IN THE COURT OF APPEALS
EIGHTH DISTRICT COURT OF APPEALS
CUYAHOGA COUNTY

STATE OF OHIO, *Plaintiff–Appellant*, v. QEYEON TOLBERT, *Defendant–Appellee*.	**No. CA-25-114748** On appeal from the Cuyahoga County Court of Common Pleas Case No. CR-24-689572-A

AMICUS CURIAE BRIEF OF THE AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF OHIO, AND NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF DEFENDANT–APPELLEE

Stephanie Kessler (0092338)
Sixth Circuit Vice-Chair, Amicus Committee
National Association of Criminal Defense Lawyers
Kessler Defense LLC
215 E. 9th St., Suite 650
Cincinnati, OH 45202
(513) 316-5807
stephanie@kesslerdefense.com

Sidney W. Thaxter, Esq.*
NACDL 4th Amendment Center
1660 L St. NW, 12th Floor
Washington, DC 20036
(202) 465-7654
sthaxter@nacdl.org

Amy R. Gilbert (100887)
Freda J. Levenson (0045916)
American Civil Liberties Union of Ohio Foundation
4506 Chester Ave.
Cleveland, OH 44103
(614) 586-1972
agilbert@acluohio.org
flevenson@acluohio.org

Nathan Freed Wessler*
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

Counsel for amici curiae

*Pro hac vice motion filed concurrently

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

INTEREST OF AMICI CURIAE

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to the principles embodied in the United States Constitution and our nation's civil rights laws. The American Civil Liberties Union of Ohio is a state affiliate of the ACLU. The ACLU has appeared before courts throughout the country in cases involving the dangers posed by unfettered police use of emerging technologies, including face recognition technology ("FRT"). Attorneys associated with the ACLU represented Robert Williams in *Williams v. City of Detroit*, No. 2:21-cv-10827-LJM-DRG (E.D. Mich.), alleging that the misuse of face recognition technology by the Detroit Police Department led to Mr. Williams's wrongful arrest, and have filed amicus briefs in other cases involving violation of constitutional rights in connection with police reliance on FRT. *See Woodruff v. Oliver*, No. 5:23-cv-11886 (E.D. Mich) (wrongful arrest); *Oliver v. Bussa*, No. 2:20-cv-12711 (E.D. Mich.) (same); *Parks v. McCormac*, No. 2:21-cv-04021 (D.N.J.) (same); *State v. Arteaga*, 476 N.J.Super. 36, 58 (App. Div. 2023) (*Brady* disclosure of details of FRT use).

The National Association of Criminal Defense Lawyers (NACDL) is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of many thousands of direct members, and up to 40,000 with affiliates. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges.

NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers. NACDL is dedicated to advancing the proper, efficient, and just administration of justice. NACDL files numerous amicus briefs each year in the U.S. Supreme Court and other federal and state courts, seeking to provide amicus assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole.

NACDL has a particular interest in cases that involve surveillance technologies and programs that pose new challenges to personal privacy. The NACDL Fourth Amendment Center offers training and direct assistance to defense lawyers handling such cases in order to help safeguard privacy rights in the digital age. NACDL has also filed numerous amicus briefs in the Supreme Court on issues involving digital privacy rights, including: *Carpenter v. United States*, 585 U.S. 296 (2018); *Riley v. California*, 573 U.S. 373 (2014); *United States v. Jones,* 565 U.S. 400 (2012).

The Court has granted leave for the filing of amici's brief. *See* Journal Entry (Mar. 10, 2025).

INTRODUCTION AND SUMMARY OF ARGUMENT

The detective in this case applied for a search warrant in reliance on a purported identification of Defendant from a face recognition technology ("FRT") search. The detective had been warned that the FRT search result was only an investigative lead. But far from disclosing the role of FRT and its lack of reliability for providing an identification, the detective scrubbed his affidavit of any mention of the technology. Instead, he misleadingly vouched only that police "received an identification" of Defendant from the "Fusion center." Had the judge known that the basis for the purported identification was an unreliable FRT search that supplied "multiple photos of multiple people," Tr. at 69, it would have been clear that the warrant lacked probable cause.

Amici write to aid the Court in rendering a decision based on an accurate understanding of face recognition technology and why the investigating officer's lack of candor in the warrant application requires suppression. This brief makes two main points. First, FRT results are fundamentally unreliable because of well-known technical limitations, racially disparate false-match rates, and human operator errors. And second, the detective's concealment of the use of FRT and representation that there had been an "identification" were materially false and misleading and thus should require suppression because the remaining facts in the affidavit cannot establish probable cause.

The importance of this issue reaches far beyond this case. Here, although police concealed their use of FRT from the judge, the prosecutor eventually disclosed it to the defendant, allowing the court below to hear the suppression motion. But police and prosecutors across the country systematically fail to disclose their use of face recognition technology to criminal defendants, meaning that people searched or arrested due to police

reliance on FRT results—which are often erroneous[1]—may never know how they came to law enforcement's notice, and therefore may not be in a position to mount a legal challenge.[2] This Court can and should provide guidance to ensure that police abide by their duty of candor to courts when submitting warrant applications in such cases.

