NOT FOR PUBLICATION WITHOUT THE
APPROVAL OF THE APPELLATE DIVISION

SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION
DOCKET NO. A-3078-21

STATE OF NEW JERSEY,

Plaintiff-Respondent,

v.

FRANCISCO ARTEAGA,

Defendant-Appellant.

APPROVED FOR PUBLICATION
June 7, 2023
APPELLATE DIVISION

Argued May 15, 2023 — Decided June 7, 2023

Before Judges Whipple, Mawla, and Walcott-Henderson.

On appeal from an interlocutory order of the Superior Court of New Jersey, Law Division, Hudson County, Indictment No. 21-01-0035.

Tamar Y. Lerer, Assistant Deputy Public Defender, argued the cause for appellant (Joseph E. Krakora, Public Defender, attorney; Tamar Y. Lerer and Elizabeth C. Jarit, Deputy Public Defender, of counsel and on the briefs).

Patrick Galdieri, Assistant Prosecutor, argued the cause for respondent (Esther Suarez, Hudson County Prosecutor, attorney; Kevin Robert Sipe, Assistant Prosecutor, on the brief).

American Civil Liberties Union of New Jersey Foundation, Tania Brief (Innocence Project, Inc.) of the

New York bar, admitted pro hac vice, Anton Robinson (Innocence Project, Inc.) of the New York bar, admitted pro hac vice, Somil Trivedi (American Civil Liberties Union Foundation) of the District of Columbia bar, admitted pro hac vice, and Nathan Freed Wessler (American Civil Liberties Union Foundation) of the Massachusetts and New York bars, admitted pro hac vice, attorneys for amicus curiae American Civil Liberties Union, American Civil Liberties Union of New Jersey and Innocence Project (Alexander Shalom, Jeanne LoCicero, Molly Linhorst, Dillon Reisman, Tania Brief, Anton Robinson, Somil Trivedi, and Nathan Freed Wessler, on the brief).

Pashman Stein Walder Hayden, Jacob Wiener (Electronic Privacy Information Center) of the District of Columbia bar, admitted pro hac vice, Jennifer Lynch (Electronic Frontier Foundation) of the California bar, admitted pro hac vice, Hannah Zhao (Electronic Frontier Foundation) of the New York bar, admitted pro hac vice, and Clare Garve (National Association of Criminal Defense Lawyers) of the New York bar, admitted pro hac vice, attorneys for amicus curiae Electronic Privacy Information Center, Electronic Frontier Foundation and National Association of Criminal Defense Lawyers (Christopher J. Frascella, Jacob Wiener, Jennifer Lynch, Hannah Zhao, Alan Silber, and Clare Garvie, on the brief).

The opinion of the court was delivered by

MAWLA, J.A.D.

We granted defendant Francisco Arteaga leave to appeal from a May 13, 2022 order, denying his motion to compel the State to provide discovery related to the facial recognition technology (FRT) used to develop a picture of him,

which was then used to identify and charge him. We reverse and remand for further proceedings consistent with this opinion.

On November 29, 2019, a man entered a store in West New York, which offered international wire transfers, cell phone repairs, and accessories. He approached the rear counter and asked an employee, Yennifer Vasquez-Arias, who was counting money, about wiring funds to South America. When she turned toward her computer, he walked toward an open door behind the counter. She assumed he was headed to see the technician in the cell phone repair area of the store. However, the door also led to an office, which contained a cash register. The man surprised Vasquez-Arias with a handgun and grabbed the money she had just counted. She tried to stop him, but he pistol-whipped her, lacerating her left ear, and escaped with $8,950.

When a police detective arrived, Vasquez-Arias described the man as a "Hispanic male wearing a black skully hat" and carrying a black handgun. She recalled he entered the store earlier in the day, stood at the end of a line of customers, and left before he could be served.

Store manager Judy Cardozo was not present for the robbery, but when reviewing surveillance footage of the incident, thought she recognized the perpetrator. She recalled that a man, who she believed to be the same person,

approached her during a prior visit, nervously asked about a cell phone case, waited in line briefly, and left the store without making a purchase. Not long afterward, she spotted him again outside adjusting his gloves as he walked back toward the store.

The store's surveillance camera captured the earlier visit, in addition to the robbery. Detectives retrieved other footage from a nearby property, which showed the man walking around near the store for approximately ten minutes. They then generated a still image from the footage and sent it to the New Jersey Regional Operations Intelligence Center (NJROIC) for facial recognition analysis. An NJROIC investigator advised there were no matches, but he could re-run the inquiry if detectives provided him with a better image. Instead, detectives sent all the raw surveillance footage to the Facial Identification Section of the New York Police Department Real Time Crime Center (NYPD RTCC). A detective there captured a still image from the footage, compared it against the center's databases, and offered defendant as a "possible match."

Detectives working the case in New Jersey created two different photo arrays, comprised of five filler photos and the photo NYPD RTCC provided of defendant from its database. The first array was shown to Vasquez-Arias and

the second to Cardozo in separate videorecorded interviews. Both witnesses independently identified defendant's photo as that of the perpetrator.

