendant's case before it is made. *U.S. v. Bagley*, 473 U.S. 667, 701 (1985)

(Marshall, J., dissenting). Thus, under *R.* 3:13-3, the State must be barred from weighing the disclosure of evidence in light of how it might *hypothetically* fit into the defendant's theory of the case and how it might *hypothetically* be presented to a jury. Cases applying *Brady* have also made this clear: even under *Brady*'s stricter standards, the prosecution's due process obligations are predicated on whether the evidence "could reasonably be taken to put the *whole case* in such a different light as to undermine confidence in the verdict." *Kyles*, 514 U.S. at 435 (emphasis added). How a particular piece of evidence might bear on the defense's overall case is fundamentally unknowable by prosecutors making discovery decisions. *See Agurs*, 427 U.S. at 108 ("[T]he significance of an item of evidence can seldom be predicted accurately until the entire record is complete").

Second, lack of transparency regarding FRT is already a widespread problem, which would only grow worse if the prosecution could selectively decide when to disclose information about it. A recent investigation by the Washington Post obtained records on FRT use from police departments in 15 states and found that, although the records documented "use of [FRT] in more than 1,000 criminal investigations over the past four years . . . , authorities

routinely failed to inform defendants about their use of the software."[61] In fact, police "often obscured their reliance on the software in public-facing reports," instead claiming that the identification came from a human source or other unspecified "investigative means."[62] For instance, in Randal Quran Reid's case, the officer who sought his arrest warrant based on an erroneous FRT "match" made no mention of FRT in his warrant affidavit, stating only that the identification came from "a credible source"; Mr. Reid was then arrested for thefts in a state he had never visited.[63] Law enforcement agencies themselves may not even know how their officers use FRT: the Georgetown Center on Privacy and Technology surveyed several state and local law enforcement agencies in 2016 and found that only nine of 52 responding agencies had ever audited how their personnel used FRT.[64]

Finally, prosecutors are, by necessity, caught in a tension between their roles as "zealous advocate[s]" who "aggressively seek convictions in court" and as "representative[s] of the state" who must prioritize "the determination

---

[61] MacMillan et al., *Police Seldom Disclose Use of Facial Recognition*, *supra* note 40.
[62] *Id.*
[63] Kashmir Hill & Ryan Mac, *'Thousands of Dollars for Something I Didn't Do'*, N.Y. Times (Apr. 6, 2023), https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html.
[64] Garvie, *supra* note 3, at 9.

of truth." *Bagley*, 473 U.S. at 696 (Marshall, J., dissenting); *see Berger v. United States*, 295 U.S. 78, 88 (1935) (characterizing prosecutors as "the representative[s] . . . of a sovereignty . . . whose interest . . . in a criminal prosecution is not that it shall win a case, but that justice shall be done."). Even assuming "absolute good faith" on the part of the prosecutor does not obviate the concern that this dual role might lead to the improper suppression of evidence. *Bagley*, 473 U.S. at 697 (Marshall, J., dissenting). It is a "curious" aspect of *Brady* that the defendant's constitutional rights depend so heavily on the evaluation of a conflicted party. *Id.* This is why *Brady* requires prosecutors to err on the side of disclosure. *See Agurs*, 427 U.S. at 108.

In this light, it is particularly inappropriate for the State to invoke the "inevitable discovery" doctrine to cut off Mr. Miles' due process rights.[65] The "inevitable discovery" doctrine has no bearing on a *Brady* or *Rule* 3:13-3 analysis. Rather, in the Fourth Amendment context, the "inevitable discovery" doctrine balances the need for deterring unconstitutional police conduct against the "social costs associated with the exclusionary rule" when police can make a showing they would have discovered illegally obtained evidence regardless. *State v. Sugar*, 100 N.J. 214, 237 (1985). In other words, even in

[65] 2T21:3-7 ("THE COURT: You mention independent. Are you arguing now some kind of inevitable discovery, independent of the facial recognition software? [STATE]: That's, ultimately, the State's argument . . . .").

that context, the "inevitable discovery" rule exists to serve the truth. Here, the State essentially invokes "inevitable discovery" to *hide* the truth. It argues that its investigation *could have* proceeded differently, conflating "inevitable" with merely *possible* or *potential* discovery. But in reality, the State used FRT. A defendant must therefore have the opportunity to probe and impeach that real investigation. The State cannot point to the hypothetical ways an investigation could have gone to avoid disclosure.

For those reasons, the Court should recognize the FRT evidence for what it unquestionably is: relevant discovery material that must be disclosed.

III. The State cannot circumvent FRT discovery obligations by outsourcing the technology to out-of-state entities.

The prosecution's discovery obligations under *Rule* 3:13-3 and *Brady* extend to items held by any law enforcement personnel who are part of the prosecution team. The duty to provide exculpatory information "is not limited to items 'within the possession, custody or control of the prosecutor,' *R.* 3:13-3(b)(1)(C)." *State v. Washington*, 453 N.J. Super. 164, 184 (App. Div. 2018). Rather, documents and other evidence of which the prosecution "is actually or constructively aware," *State v. Robertson*, 438 N.J. Super. 47, 69 (App. Div. 2014), must also be disclosed if held by another law enforcement agency that has "act[ed] on the government's behalf in the case," *Kyles*, 514 U.S. at 437.