ARGUMENT

I. Face recognition technology is inherently unreliable and cannot be relied on as a positive identification of a suspect.

As the trial court put it, the purported identification of the suspect based on face recognition technology search results in this case was "admittedly unreliable." Tr. at 92. The disclaimer appearing prominently at the bottom of each page of the Clearview AI FRT results provided to the investigating officer warned that "[f]acial recognition search results are to be treated as investigative leads" only and must be "independently verified" through "thorough investigation[]." Def's Ex. B. As Clearview further warns on its public website, its FRT system is "neither designed, nor intended . . . to be used as a sole source system for conclusively establishing or determining an individual's identity." Def's Ex. C.

---

[1] Police reliance on erroneous FRT results has been responsible for at least seven known wrongful arrests. *See* Douglas MacMillan, David Ovalle & Aaron Schaffer, *Arrested by AI: Police Ignore Standards After Facial Recognition Matches*, Wash. Post (Jan. 13, 2025), https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/.

[2] 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/ ("Police departments in 15 states provided The Post with rarely seen records documenting their use of facial recognition in more than 1,000 criminal investigations over the past four years. According to the arrest reports in those cases and interviews with people who were arrested, authorities routinely failed to inform defendants about their use of the software . . . .").

That is because "real world conditions" can "reduce the accuracy of Clearview search results," and in all conditions the system is designed only to be "indicative and should not be considered definitive." *Id.* The Ohio Attorney General's Office agrees, stating publicly that Clearview searches produce "mixed results," and that those "results are merely an investigative lead that must then be followed up on by the investigator."[3]

There is good reason for these warnings: Face recognition algorithms are unreliable and indeed are not even *designed* to generate matches. Instead, they produce *possible* leads, which are often incorrect, especially in "real world conditions" where low photo quality and other variables are at play. An accurate understanding of *why* FRT systems are unreliable is instructive in explaining why police lacked probable cause for the search of Defendant–Appellee's home in this case.

When police personnel run an FRT search, the algorithm extracts a "faceprint" or "template"[4] from the image of an unknown suspect (the "probe image" or "search image") and compares it to a database of faceprints taken from images of known individuals (for example, arrest photos, drivers' license photos or, in this case, photos scraped from the internet). The system generates similarity scores for each comparison and then outputs a "candidate list" of possible matches, generally organized in order of similarity score.

---

[3] Jeremy Pelzer, *Ohio Continues Facial-Recognition Searches Using Controversial Photo-Collection Firm Clearview AI*, cleveland.com (Feb. 21, 2024), https://www.cleveland.com/news/2024/02/ohio-continues-facial-recognition-searches-using-controversial-photo-collection-firm-clearview-ai.html.

[4] A faceprint is a "map written in code that measures the distance between features, lines, and facial elements." *State v. Arteaga*, 476 N.J.Super. 36, 58 (App. Div. 2023) quoting Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 Minn. L. Rev. 1105, 1111 (2021)).

Although higher scores indicate the algorithm's calculation that the candidate appears more similar to the probe image than candidates with lower scores further down the list, a true match may appear anywhere in the candidate list, if it appears at all. Accordingly, face recognition algorithms used by police are not designed to (and do not) return a single definitive match. Rather, they are probabilistic systems that return a number of *potential* candidates based on an "algorithmic best guess."[5] As one court put it, "[i]nstead of being designed to produce accurate results, [the FRT algorithm] is designed to produce possibilities." *State v. Archambault*, No. 62-CR-20-5866, slip op. at 14 (Minn. 2d Dist. Ct. Sept. 13, 2024), attached as Ex. A.

FRT searches usually return multiple results. In this case, the search returned at least eight possible-match candidate photos. Def's Ex. B; *see also* Tr. at 69 ("multiple photos of multiple people"). The number can often be higher, depending on the algorithm used and its settings. As a Detroit Police Department ("DPD") employee testified in another case, for example, FRT searches run by the DPD can return "anywhere up to 10 to 100 or 500" potential matches. Dep. of Joseph Dablitz 18:17–18, *Oliver v. Bussa*, No. 2:20-cv-12711 (E.D. Mich.), ECF No. 51-3. Naturally, only one of the many candidates can be an accurate identity match. The rest will be innocent "false positives."

Furthermore, a true match to the suspect photo often will not appear in the results at all, either because the quality of the probe image is low, or because the database of images being searched does not include the true match, or for other reasons. *See* Def's Ex.

[5] Eyal Press, *Does A.I. Lead Police to Ignore Contradictory Evidence*, The New Yorker (Nov. 20, 2023), https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence/.

C ("The quality of a submitted probe image, the lack of online images of a depicted individual in Clearview's Database, and other factors can impact and potentially reduce the accuracy of the Clearview search results.").[6]

Moreover, because many people share similar-looking facial characteristics, "[a]s more individuals are enrolled into a database, the possibility of a mismatch increases."[7] Clearview AI searches against a database comprised of "50+ billion facial images" scraped from the internet—an average of six photos for every person on earth.[8] A database in the billions means there is a high chance that any search will produce false positives.