A Hudson County grand jury indicted defendant with: first-degree robbery, N.J.S.A. 2C:15-1(a)(1); third-degree aggravated assault, N.J.S.A. 2C:12-1(b)(2); fourth-degree aggravated assault, N.J.S.A. 2C:12-1(b)(4); second-degree possession of a weapon for an unlawful purpose, N.J.S.A. 2C:39-4(a)(1); first-degree unlawful possession of a weapon, N.J.S.A. 2C:39-5(j); and second-degree certain persons not to have a weapon, N.J.S.A. 2C:39-7(b)(1).

Upon learning FRT played a role in identifying defendant, defense counsel sent the State a letter pursuant to Rule 3:13-3 and Brady v. Maryland, 373 U.S. 83 (1963), seeking the following discovery:

> 1. The name and manufacturer of the facial recognition software used to conduct the search in this case, and the algorithm(s) version number(s) and year(s) developed;
>
> 2. The source code for the face recognition algorithm(s);
>
> 3. A list of what measurements, nodal points, or other unique identifying marks are used by the system in creating facial feature vectors including, if those marks are weighted differently, the scores given to each respective mark;
>
> 4. The error rates for the facial recognition system used, including false accept and false reject rates (also called false match and false non-match rates—FMR

and FNMR), as well as documentation as to how the error rates were calculated, including whether they reflect test or operational conditions;

5. The performance of the algorithm(s) used on applicable NIST[1] Face Recognition Vendor Tests, if available;

6. The original copy of the query or "probe" photo[2] submitted to the Real Time Crime Center[—]Facial Identification Section;

7. All edited copies of the query or "probe" photo submitted to the facial recognition system, noting if applicable, which edited copy produced the candidate list that the defendant was in, and a list of edits, filters, or any other modifications made to that photo;

8. A copy of the database photo matched to the query or "probe" photo and the percentage of the match, rank number, or confidence score assigned to the photo by the facial recognition system in the candidate list;

9. A list or description of the rank number or confidence scores produced by the system, including the scale on which the system is based (e.g. percentage, logarithmic, other);

---

[1] National Institute of Standards and Technology.

[2] A probe photo is an image inputted to the FRT for analysis. Emma Lux, Facing the Future: Facial Recognition Technology Under the Confrontation Clause, 57 Am. Crim. L. Rev. Online 20, 22 (2021). The NYPD FRT Patrol Guide defines a "probe image" as "[a]n image of an unidentified person obtained by the assigned investigator from witnesses, victims, or other reliable sources." Facial Recognition Technology, N.Y.C. Police Dep't (Mar. 3, 2020), https://www.nyc.gov/assets/nypd/downloads/pdf/nypd-facial-recognition-patrol-guide.pdf.

10. A copy of the complete candidate list returned by the face recognition or the first [twenty] candidates in the candidate list if longer than [twenty], in rank order and including the percentage of the match or confidence score assigned to each photo by the facial recognition system;

11. A list of the parameters of the database used, including:

1. How many photos are in the database;

2. How are the photos obtained;

3. How long the photos are stored;

4. How often the database is purged;

5. What the process is for getting removed from the database;

6. Who has access to the database;

7. How the database is maintained;

8. The Privacy Policy for the database;

12. The report produced by the analyst or technician who ran the facial recognition software, including any notes made about the possible match relative to any other individuals on the candidate list; and

13. The name and training, certifications, or qualifications of the analyst who ran [the] facial recognition search query.

While the discovery request was pending, defendant moved to suppress Vasquez-Arias's and Cardozo's out-of-court identifications of him. He argued the detective who interviewed Vasquez-Arias failed to record three conversations he had with her prior to showing her the array, namely, when he met her at the store, during the drive back to the police precinct, and at the precinct prior to the identification. Defendant argued the detective failed to "elicit a statement of confidence from . . . Vasquez-Arias, in her own words, once she had made the identification." The detective did not ask her if she had spoken with anyone about the description and identification of her attacker. Defendant raised similar arguments regarding Cardozo's identification.

Defendant also argued the detective who transported Vasquez-Arias to the identification procedure was not a blind administrator because he was involved in the investigation, having received the still image from another detective, located, reviewed, and written a report regarding the surveillance video. Furthermore, Vasquez-Arias was told she was being transported to the precinct to identify the perpetrator; she was never told she did not have to select a photo.

Defendant also challenged the photo array police used with Vasquez-Arias, noting he stood out from the others in the array because he was the only one without "prominent facial hair, and . . . the only person depicted in a grey

shirt." He asserted Vasquez-Arias's identification was problematic because she was under substantial stress at the time of the robbery and the robber had a weapon, which lessened her ability to identify him. Her interaction with the robber was fleeting; she suffered a head injury and was visually impaired at the time of the accident. Cardozo's interaction was also brief.