The concept of the "prosecution team" has never been as important as it is in our current era of widespread interagency data-sharing. Modern police departments frequently "outsource" control of investigative tools to extra-jurisdictional agencies or law enforcement task forces. Those agencies in turn may rely on opaque investigative tools from private software vendors, who often resist revealing any information about their tool on excessive claims of trade secrecy. Safeguarding due process requires that courts enforce the prosecution's well-established burden to obtain and disclose evidence held by any such entities acting at its direction.

Law enforcement agencies in New Jersey have evaded accountability for their use of FRT precisely because of this sort of "investigative outsourcing." Local law enforcement agencies have relied on advanced investigative tools like FRT that are not directly housed within the agency. The result has been a kind of accountability shell game as those agencies disclaim any knowledge of the tool. Unfortunately, this is a pattern that has arisen in multiple FRT-related cases in New Jersey. *See Arteaga*, 476 N.J. Super. at 42-43; Amicus Curiae Brief of the American Civil Liberties Union and the American Civil Liberties Union of New Jersey in Support of Plaintiff's Opposition to Defendants' Motion for Summary Judgment, *Parks v. McCormac*, No. 2:21-cv-04021-JKS-LDW (D.N.J. Jan. 29, 2024) (ECF No. 113). We urge the Court to reaffirm and

strengthen the holding of *Arteaga* to make it clear that any FRT tool relied upon in an investigation is fairly within the "constructive awareness" of the prosecution team, claims of trade secrecy notwithstanding.

A. *Brady* and discovery obligations extend to any agency that played a role in the "prosecution team."

As the Appellate Division in *Arteaga* correctly recognized, the State cannot evade its *Brady* and discovery obligations by enlisting other agencies to undertake parts of the investigation at its behest. *Arteaga*, 476 N.J. Super. at 57. In *Arteaga*, the local law enforcement agency investigating the case first requested an FRT search from the New Jersey Regional Operations Intelligence Center (NJROIC); when the NJROIC investigator reported no matches, a similar request went to the New York Police Department Real Time Crime Center (NYPD RTCC), which returned Mr. Arteaga as a "possible match." *Id.* at 42-43. The Appellate Division rejected the State's argument that the NYPD RTCC was not part of the prosecution team, pointing out that "the prosecutor sent a request to the NYPD RTCC, which in turn complied by producing the information used to accuse" Mr. Arteaga. *Id*. at 57. Moreover, the prosecutor—as here—did obtain some of the discovery materials sought from the NYPD RTCC. *Id*. The Appellate Division therefore rejected the assertion that the defense should have to subpoena the rest, holding that "the burden lies with the State given the fact FRT is novel and untested." *Id.*

The Appellate Division's reasoning applies with equal if not greater strength here. In this case, a JCPD officer directly performed the FRT search, accessing the software through a portal administered by the NY/NJ HIDTA. The NY/NJ HIDTA system includes mugshots of formerly detained people across much of New York and New Jersey, including people who were never convicted.[66] If the explicit request from one agency to another in *Arteaga* was enough to establish the NYPD RTCC as part of the prosecution team, JCPD's direct access to the NY/NJ HIDTA FRT portal is more than sufficient here. The State was no passive or accidental recipient of information held by another. When the State explicitly requests an FRT search from another entity or, as here, directly accesses FRT software hosted by that other entity to perform its own search, it makes that entity part of the prosecution team for purposes of FRT-related discovery.

This pattern is evident in other recent FRT cases. *Arteaga* itself, as noted, involved an FRT search request from a New Jersey agency to the NYPD. *Arteaga*, 476 N.J. Super. at 43. Similarly, the FRT-based wrongful arrest of Nijeer Parks in Woodbridge Township involved a law enforcement request made to the Rockland County Intelligence Center. *See* Amicus Curiae

[66] *See, e.g.*, *State v. Green*, 239 N.J. 88, 92 (2019) (noting that New Jersey police departments like Newark's contribute mugshots to the NY/NJ HIDTA's "PhotoManager System").

Brief of the American Civil Liberties Union and the American Civil Liberties Union of New Jersey in Support of Plaintiff's Opposition to Defendants' Motion for Summary Judgment, *Parks v. McCormac*, No. 2:21-cv-04021-JKS-LDW (D.N.J. Jan. 29, 2024) (ECF No. 113). In both cases, these interagency requests took advantage of the NY/NJ HIDTA system.