These features of FRT systems mean that "[a]t best, any one of th[e] results is potentially a false positive. At worst, all results are undeniably false positives." *Archambault*, slip op. at 18. As the former Detroit Police Chief put it, "[i]f [police] were just to use the technology by itself, to identify someone, I would say 96 percent of the time it would misidentify."[9]

Although FRT algorithms generate false positives even in controlled test conditions, they are especially prone to error when probe image quality is low (as is often the case in real-world conditions), or when there are differences between the probe image

---

[6] *See* Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* 5, Nat'l Inst. of Standards & Tech. (2019), https://perma.cc/7L99-A2QJ.

[7] Nat'l Acads. of Scis., Eng'g, & Med., *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance* 53 (2024) [hereinafter "National Academies Report"], https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance.

[8] Clearview AI, *Company Overview*, https://www.clearview.ai/overview.

[9] Jason Koebler, *Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time*, Vice News (June 29, 2020), https://perma.cc/5YVX-PTET.

and the database images it is being compared against. As the Ohio Attorney General Facial Recognition Task Force explained in a 2020 report, "the performance of a facial recognition system depends on the quality of the image. Image quality is dependent on several factors including background, lighting, angle, facial expression and pose."[10] Other sources agree that lighting, shadow, angle, facial expression, and partial occlusion of the face all affect accuracy.[11] The resolution of an image (i.e., its blurriness or pixel density) can also have a huge effect on the ability of a FRT algorithm to produce an accurate match.[12] Each of these issues is well known to affect accuracy of a search.[13] And "[w]hen a face image simultaneously contains multiple confounding factors," the accuracy of the FRT search can be even further degraded.[14]

---

[10] Ohio Atty Gen. Facial Recognition Task Force, *Report & Recommendations* 10 (Jan. 26, 2020), https://perma.cc/H4NF-ANNU.

[11] *See, e.g.*, Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 2: Identification* 9–10, Nat'l Inst. Standards & Tech. (2019), https://perma.cc/BR6Y-6X6D; U.S. Dep't of Homeland Sec., DHS/ICE/PIA-054, *Privacy Impact Assessment for the ICE Use of Facial Recognition Services* 26 (2020), https://perma.cc/2TMV-JMGH.

[12] *See, e.g.*, Aman Bhatta et al., *Impact of Blur and Resolution on Demographic Disparities in 1-to-Many Facial Identification*, Proc. of the IEEE/CVF Winter Conf. on Applications of Comput. Vision (WACV) Workshops 412–20 (2024), https://perma.cc/MCQ3-QV5V.

[13] *See, e.g.*, National Academies Report, *supra* note 6, at 43 ("Typical problems include blur owing to motion; the subject not facing the camera; part of the face not visible owing to the subject wearing a cap, scarf, sunglasses, or the like; or the subject presenting a non-neutral expression."); *id.* at 46 (discussing effects of low "face quality" and "face aging").

[14] *Id.* at 47.

In this case, the probe image appears to have at least several features that render it likely to produce an inaccurate search result.[15] The probe image is a still from a store's surveillance camera video, in which the suspect is far away from the camera (and therefore the face is relatively small) and appears to be looking away at an angle. Images captured from business security cameras typically have relatively low image resolution, which impedes the accuracy of results, especially when combined with small image size, off-center angle, and poor lighting conditions.

Even where probe image quality is ideal, face recognition systems exhibit race, gender, and age bias, with higher rates of false matches when used on people of color, women, and young adults than on white people, men, and older people.[16] According to the National Institute of Standards and Technology, "even the best algorithms can be wrong more than 20 percent of the time" in test conditions,[17] and "Asian and African American people were up to 100 times more likely to be misidentified than white men, depending on the particular algorithm and type of search."[18] These disparities are a result of FRT algorithms being "trained mostly on White faces," on lighting and color contrast

---

[15] The version of the FRT images in the record is an extremely low-quality photocopy, which makes assessing the quality of the original images difficult. *See* Def's Ex. B.

[16] *See, e.g.*, National Academies Report, *supra* note 6, at 55–57; Grother, *supra* note 8, at 7–8; 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, 8–20 (2020), https://ieeexplore.ieee.org/document/9001031.

[17] Khari Johnson, *The Hidden Role of Facial Recognition Tech in Many Arrests*, Wired (Mar. 7, 2022), https://perma.cc/ECB6-LM22.

[18] Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, Wash. Post (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

issues with digital photography that result in images of darker skinned people being underexposed, and other factors.[19] In nearly every known U.S. suit against police alleging wrongful arrest due to police reliance on an incorrect FRT result, the person falsely identified and wrongly arrested is Black.[20] Defendant–Appellee in this case is Black.