Defendant argued the robber wore a hat, which obscured some of his features and Vasquez-Arias viewed the photo array three weeks after the incident. Further, the court had no means of comparing Vasquez-Arias's initial description of the robber with the photo array because she did not give one. Defendant made similar arguments regarding Cardozo's photo array process, noting she repeatedly attempted to tell detectives she had a difficult time identifying defendant because of his hat and different facial hair. Vasquez-Arias hesitated to identify defendant for over two minutes during the photo array. Cardozo did not make an initial identification during her review of the array either.

The motion judge conducted a Wade[3] hearing and considered testimony from Vasquez-Arias, Cardozo, and both West New York police detectives

[3] United States v. Wade, 338 U.S. 218 (1967).

involved in the investigation. She issued a written opinion, finding although the identification procedure "did not include all that Delgado[4] and R[ule] 3:11 require, [it] does not warrant suppression."

The judge addressed each deficiency. She credited Vasquez-Arias and a detective's testimony that they did not speak at any point prior to the official identification procedure. Although the detective "established a confidence interval by asking [Vasquez-Arias] 'One Hundred Percent?' [after she picked defendant's photo, she] chose the photo herself, replied in the affirmative to [the detective's] question, and confirmed her confidence in her testimony." Despite the detective not asking Vasquez-Arias if she had spoken to others, "testimony confirms that she had spoken with other officers and . . . Cardozo." The judge concluded defendant could address the "issues of outside influence . . . at trial through cross-examination." Further, "these deviations . . . taken together, may be remedied by a jury instruction, direct examination, and cross-examination during trial." The judge reached a similar conclusion regarding the identical deficiencies in Cardozo's identification process.

The motion judge rejected defendant's argument the system and estimator variables in the identification process created a substantial likelihood of

4 State v. Delgado, 188 N.J. 48 (2006).

misidentification. She found even though the detective who located surveillance footage of the suspect was involved in showing Vasquez-Arias the photo array, "he did not prepare the photo array, never opened the sealed envelope until the photo array, and did not know the identity of . . . [d]efendant at the time." The judge noted "the pre-identification instructions were unquestionably inaccurate. [The detective] fumbled his words and did not read the instructions exactly as they were stated on the page. Further, . . . Vasquez-Arias testified that she did not read the instructions herself and just signed where they told her to sign." However, the detective did tell her she should not conclude the perpetrator's photo was in the array and the fact she was being shown the photos "'doesn't mean that the criminal is or is not in this group of pictures.' . . . Further, . . . Vasquez-Arias . . . affirmed her selection of a photo after [the detective] asked her if she was 'one hundred percent.'"

The judge found the detective asking Vasquez-Arias if she was one hundred percent about her selection of the perpetrator's photo was "unlikely to have provided any significant feedback or have influenced . . . Vasquez-Arias's confidence." This is because "she took her time during the identification because she wanted to be one hundred percent sure that [this] was the person who tried to attack her." The judge found the presence of the second detective

investigating the case did not influence Vasquez-Arias because she "testified . . . he did not say anything, nor make any suggestive signals." Although Vasquez-Arias only saw the perpetrator briefly, she testified the lighting was clear, she was wearing her glasses, and stood close to him. The judge found Vasquez-Arias's careful identification of the perpetrator outweighed the fact she had spoken with others regarding the robbery. She also denied being under stress during the incident, despite "everything happen[ing] so quickly" and having been "hit so hard."

The judge also concluded there was no substantial likelihood of a misidentification by Cardozo, because like Vasquez-Arias, she was instructed the perpetrator "may or may not be in the . . . array and she was not obligated to pick someone out." She also affirmed her selection after the detective asked her if she was one hundred percent. Like Vasquez-Arias, the judge found the detective asking Cardozo if she was one hundred percent did not influence Cardozo because she testified "she was 'super sure' of the identification she had made." Moreover, the presence of the second detective involved in the investigation during the identification did not influence her.

Although Cardozo watched the surveillance footage "approximately two-to-three times before her identification . . . she testified that she was sure . . .

[d]efendant was the perpetrator before viewing the video." The judge noted Cardozo had viewed defendant "three times, under clear lighting conditions, and testified that she had specifically noticed . . . [d]efendant because she thought it was strange that after their conversation, he left and picked up a brochure." The judge found Cardozo's interaction with defendant outweighed the fact her identification may have been influenced by speaking with Vasquez-Arias about the robbery.

The motion judge rejected defendant's arguments regarding the photos in the array. She concluded

> the filler photographs sufficiently matched [d]efendant's appearance to constitute a proper array. The individuals in the photo array are all Hispanic males with varying degrees of facial hair. The filler photographs contained no marks, scars, or tattoos on their face[,] which would set them apart from . . . [d]efendant who also did not possess any of those facial features.

The State answered defendant's discovery request by providing the items sought in the eighth and tenth requests in defense counsel letter. Specifically, the State provided: the NYPD RTCC search result report identifying defendant as a possible match to the individual in the surveillance footage; the still images used for comparison; the first ten possible matching candidates for each, presented in rank order and accompanied by their confidence scores; and a short

series of handwritten notes by an NYPD RTCC analyst. Notably, many of the results attached to the report entailed two independent sets of possible matches for a given probe, suggesting either the probes were compared against more than one database, or more than one FRT was used.