The instant case involves that same system, which is plainly part of the "prosecution team" in any case where it is used. The NY/NJ HIDTA is an amorphous creature of federal law: HIDTAs are not "entities unto themselves," but are rather a vehicle for federal funding to be put toward joint initiatives by groups of federal, state, local, and tribal law enforcement agencies. *See, e.g.*, *Milteer v. Navarro Cnty., Tx.*, 99 F.4th 268, 273 (5th Cir. 2024). They are controlled by a board of their law enforcement members, and though they may appear to have a life of their own, they are not distinct legal entities but rather an arm of the constituent agencies. *See id.* at 274 (finding in a case concerning the management of a HIDTA, the actions of the HIDTA can be "imputed" to the local law enforcement agency). Responsibility for the NY/NJ HIDTA's functions is diffuse and distributed among the agencies that participate in it.[67]

[67] *See, e.g.*, BOTEC Analysis Corporation, *Assessment of the HIDTA Program: High Intensity Drug Trafficking Areas*, at 102 (June 30, 2001), https://www.ojp.gov/pdffiles1/nij/grants/194118.pdf (submitted to Dep't of Just. Apr. 2002).

As such, the burden of obtaining information about the NY/NJ HIDTA's FRT platform belongs to the entities with decision-making power over how the HIDTA should function and whether to join it in the first place—that is, law enforcement agencies like JCPD and, by extension, the State.

Permitting the State to escape discovery obligations by outsourcing portions of its investigations would exacerbate the asymmetry in evidence access that already exists between the prosecution and defense. The State—prosecutors and law enforcement agencies—has the power to determine whether to contract for a particular technology, which vendors to use, and whether and how to share data or access to technology with other law enforcement agencies. When executing software licenses, vendor contracts, or interagency memoranda of understanding, the State has both information access and negotiating power that defendants wholly lack. These factors already produce asymmetries of information that favor the prosecution and disadvantage defendants. The State cannot then exploit them further by claiming they are grounds to avoid discovery.

B. The State cannot use trade secrets claims to evade constitutional obligations.

As a final matter, to the extent the State may seek to avoid disclosure of the FRT information sought on the grounds that this information includes trade secrets belonging to FRT vendors or developers, trade secrets claims cannot

supersede the fundamental right to due process. *See Pickett*, 466 N.J. Super. at 304-05. To an ever-greater degree, law enforcement agencies are turning to technological tools developed by private vendors to complete investigative and surveillance tasks that historically would have been the province of the agencies themselves—or that would have been logistically impossible.[68] Yet despite their increasingly integral role in police investigations, developers of software and other technologies often seek to shield their products from court scrutiny.[69] This creates a fundamental due process problem: defendants cannot meaningfully evaluate the reliability of the evidence against them, let alone challenge it, when courts put trade secrets claims above the fundamental constitutional rights of the accused.

New Jersey has already recognized this problem and taken efforts to safeguard due process against over-expansive trade secrets claims. In another recent case dealing with opaque software, in that instance a probabilistic genotyping program, the Appellate Division ordered disclosure of the software's source code. *Pickett*, 466 N.J. Super. at 323-24. The Appellate Division first noted that the party seeking to assert the trade secrets privilege

---

[68] Rebecca Wexler, *Life, Liberty, and Trade Secrets*, 70 Stan. L. Rev. 1343, 1346-48 (2018) (detailing several examples of growing automation and technology use in policing and the criminal legal system).

[69] *See id.* at 1360-62 (documenting cases in which companies invoked the trade secrets privilege to avoid disclosing details about their software to defendants).

bears the burden of showing that the information at issue is subject to the privilege. *Id.* at 304. But the Appellate Division then emphasized that, "even once that showing of privilege is made, a criminal defendant should nonetheless be entitled to discovery of the information sought to the extent necessary to ensure a fair trial." *Id.* at 304-05. The Appellate Division's reasoning was sound and applies equally to FRT algorithms developed by private vendors.

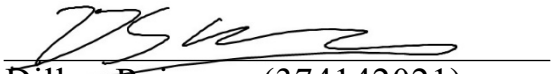
If law enforcement is permitted to evade discovery by asserting that tools they use are in the possession or control of a private company—while the private company simultaneously avoids scrutiny by asserting the trade secrets privilege—then an increasing amount of the evidence used to develop and pursue prosecutions will become entirely inaccessible to the people facing those prosecutions. This is a recipe for a criminal legal system that is opaque, unaccountable, and rife with the risk of wrongful conviction. Amici urge this Court not to take this path, but rather to uphold due process and meaningful access to evidence in the face of increasingly complex contractual arrangements.

CONCLUSION

For the reasons set forth above, the Court should affirm the order to produce discovery and require the State to disclose all FRT evidence sought.

Dated: May 28, 2025

Respectfully submitted,



Dillon Reisman (374142021)
Ezra Rosenberg (012671974)
Jeanne LoCicero (024052000)
AMERICAN CIVIL LIBERTIES UNION
OF NEW JERSEY FOUNDATION
[redacted]
P.O. Box 32159
Newark, NJ 07102
(973) 854-1718
dreisman@aclu-nj.org

Maithreyi Nandagopalan*
INNOCENCE PROJECT, INC.
40 Worth Street, Suite 701
New York, NY 10013
(212) 364-5340
mnandagopalan@innocenceproject.org

Nathan Freed Wessler*
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Fl.
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

Attorneys for Amici Curiae American Civil Liberties Union, American Civil Liberties Union of New Jersey, Collaborative Research Center for Resilience, & Innocence Project

**Pro hac vice applications forthcoming*