On top of these technical problems, additional risk of error is introduced by human review of the FRT search results. Research has consistently shown that it is difficult for people to accurately identify people from other racial and ethnic groups.[21] When a human analyst does an initial review of a list of FRT-generated candidates, the analyst's own cognitive biases can compound racial biases in the FRT-generated candidate list.

Even further, people reflexively over-rely on computer outputs because of "automation bias," "a heuristic replacement for vigilant information seeking and processing" that can "lead to decisions that are not based on a thorough analysis of all available information but that are strongly biased by the automatically generated advice."[22] Automation bias lulls human users of automated technologies, such as FRT, into an over-reliance on seemingly foolproof computers, leading the analysts to uncritically accept the computer's returns.[23] Automation bias means analysts will be less

---

[19] U.S. Comm'n on Civil Rights, *The Civil Rights Implications of the Federal Use of Facial Recognition Technology* 24–29 (2024), https://perma.cc/D4VS-5866.

[20] *See* MacMillan et al., *supra* note 1.

[21] *See The Handbook of Eyewitness Psychology*, *Volume 1: Memory for Events* 257–81 (Michael P. Toglia et al. eds., 2007) (detailing dozens of studies); Kate Crookes & Gillian Rhodes, *Poor Recognition of Other-Race Faces Cannot Always Be Explained by a Lack of Effort*, 25 Visual Cognition 430 (2017).

[22] Raja Parasuraman & Dietrich Manzey, *Complacency and Bias in Human Use of Automation: An Attentional Integration*, 52 Hum. Factors 381, 391 (2010).

[23] *Id.* at 391–97.

critical and discerning when selecting a possible match, including by deferring to the ranking of similarity scores generated by the algorithm in place of the analyst's own judgment. Human analysts may also assume there is an accurate match in a computer's returns even when there is not.

For these and additional reasons, research shows that human operators make errors on average 50 percent of the time "when deciding which faces in candidate lists match the search image. This is consistent with research on eye-witness identification—which is known to be unreliable, with well-meaning witnesses often mistakenly identifying innocent suspects."[24]

Because of these and other sources of unreliability and error in the FRT search process, it is commonly agreed that the results of a face recognition search do not constitute a positive identification of a suspect, and that additional reliable investigation is needed to develop probable cause.[25] But far from detailing a reliable confirmatory investigation, the warrant affidavit in this case provided no independent confirmatory

---

[24] David White et al., *Human Oversight of Facial Recognition Technology in Forensic Applications* ¶ 5 (U.K. Parliament 2021), https://committees.parliament.uk/writtenevidence/38555/html/. *Accord* David White et al., *Error Rates in Users of Automatic Face Recognition Software*, 10 PLoS ONE e0139827 1, 1 (2015) (the selection process "potentially reduc[es] benchmark estimates [of FRT accuracy] by 50% in operational settings").

[25] Law enforcement policies on FRT use have long specified that FRT results do not constitute probable cause. *See, e.g.*, Lucas Daprile, *Northeast Ohio Police Have Access to AI-Powered Facial Recognition. Here's One of the Area's First Policies in Using it*, cleveland.com (Jan. 29, 2025), https://www.cleveland.com/news/2025/01/northeast-ohio-police-have-access-to-ai-powered-facial-recognition-heres-one-of-the-areas-first-policies-in-using-it.html (Northeast Ohio Regional Fusion Center's FRT policy "says its facial recognition reports are meant only to generate leads and cannot be used as probable cause"); Bureau of Just. Assistance, U.S. Dep't of Just., *Face Recognition Policy Development Template* 22 (2017), https://perma.cc/CWM7-2E88 (similar).

evidence for probable cause. As explained below, had police revealed accurate information about the FRT search to the judge when applying for the search warrant, the judge would have understood probable cause to be lacking, and could not have approved the warrant.

II. Suppression was proper because the issuance of a search warrant without probable cause was attributable to the detective's intentionally or reckless false statements in the warrant application.

"[A] warrant affidavit must set forth particular facts and circumstances underlying the existence of probable cause, so as to allow the magistrate to make an independent evaluation of the matter." *Franks v. Delaware*, 438 U.S. 154, 165 (1978). A magistrate cannot carry out their independent evaluation, however, when the affiant makes a "deliberately or reckless false statement." *Id.* In that circumstance, the magistrate "cannot be viewed as neutral and detached," because their evaluation is reliant on the officer's falsehoods rather than on an accurate recital of the facts. *State v. Castagnola*, 2015-Ohio-1565, ¶ 41.

"To successfully attack the veracity of a facially sufficient search warrant affidavit, a defendant must show by a preponderance of the evidence that the affiant made a false statement, either intentionally, or with reckless disregard for the truth." *State v. McKnight*, 2005-Ohio-6046, ¶ 31 (citation & quotation marks omitted). "'Reckless disregard' means that the affiant had serious doubts about the truth of an allegation." *Id.* Both misstatements and omissions may constitute false statements; "Omissions count as a false statement if designed to mislead, or made in reckless disregard of whether they would mislead, the magistrate." *Id.* (citation & quotation marks omitted).