Defendant moved to compel the State to provide the remaining eleven items in the defense's discovery request. The motion attached a detailed declaration from the defense's proposed FRT expert, opining about the accuracy issues associated with FRT and why the defense needed the discovery. The expert stated: "Understanding the [NYPD RTCC's facial recognition] model, the data that was used to train the model, and the class-specific performance for the image(s) in this case are critical to understand the reliability of the output." He concluded "without this additional information, the current results of the image recognition software in this case cannot be considered scientifically replicable or relevant."

Defense counsel argued the reliability of the FRT could not be assessed without the discovery sought because it was "highly system-dependent" and dependent on choices made by the operator "at every step of the process." The defense cited research and data, including NIST, showing "face recognition can be extremely poor at identifying a person in a low-resolution image" like the

surveillance still used here. Moreover, the images are manipulated by the FRT operator to obtain a "normalized" face to run against the database. Defendant alleged the FRT algorithm could have a high error rate, and large databases can return an incorrect match, due to the over-representation of racial minorities—an imbalance which stems from the fact that the databases are populated by photographs taken during arrest and parole. The defense also noted "a human must choose which photo from the candidate list [generated by the FRT] will be forwarded to the investigating agency as the 'match.'" Defendant contended this part of the process was entirely subjective.

Defendant asserted because the FRT could produce "high levels of false positives . . . [i]t is therefore critical for the defense to know exactly which tools were employed and how they were used in order to evaluate the reliability of the methods that were used to bring [defendant] into this case." The remaining eleven items the State failed to produce were necessary to provide context for and assess the reliability of the match.

Defendant argued he had a constitutional right to the discovery because the FRT directly inculpated him, and he had the right to mount a complete defense. He asserted Rule 3:13-3(b) required the State to provide this information because it was exculpatory and necessary to a fair trial.

Furthermore, the discovery was relevant to impeaching the thoroughness of the State's investigation. The discovery was also necessary to impeach the witnesses' identification because "the use of unreliable technology to create the photo array undermines the array and the identification itself." The failure to disclose how the array was compiled violated due process.

The defense noted its discovery requests were specific and tailored. Moreover, "no claim[s] of intellectual property issues" were raised and a protective order could address such claims in any event. Defendant argued "[t]his is the first known and disclosed use of facial recognition in New Jersey. [Therefore, t]he public interest requires a full and fair examination of this technology."

The motion judge issued a written opinion concluding the State had no obligation to produce the discovery because the FRT was not within its care, custody, or control. The judge likened the NYPD RTCC to the New Jersey State Police Lab in State v. Washington, where we held a county prosecutor did not have to produce a draft DNA report prepared by the lab because it was an entity separate from the prosecutor. 453 N.J. Super. 164, 174-75 (App. Div. 2018).

The judge further found the discovery was "not Brady material" because the FRT produced

> nothing more than a photograph that resembles the photograph provided from the still shot of the video taken from the scene of the incident. At best, the West New York Police Department was provided with an additional photograph to compile the six pack that was shown to the witness in this case. It was the witnesses' identifications that formed the basis for probable cause to arrest [d]efendant.

The defense also relied on State v. Pickett, where we granted the defendant discovery regarding a novel DNA testing program, including the "software's source code and supporting software development and related documentation . . . pertaining to testing, design, bug reporting, change logs, and program requirements . . . to challenge the reliability of the software and science underlying" the State's expert's testimony at a Frye[5] hearing. 466 N.J. Super. 270, 279 (App. Div. 2021). The judge distinguished Pickett because here the State would not be relying on expert testimony regarding the FRT and a "Frye hearing is not contemplated . . . as the State is not looking to introduce facial recognition software in its case in chief. The State only seeks to admit the identifications made by the two witnesses, which were not determined to be impermissibly suggestive." The motion judge denied the defense's motion for the discovery.

[5] Frye v. United States, 293 F. 1013 (D.C. Cir. 1923).

I.

Defendant raises the following arguments on appeal:

> WITHOUT ANY INFORMATION ABOUT THE RELIABILITY OF THE [FRT], THERE CAN BE NO FAIR TRIAL IF THE FRUITS OF THAT TECHNOLOGY'S USE ARE ADMITTED INTO EVIDENCE.
>
> > A. The Reliability of [FRT] Are Highly System and Analyst Dependent.
> >
> > B. The Discovery Sought Is Necessary To Assess The Reliability Of The Match In This Case.
> >
> > > 1. Each item sought is necessary to assess the accuracy of the [FRT] used.
> > >
> > > 2. The accuracy of the facial recognition system used relates directly to the reliability of the identification of defendant from the subsequent identification procedure and thoroughness of the police investigation.
> > >
> > > > a. The details of how defendant was selected by the [FRT] is essential to understanding the construction of the array and the reliability of the identifications.
> > > >
> > > > b. Information about the facial recognition systems used is

> exculpatory because it impeaches the thoroughness of the investigation and presents possibilities for third-party guilt.
>
> c. If the fruits of the [FRT] are to be used in court, then the defense must be able to fully understand and confront the use of that technology.
>
> C. . . . Defendant Is Entitled To The Discovery Sought Under Our Court Rules And Case Law.