Once a defendant demonstrates "by a preponderance of the evidence that the affidavit contains deliberately or recklessly false statements," the warrant must be suppressed if "the affidavit, without the false statements . . . [no longer] provides the requisite probable cause to sustain the warrant." *State v. Weimer*, 2009-Ohio-4983, ¶ 32 (8th Dist.) (quoting *United States v. Charles*, 138 F.3d 257, 263 (6th Cir. 1998); *see also Franks*, 438 U.S. at 156.

The relevant false statement in this case is in Paragraph 20 of the Affidavit:

> Affiant avers that utilizing the Fusion center they received an identification of the, as of yet, unidentified male suspect, based on the recovered surveillance video, and it was learned this male was currently paroled to the address 403 E 52nd Street, Apartment #1.

Aff. ¶ 20.

The claim that the officer "received an identification of the . . . suspect" contains both material omissions and an affirmative false representation.

The affidavit omits at least the following facts, which were known to Detective Legg, and the omission of which misled the judge by leaving the impression that the Fusion Center somehow made a reliable, definitive identification:

- The purported "identification" was derived from a face recognition technology search. S*ee* Def's Ex. B (Clearview AI FRT results); Tr. at 15–16 (Det. Legg acknowledging receipt of the FRT search results);
- The FRT search returned multiple photos of multiple people as investigative leads. *See* Def's Ex. B (Clearview AI FRT results showing at least eight possible-match candidate photos); Tr. at 60 (Det. Legg acknowledging that he "received multiple images" from the FRT search);

- FRT results are to be considered "investigative leads" only, and must be followed by "thorough investigations" to "independently verify" that an individual flagged by FRT is in fact a correct match, *See* Def's Ex. B (disclaimer on Clearview AI FRT search results); Tr. at 17 (Det. Legg acknowledging receipt of disclaimer).[26]

Moreover, the claim that Detective Legg "received an *identification*" (emphasis added) is false, because FRT cannot provide positive identifications. *See supra* Part I. Instead, as the Clearview AI search results explained, the technology can only provide "investigative leads." *See* Def's Ex. B. Similarly, the email from the Northeast Ohio Regional Fusion Center that was forwarded to Detective Legg (but not described in the warrant affidavit) explained that the FRT search process produced only a "*likely* match for Qeyeon Tolbert" based on "*similar* facial features between the individual in the photo you provided and the booking photo." Tr. at 15 (emphases added). These descriptions reflect a tentative lead, not a positive identification. This is material to the probable cause showing because, "[w]hile an unequivocal identification is generally sufficient to establish probable cause, an identification that is tentative or uncertain may, on its own, be insufficient." *Williams v. City of New York*, 2012 WL 511533, at *3–4 (E.D.N.Y. Feb. 15, 2012) (citing cases).

[26] Although the State now asserts that the detective conducted follow-up investigation to verify the FRT result, Appellant's Br. 13–14, the details of any such investigation were omitted from the affidavit, and so could not supply probable cause for issuance of the warrant. Indeed, in support of its argument in this Court, the State cites only the post-hoc description of the investigation proffered by the detective at the suppression hearing, not the text of the warrant affidavit submitted to the warrant-issuing judge. *See id.* at 13. Without presenting details of any follow-up investigation to the issuing judge, the detective deprived the judge of the critical opportunity to evaluate whether that investigation provided independent verification, or instead was tainted by possible errors or unreliability in the FRT search process.

The detective's falsehoods here are analogous to an officer falsely averring that a witness has positively identified a suspect, where actually the witness made only a tentative or uncertain identification. In *Pinkney v. Meadville, Pa.*, for example, the officer stated in the warrant affidavit that a witnesses "recognized" the suspect when presented with his photo. 648 F. Supp. 3d 615, 631 (W.D. Pa. 2023), aff'd, 95 F.4th 743 (3d Cir. 2024). In fact, the witness had said only that the suspect "*look[ed] an awful lot like* who [he] saw throw the punch at the bar." *Id.* at 635 (emphasis in original; first alteration added). The court held that because the witness's "statement was tentative rather than positive or certain," the representation in the affidavit of the witness's "identification of [the suspect] as positive and definitive" was misleading. *Id.* at 635, 642. Likewise here.

In addition to being factually false, the representation that the Fusion Center provided an "identification" also usurped the magistrate's role by presenting the detective's inference (that Defendant–Appellee was a match to the suspect) as fact. The Fusion Center did not purport to provide an "identification" when it passed along the FRT search results. Rather, it provided an "investigative lead." Detective Legg inferred that the FRT result plus other information meant that Defendant–Appellee was a match to the suspect. But rather than explain the basis of that inference, he passed it off as fact. "[T]he detective, by not disclosing that he had drawn an inference but instead presenting the inference as an empirical fact, usurped the inference-drawing function of the magistrate in determining probable cause." *Castagnola*, 2015-Ohio-1565, ¶ 42.

Faced with this scenario, the Ohio Supreme Court has explained that courts must "[d]etermine whether the hidden inference was so significant as to cross the line between permissible interpretation and usurpation." *Id.* ¶ 49. "A hidden inference should be

deemed significant if it can be fairly concluded that it had a substantial bearing on the magistrate's determination of probable cause in each of two respects:" its "[r]elevance . . . to the magistrate's inquiry," and its "[c]omplexity," meaning that "[t]he more complex and attenuated the logical process by which a relevant conclusion is reached, the more important it is that the magistrate receive an opportunity to test the inference for validity." *Id.* ¶ 49–50. If a hidden inference is deemed "significant," courts must determine whether the affiant "acted intentionally or with conscious indifference, [in which case] the warrant should be invalidated and the evidence suppressed." *Id.* ¶ 50.

Here, the "identification" inference was highly relevant because it was "required to provide the nexus," *id.* ¶ 58, between the alleged crime and the place to be searched, Defendant–Appellee's home. *See infra*. Moreover, the inference was complex, in that it required weighing the reliability of the FRT search results, the Fusion Center's interpretation of those results, and other purportedly confirmatory information. "This determination is so profoundly significant that the issuing magistrate should have been given the opportunity to test the validity of the undisclosed inference." *Id.*

As explained above, *supra* Part I, FRT systems are not designed to provide "identifications." Detective Legg knew as much, since he received an express disclaimer to that effect. Def's Ex. B. His false statements and misrepresentation were therefore at least reckless. He knew that FRT was the source of the purported identification, and the FRT results in his possession expressly warned that they were only "investigative leads." *Id.* And yet he concealed the source of the purported "identification" and vouched a level of certainty that the FRT search process could not sustain.

Once Paragraph 20 is stripped away, the affidavit lacks probable cause.[27] Contrary to the State's claim, Appellant's Br. 17, the other information in the warrant affidavit does not establish probable cause to search Defendant's apartment. At most, the remaining paragraphs of the affidavit show only that the unidentified suspect came and went from 403 E 152nd Street six days after the incident. Aff. ¶¶ 18, 21. But that building is a "three story, multiple unit residential dwelling." *Id.* at 1. Identifying a connection with a multi-unit apartment building *in general* does not establish probable cause to search a *specific* apartment within—here, Apartment 1. *State v. Smith*, 2002-Ohio-1069, at *4 (8th Dist.) ("search warrants generally are void if they describe a multiunit building when probable cause to search attaches to less than all units"). The misleading assertion of an "identification" by the Fusion Center was the only basis in the affidavit for a nexus between the suspect and Apartment 1. Aff. ¶ 21.[28] Consequently, the trial court's suppression order was proper.

CONCLUSION

For the forgoing reasons, amici urge the Court to affirm the suppression order.

---

[27] Under *Castagnola*, if a significant inference was represented as fact "intentionally" or with "conscious indifference," the warrant must be suppressed without assessing whether there would have been probable cause in the absence of the misrepresentation. *Castagnola* at ¶¶ 50, 60. If "the affiant negligently usurped the magistrate's inference-drawing authority," the court must "excise the inference, insert the omitted underlying facts, and reassess the affidavit for probable cause." *Id.* ¶ 51.

[28] The Ohio Attorney General argues that the detective's query of the Ohio Law Enforcement Gateway (OHLEG) revealing that Mr. Tolbert "was 'paroled to the address' in question" provided independent grounds for issuing the warrant. Ohio Atty Gen. Br. at 18 (quoting Aff. ¶ 20). But that parole status assertion relies on the predicate "identification" of the suspect; when the misleading assertion of an "identification" by the Fusion Center is removed, there is no nexus to the suspect's identity and no basis for asserting that "this male['s]" parole status and address was reliably known. Aff. ¶ 20.

Dated: April 4, 2025

Respectfully submitted,

/s/ Amy R. Gilbert
Amy R. Gilbert
Freda J. Levenson
American Civil Liberties Union of Ohio Foundation
4506 Chester Ave.
Cleveland, OH 44103
(614) 586-1972
agilbert@acluohio.org
flevenson@acluohio.org

Nathan Freed Wessler*
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

Stephanie Kessler (0092338)
Sixth Circuit Vice-Chair, Amicus Committee
National Association of Criminal Defense Lawyers
Kessler Defense LLC
215 E. 9th St., Suite 650
Cincinnati, OH 45202
(513) 316-5807
stephanie@kesslerdefense.com

Sidney W. Thaxter, Esq.*
NACDL 4th Amendment Center
1660 L St. NW, 12th Floor
Washington, DC 20036
(202) 465-7654
sthaxter@nacdl.org

Counsel for Amici

*Pro hac vice motion filed concurrently

CERTIFICATE OF SERVICE

I hereby certify that the foregoing document was electronically filed on April 4, 2025 via this court's electronic filing system. Notice of this filing will be sent to counsel for all parties by function of that system, and it may be accessed through that system.

/s/ Amy R. Gilbert
Amy R. Gilbert (0100887)

Exhibit A

STATE OF MINNESOTA | DISTRICT COURT

COUNTY OF RAMSEY | SECOND JUDICIAL DISTRICT

State of Minnesota, | File No. 62-CR-20-5866

Plaintiff

ORDER

vs.