Defendant is joined by amici, namely, the American Civil Liberties Union, American Civil Liberties Union of New Jersey, and Innocence Project. They argue: identifications derived from an FRT match are inherently subjective; discovery regarding FRT is Brady material and the State is obligated to obtain the discovery because NYPD RTCC conducted the search on the State's behalf, thereby making it part of the prosecution team; and the ongoing cooperation between both agencies requires the court protect New Jerseyan's access to exculpatory information, especially "where advanced and untested surveillance tools are at issue."

The Electronic Privacy Information Center, Electronic Frontier Foundation, and National Association of Criminal Defense Lawyers also join as

amici. They also assert defendant should have the discovery under Brady. In their view, discovery is also necessary to address: the risk of error in FRT; the fact human review cannot cure algorithmic errors; and FRT searches routinely result in wrongful arrests.

II.

We "generally defer to a trial court's disposition of discovery matters unless the court has abused its discretion or its determination is based on a mistaken understanding of the applicable law." State v. Ramirez, 252 N.J. 277, 298 (2022) (quoting State v. Brown, 236 N.J. 497, 521 (2019)). "A trial court can abuse its discretion 'by failing to consider all relevant factors.' [We] . . . will set aside or modify such decisions if they do not comport with the applicable law or do not give sufficient regard to pertinent considerations." Ibid. (internal citations omitted). However, where a matter involves novel scientific evidence in a criminal proceeding, we may exercise independent review of "the relevant authorities, including judicial opinions and scientific literature." Pickett, 466 N.J. Super. at 303 (internal citations omitted) (quoting In re Commitment of R.S., 339 N.J. Super. 507, 531 (App. Div. 2001)).

III.

"As codified in Rule 3:13-3, New Jersey has a tradition of what is often described as an 'open file' model of reciprocal pretrial criminal discovery. . . . Thus, criminal defendants are 'entitled to broad discovery' because it 'advances the quest for truth.'" Ramirez, 252 N.J. at 295 (quoting State v. Scoles, 214 N.J. 236, 252 (2013)).

> Nevertheless, despite a criminal defendant's general and automatic right to "broad discovery," . . . "criminal discovery has its limits." . . . Defendants are not permitted to conduct a "fishing expedition," or "transform the discovery process into an unfocused, haphazard search for evidence." Hence, information must be shown to be relevant to the issues in the case in order to be subject to disclosure.
>
> [Id. at 296 (internal citations omitted).]

Relevant information has "'a tendency in reason to prove or disprove [a] fact of consequence to the determination of the action[,]'" State v. Gilchrist, 381 N.J. Super. 138, 146 (App. Div. 2005) (quoting N.J.R.E. 401), or lead to the discovery of relevant evidence. State v. Ballard, 331 N.J. Super. 529, 538 (App. Div. 2000). Where discovery is sought but not provided, "the question is whether in the absence of the undisclosed evidence the defendant received a fair trial, 'understood as a trial resulting in a verdict worthy of confidence.'" State v. Nelson, 155 N.J. 487, 500 (1998) (quoting Kyles v. Whitley, 514 U.S. 419, 434 (1995)).

The State has a duty to disclose evidence potentially favorable to the defense. Brady, 373 U.S. at 87. This sort of evidence need not be directly exculpatory so long as it has value for impeachment purposes. State v. Nash, 212 N.J. 518, 544 (2013). Exculpatory evidence is not limited to evidence within the State's possession, custody, or control. Washington, 453 N.J. Super. at 184. "The Brady disclosure rule applies only to information of which the prosecution is actually or constructively aware." Nelson, 155 N.J. at 498. "This . . . means that the 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." Kyles, 514 U.S. at 437; see Nelson, 155 N.J. at 499 (citing Smith v. Sec'y of N.M. Dep't of Corr., 50 F.3d 801, 824 (1995)) ("[T]he 'prosecution' for Brady purposes . . . extends to . . . law enforcement personnel and other arms of the state involved in investigative aspects of a particular criminal venture."); State v. Robertson, 438 N.J. Super. 47, 69 (App. Div. 2014) ("A prosecutor's obligation under Brady extends to documents of which it is actually or constructively aware, including documents held by other law enforcement personnel who are part of the prosecution team.").

We briefly review our past application of these principles. In Robertson, we found no Brady violation warranting reversal of the defendant's driving while

intoxicated conviction where the State did not provide data and repair records for an Alcotest device used to test defendant the night of his arrest. 438 N.J. Super. at 72. Defendant produced an expert who opined the repair and data records were necessary to provide a "complete picture of the operability of the instrument." Id. at 57. However, the State could not provide the information because the data was routinely erased following each re-calibration. Id. at 60. We concluded there was no evidence the State controlled the repair data generated by the private company maintaining the Alcotest machines and it was incumbent on defendant to subpoena those records from the company. Id. at 69. Furthermore, the State's "Brady disclosure obligation [did] not extend to documents held by a private contractor . . . ." Ibid.