Gerald Paul Archambault,

Defendant

The Ramsey County Attorney's Office alleged, via complaint, that on or about May 28, 2020, Gerald Paul Archambault did commit:

1. Burglary-3rd Degree-Steal/Commit Felony or Gross Misdemeanor in violation of Minn. Stat. § 609.582.3.

The Complaint was filed on September 15, 2020. On May 2, 2022, Mr. Archambault filed a motion seeking to prohibit the State from offering HCSO analyst Nicole Hughes's testimony and any facial recognition "match" under *Frye-Mack* and Minnesota Rules of Evidence 702. The Court heard part of the motion on November 8, 2022, but did not take up the *Frye-Mack* issue at that time. On March 15, 2024, Mr. Archambault filed a motion for an order seeking, in relevant part: (1) dismissal of the complaint due to lack of probable clause, (2) preclusion of IIT results as not generally accepted, (3) preclusion of IIT results as foundationally unreliable, and (4) preclusion or dismissal on due process grounds. The matter came before the Court for an all-day contested hearing on May 14, 2024. The issue was taken under advisement as of July 15, 2024. The Court has reviewed the submissions of the parties. Based on the following *Findings of Fact* and *Conclusions of Law*, the Court makes the following:

ORDER

1. FaceVACS Investigative Imaging Technology and the process employed here in determining an investigatory lead do not reliably and consistently produce accurate results. They fail the *Frye/Mack* test.

2. Mr. Archambault's motion to suppress evidence pertaining to the use of that facial recognition technology is **GRANTED**.

3. The due process concerns raised by Mr. Archambault are moot.

4. The Court takes no action on the discovery violations noted by Mr. Archambault because they relate to the use of facial recognition technology in this case.

5. The independent tip provided to law enforcement that identifies Mr. Archambault as the suspect in this case is enough for this matter to survive a challenge for probable cause.

6. Mr. Archambault's motion to dismiss for lack of probable cause is **DENIED**.

Dated: September 13, 2024

BY THE COURT:

Andrew S. Gordon
Judge of District Court

FINDINGS OF FACT

1. On May 28, 2020—amidst the period of civil unrest prompted by the murder of George Floyd—HealthEast Midway Clinic in Saint Paul, Ramsey County, was burglarized.
2. The Saint Paul Police Department's ("SPPD") Civil Unrest Task Force obtained and reviewed surveillance footage from the clinic. They observed footage of a man taking a large television from the clinic. Several other individuals were also observed on surveillance footage committing other independent acts.
3. Task Force members took screenshots of suspects seen on the surveillance footage. These images were disseminated to other law enforcement agencies, the public at large, and to the Criminal Information Sharing and Analysis ("CISA") Unit of the Hennepin County Sherriff's Office ("HCSO"). Analyst Nicole Hughes ("Analyst Hughes") received and reviewed these screenshots.
4. One of the screenshots provided to Analyst Hughes was of the aforementioned man seen on footage carrying the television out of the clinic.
5. On September 8, 2020, Analyst Hughes ran this image through the FaceVacs Investigative Imaging Technology ("IIT") program at the HCSO. She reviewed the FaceVacs results, which included 20 booking photos. Analyst Hughes ruled out several individuals from the photos based on physical dissimilarities. She then did a subjective visual comparison of Mr. Archambault's booking photos with the suspect photo and determined Mr. Archambault was possibly the person depicted in the HealthEast Midway Clinic footage. She did not retain the IIT run results but did provide Mr. Archambault as a potential lead to the taskforce.

6. On that same day, Sergeant Jennifer O'Donnell ("Sergeant O'Donnell"), who was a member of the Civil Unrest Taskforce, received and reviewed an anonymous email alleging that Mr. Archambault was the person seen removing the television from the clinic.
7. Sergeant O'Donnell then reviewed the surveillance footage and compared it to a prior booking photo of Mr. Archambault. Sergeant O'Donnell thought that Mr. Archambault's booking photo matched the man seen in the surveillance footage in question.
8. On September 15, 2020, Mr. Archambault was charged with a single count of felony third-degree burglary based almost entirely on the identifications noted above.
9. At the May 14, 2024 *Frye-Mack* hearing, the State called three witnesses: Dr. Manjeet Rege,[1] Joseph Courtesis,[2] and Analyst Hughes. Mr. Archambault called two witnesses: Thomas Runyon[3] and Dr. Michael King.[4] Each witness has some experience with the use of

[1] Dr. Rege is a professor of data science at the University of St. Thomas. Dr. Rege has a PhD in Computer Science from Wayne State University. Dr. Rege's expertise is in artificial intelligence, machine learning, big data management, data visualization, and statistical data analysis. (Ex. 5.). Dr. Rege has written or collaborated on nearly eighty peer-reviewed articles in his related fields of expertise.