Similarly, in Washington, the State challenged trial court orders granting the defendant's motion to exclude DNA evidence provided by way of a State Police Lab report, on account of a speedy trial violation. 453 N.J. Super. at 175-77. The State moved for reconsideration of the trial judge's order and provided certifications from the lab scientist and the prosecutor explaining the reasons for the delay, including that the testing protocols had changed. Id. at 177-78.

We held there was no discovery violation because a county prosecutor lacked supervisory authority over the State Police Lab that was a part of the New

Jersey State Police "within the Department of Law and Public Safety, which is headed and supervised by the Attorney General." Id. at 181. We also noted: "Importantly, there is no claim the DNA report was exculpatory evidence." Id. at 184.

State v. Ghigliotty involved whether a Frye[6] hearing was required to assess novel software used to determine if the defendant's gun fired the bullets recovered from the victim. 463 N.J. Super. 355, 360 (App. Div. 2020). On appeal, the State argued a Frye hearing was unnecessary because its expert did not rely on the novel technology but instead based "his 'ultimate results and conclusions' . . . using only a standard comparison microscope." Id. at 379. We concluded the trial court correctly held a Frye hearing was necessary because although the expert used a traditional method to analyze the bullet, the untested, newer technology caused him to change his conclusion and "clearly aided and influenced the course of his investigation and informed his ultimate opinion . . . ." Id. at 380. Indeed, the expert admitted he could not reach a conclusion using the traditional method until he utilized the new technology. Id. at 380-81.

[6] Our Supreme Court has since departed from the Frye standard in favor of the standard outlined in Daubert v. Merrell Dow Pharmaceuticals Inc., 509 U.S. 579 (1993). See State v. Olenowski, 253 N.J. 133, 139 (2023).

A Frye hearing was necessary to demonstrate the reliability of the technology because it was "a new, untested device, operated by . . . a novel software product." Id. at 383. Moreover, "[t]he parties did not provide the court with any judicial opinions or authoritative scientific and legal writings demonstrating the reliability of this machine." Ibid. And neither expert involved with the case "were experts in the science behind the . . . system and, therefore, were unable to address whether it provided reliable images." Ibid.

In Pickett, the trial court conducted a Frye hearing regarding the reliability of novel software used for DNA testing, which used a "complex probabilistic genotyping software program [the State's expert utilized] to testify that defendant's DNA was present, thereby connecting defendant to a murder and other crimes." 466 N.J. Super. at 277. The defense sought access to proprietary information, including the software, source code, and other materials to cross-examine the State's expert and to enable the defense expert to test the reliability of the software. Ibid. On leave to appeal, we reversed the trial court's order denying defendant's access to the information. Id. at 280.

Although Pickett involved a Frye hearing and a scenario in which the State intended to introduce expert testimony using the novel software to prove defendant's guilt, it expressed principles which apply in this case, namely: "In

appropriate circumstances, especially where civil liberties are on the line, independent source-code review is critical when determining reliability at a Frye hearing." Id. at 279. We further held that, in instances where the State intends to rely upon an expert who uses novel technology, the "defendant is entitled to access" discovery related to novel technology. Id. at 278-79. The discovery was to be provided under a protective order rather than hidden from the defense. Ibid. Whether a defendant has shown "a particularized need for such discovery" requires the trial judge

> consider: (1) whether there is a rational basis for ordering a party to attempt to produce the information sought, including the extent to which proffered expert testimony supports the claim for disclosure; (2) the specificity of the information sought; (3) the available means of safeguarding the company's intellectual property, such as issuance of a protective order; and (4) any other relevant factors unique to the facts of the case.
>
> [Id. at 279.]

Applying the principles of these holdings here, and pursuant to our independent review of the record, we reverse the denial of discovery. We are keenly aware the cases we have discussed involved instances concerning Frye hearings and potential expert testimony, and that here, we are dealing instead with eyewitnesses who have already identified the perpetrator, and the

identification found admissible under Wade. However, the facts of this case convince us defendant will be deprived of due process if he "does not have 'access to the raw materials integral to the building of an effective defense' . . . ." In re A.B., 219 N.J. 542, 556 (2014) (quoting Ake v. Oklahoma, 470 U.S. 68, 77 (1985)). 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.

We are not convinced the NYPD RTCC was not a part of the prosecution team. The prosecutor sent a request to the NYPD RTCC, which in turn complied by producing the information used to accuse defendant. Moreover, the prosecutor obtained discovery materials from the NYPD RTCC by responding to two items in defense counsel's discovery letter. The State does not argue it cannot obtain the additional information sought by defendant for proprietary or other reasons, only that defendant should subpoena the information. We reject this assertion because the burden lies with the State given the fact FRT is novel and untested, and the possibility that errors in the technology may exculpate defendant.

There is little evidence in the record regarding the software at issue here. However, defendant through his expert, and the secondary sources cited by defense counsel and amici, provide us convincing evidence of FRT's novelty, the human agency involved in generating images, and the fact FRT's veracity has not been tested or found reliable on an evidential basis by any New Jersey court.

FRT can detect a human face within an image.[7] It uses an algorithm to make the analysis, which recognizes "nodal points" on the face—the "peaks and valleys that make up human facial features"—and measures them against corresponding features in comparison images. Kirill Levashov, Note, The Rise of a New Type of Surveillance for Which the Law Wasn't Ready, 15 Colum. Sci. & Tech. L. Rev. 164, 167-68 (2013). The underlying algorithm is developed through machine learning that is trained over time to recognize potential matches by being asked to compare several thousand images against a database. Lux, 57 Am. Crim. L. Rev. Online at 21. In each instance, the program estimates whether a match exists, is told whether the result is correct, and then uses this data regarding successes or failures to inform subsequent evaluations, ibid.,

[7] Thorin Klosowski, Facial Recognition Is Everywhere. Here's What We Can Do About It, N.Y. Times (July 15, 2020), https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/.

eventually focusing on those features that have been the most reliable indicators of a match.[8]

The process begins when the person operating the software selects a probe image captured from surveillance footage that features the perpetrator's face. Henry H. Perritt, Jr., Defending Face-Recognition Technology (And Defending Against It), 25 J. Tech. L. & Pol'y 41, 57 (2021). Poorer quality images can be edited for lighting or color correction, to enhance detail, or even to change facial expression.[9] The technology then breaks down the image into component features and distills them into a "faceprint"—a "map written in code that measures the distance between features, lines, and facial elements." Andrew Guthrie Ferguson, Facial Recognition and the Fourth Amendment, 105 Minn. L. Rev. 1105, 1111 (2021). It then compares this "faceprint" against others in the database, assigning scores to each based on the extent to which corresponding features line up, and returning a list of those with the highest scores ordered by

[8] Clare Garvie et al., The Perpetual Lineup: Unregulated Police Face Recognition in America, Geo. L. Ctr. on Priv. & Tech. (Oct. 18, 2016), https://www.perpetuallineup.org/.

[9] See Clare Garvie, Garbage In, Garbage Out: Face Recognition on Flawed Data, Geo. L. Ctr. on Priv. & Tech. (May 16, 2019), https://www.flawedfacedata.com/.

rank. U.S. Gov't Accountability Off., GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 14 n.35 (2016).

The reliability of the results may depend on many variables encountered throughout the process. Some literature suggests the quality and diversity of images used for training the technology may influence the technology's ability to recognize faces differing from those in the initial set, often resulting in poor performance with analysis of non-white faces. Sidney Perkowitz, The Bias in the Machine: Facial Recognition Technology and Racial Disparities, MIT Case Stud. Soc. & Ethical Resps. Computing, Feb. 5, 2021, at 6-7. Moreover, the quality of a probe image, including its resolution, ambient lighting, and facial expression, U.S. Dep't of Homeland Sec., DHS/ICE/PIA-054, Privacy Impact Assessment for the Use of Facial Recognition Services 26 (2020), as well as the extent of any editing performed to it, Garvie, Garbage In, Garbage Out, § 2, may impact the accuracy of the resulting "faceprint" and the software's ability to meaningfully compare it with those in the database.

Defendant argues the reliability of FRT is highly dependent on its design and training, as well as the parameters used by the analyst who operates it. He asserts the discovery sought is relevant to assessing the reliability of the FRT results used to identify him. The defense expert explains the source code and

related materials are necessary to analyze the software's design and training methods for inherent structural flaws in the software that could introduce bias compromising the accuracy of the results generated by the software. The reliability of the technology implicates the accuracy of the eyewitness identifications, the thoroughness of the State's investigation, and the ability to prove the existence of other viable suspects. Defendant asserts if the discovery is not provided, the State should be barred from introducing Vasquez-Arias and Cardozo's identifications because they are the "fruits" of the untested technology.

We reject the last assertion because our review of the Wade hearing record and the motion judge's opinion convince us the witness identification process, while flawed, was not so irreparably flawed as to be inadmissible at trial. The inquiry at a Wade hearing is whether the identification procedure presented a "very substantial likelihood of irreparable misidentification" to undermine the reliability of the result as a genuine product of the eyewitness's memory rather than of improper influence. State v. Henderson, 208 N.J. 208, 289 (2011). The identification process is analyzed in light of a set of established factors—"system variables" within the State's control, such as blind administration of the procedure, pre-identification instructions, and construction and presentation of

the array, as well as "estimator variables" beyond the State's control, such as the duration for and conditions under which the witness observed the event, individual characteristics of the witness or perpetrator that might bear on memory or perception, or temporal distance from the event. Id. at 248, 261, 289-92.

Although the construction of the array is a factor for consideration, the concern with the construction is whether the suspect stands out from others featured in the array or whether the array includes sufficient "fillers" other than the suspect, to ensure that it properly "test[s] a witness' memory and decrease[s] the chance that a witness is simply guessing." Id. at 251. The reason why a particular individual is a suspect and consequently included in the array is not relevant to that inquiry. Cf. State v. Guerino, 464 N.J. Super. 589, 607 (App. Div. 2020) (concluding that a detective's brief comment to the victim the State had developed array based on "investigative sources" was not unduly suggestive, because it "merely made explicit that which is implicitly understood by witnesses participating in an identification procedure, that is, there must be some reason why the police selected the photographs that were included in the array").

Based on our review of the Wade hearing record, we cannot conclude Vasquez-Arias and Cardozo felt pressure to identify a perpetrator from among

the photos in the arrays presented to each of them. The record does not support the contention there was a substantial likelihood of irreparable misidentification.

However, the discovery dispute stands separate from the Wade hearing, and we view the request for the FRT discovery as relevant to defendant's ability to impeach the identification and the investigation, and his overall ability to establish reasonable doubt at trial. The FRT's reliability has obvious implications for the accuracy of the identification process because an array constructed around a mistaken potential match would leave the witness with no actual perpetrator to choose. The reliability of the technology bears direct relevance to the quality and thoroughness of the broader criminal investigation, and whether the potential matches the software returned yielded any other viable alternative suspects to establish third-party guilt. Defendant's request for the identity, design, specifications, and operation of the program or programs used for analysis, and the database or databases used for comparison are relevant to FRT's reliability.

At trial, the State will likely have the investigating officer explain the police investigation, including the process of retrieving the still photo from the surveillance cameras ultimately used to generate an image of defendant. Although we do not speculate regarding the exact nature of this testimony and

whether defendant will seek to impeach it, the fact the State does not bear the burden of adducing testimony regarding the composition of the photo array does not bar the defense access to the discovery sought.

In State v. Branch, the Supreme Court held that testimony why an "officer placed the defendant's photograph in the array is of no relevance to the identification process and is highly prejudicial." 182 N.J. 338, 352 (2005). The officer in Branch testified "he placed a defendant's picture in a photographic array 'upon information received.'" Ibid. The Court found this problematic because it "swe[pt] in inadmissible hearsay. It implie[d] that the police officer has information suggestive of the defendant's guilt from some unknown source." Ibid. However, the Court noted "[t]he exception would be the defendant who opens the door by flagrantly and falsely suggesting that a police officer acted arbitrarily or with ill motive[,]" in which case, "the officer might be permitted to dispel that false impression, despite the invited prejudice the defendant would suffer." Ibid.

Here, the implication of Branch is not that defendant will open the door by suggesting to the jury the inclusion of his photo in the array was the product of bad faith, but rather that the defense may inquire into the reason for defendant's identification as a suspect. The discovery is relevant to defendant's

ability to open the door and convince the jury the FRT is unreliable and identified the wrong suspect.

The State recognizes its obligation to turn over exculpatory evidence but argues the exculpatory nature of the evidence sought here is "purely speculative" and is merely "potentially exculpatory." We have previously explained, in the context of a similar argument:

> The State's position [a witness's statement's exculpatory nature was speculative] begs the question. The defense is left to speculate because the judge failed to require the State to produce the document for inspection so he and counsel would be aware of its contents and could determine its relevance and materiality. It may be, as the State suggests, irrelevant and immaterial. However, it may be, as defense suggests, highly relevant and material and even exculpatory . . . .
>
> [State ex rel. L.E.W., 239 N.J. Super. 65, 76 (App. Div.), certif. denied, 122 N.J. 144 (1990).]

Here, the items sought by the defense have a direct link to testing FRT's reliability and bear on defendant's guilt or innocence. Given FRT's novelty, no one, including us, can reasonably conclude without the discovery whether the evidence is exculpatory or "merely potentially useful evidence." Robertson, 438 N.J. Super. at 67. For these reasons, it must be produced.

Like Pickett, defendant here has demonstrated a "particularized need for [the] discovery." 466 N.J. Super. at 279, 289. He has produced a list of specific items sought, aided by an expert, which is neither broad, unduly burdensome, or untethered to the evidence necessary to mount a defense. As then-Judge Fasciale put it in Pickett,

> [a]s technology proliferates, so does its use in criminal prosecutions. Courts must endeavor to understand new technology . . . and allow the defense a meaningful opportunity to examine it. Without scrutinizing its software's source code—a human-made set of instructions that may contain bugs, glitches, and defects—in the context of an adversarial system, no finding that it properly implements the underlying science could realistically be made. Consequently, affording meaningful examination of the source code, which compels the critical independent analysis necessary for a judge to make a threshold determination as to reliability at a [Daubert] hearing, is imperative.
>
> [Id. at 323-24.]

We are convinced this is true for FRT as well.

Defendant must have the tools to impeach the State's case and sow reasonable doubt. For these reasons, we reverse and remand for entry of an order directing the State to provide the eleven remaining items of discovery requested by the defense. Naturally, the motion judge may enter any appropriate

protective order, order the in-camera review of the materials received from the State, and hold a Daubert hearing if necessary.

Reversed and remanded. We do not retain jurisdiction.

I hereby certify that the foregoing is a true copy of the original on file in my office.

CLERK OF THE APPELLATE DIVISION