[2] Mr. Courtesis served with the New York Police Department ("NYPD") for twenty-seven years. He is the former Commander of the NYPD Central Investigations Division. His work included direct supervision of the NYPD's facial recognition technology unit. He oversaw thousands of investigations that utilized facial recognition technology. Mr. Courtesis helped other police departments build out their own policies. He wrote and co-wrote several working documents, position papers, and policy documents on the subject. Mr. Courtesis is a member of several relevant organizations and committees, including the Facial Identification Scientific Working Group, the Biometric Institute's Technology and Innovation Group, the Security Industry Association's Facial Recognition Working Group, the International Association of Chiefs of Police Crime Prevention Committee, and the IIJS Institute's Law Enforcement Committee.

[3] Mr. Runyon possesses two math degrees, worked for the National Security Agency (doing pattern recognition in large-scale datasets), and now works for the Maryland Test Facility—which supports the work of the Department of Homeland Security. He has spent 15 years building systems and applications that perform identifications in large-scale datasets.

[4] Dr. King has a doctorate in electrical engineering and has spent much of his career studying neural networks. After receiving his PhD, he started work with the NSA. Dr. King focuses his research on FRT. Shortly after Dr. King began at the NSA, he started working on face recognition with a human interface security focus. After the NSA, he moved to the Central Intelligence Agency ("CIA"), researching biometrics. Dr. King then went to the Intelligence Advanced Research Projects Activity ("IARPA").[4] Since leaving IARPA, Dr. King has worked in academia, researching FRT relative to demographics. Lastly, Dr. King participated as a committee member on the National Academies of Sciences, Engineering, and Medicine's recent facial recognition technologies study.

facial recognition technology, the policies underlying its use, and best practices in the appropriate scientific field. However, it was Dr. Rege, Mr. Courtesis, Mr. Runyon, and Dr. King who were presented as expert witnesses.[5]

The technology.

10. FaceVACS Investigative Imaging Technology ("IIT") is a facial recognition technology ("FRT") software produced by the company Cognitec.[6] FRT captures facial information from a photo, often referred to as a "probe photo," and creates a template that is then compared to other facial templates. In doing so, the algorithm will produce a similarity score or confidence score that indicates how similar the probe template is to the existing templates in a dataset. IIT specifically "compares digital facial images from different sources to large facial image databases." (Ex. 2 at 6.) In doing so, for a given probe photo, IIT returns the top twenty results. It does indicate a confidence score, but no threshold is used; results with low confidence scores could show up in the top twenty results if there are no results with higher confidence scores. The technology is not absolute—it is evolving and remains a "hit-or-miss technology" that "is not a method to positively identify an individual." (Ex. 6). IIT is not reliable. *Id*.
11. But FRT, of which IIT is an implementation, is not new. Neither are its uses. The public uses it daily to unlock their phones with their face. Law enforcement uses it on license plate readers. Social media companies use it to suggest individuals whom a user might tag in posts and photos.

[5] Both the State and the Defense did excellent jobs summarizing the respective testimony of each of the witnesses. The Court will not reproduce their work and will instead more generally summarize the salient information.

[6] When discussing facial recognition technology generally, the Court will refer to it as FRT. When discussing the specific implementation at issue here, the Court will refer to it as IIT.

12. Each of these implementations involve the use of a probe image and the search of some kind of image repository or database; often, implementations involve processes which calculate a confidence score and determine whether there is "a match" between faces based on that confidence score. In some cases, like when we unlock our phone, it is a "one-to-one" use. When a picture of our friends and family gets uploaded to the cloud and those images get grouped into categories such as "spouse's images" or "your friends," the involved FRT employs a "one-to-little-n" use. Last, when a photo is uploaded to Facebook or Instagram and the service prompts us to tag a friend, FRT has been used in a "one-to-big-N" manner.

13. Despite the seeming ubiquitousness of FRT, the technology can and does make mistakes. A false positive occurs when a result indicates a match that should not be a match. A false negative occurs when the technology fails to return a positive result when the result should be a match. Low-quality probe images[7] have significant impacts on whether FRT can produce an accurate result. The underlying algorithms also struggle with persons of color because, for better or worse, they are not routinely trained on datasets that include populations of color.[8]

14. To reduce the chances that FRT produces an inaccurate result, most implementations employ the use of a threshold on its confidence scores. That threshold determines whether the technology categorizes a probe photo as a match to one or more images in its database.[9] The

[7] For example, where an individual may be wearing a mask, or the lighting is poor, or where both eyes cannot be seen. Similarly, a low-quality probe image may be the result of the distance of the subject or even whether their face is seen at an angle as opposed to directly in front of an individual's face. Dr. King specifically noted that surveillance footage often produces low-quality probe photos because they are almost always from a vantage point above an individual. See also Ex. 16 at pgs. 47, 52 and 56.

[8] Dr. Rege specifically notes that an algorithm "not trained on a large number of Native American faces . . . could have a hard time correctly identifying people of a Native American descent." (T. 56).

[9] When a threshold setting is set higher, the technology will require more similarities between the probe image and the images in its database. A higher threshold will potentially generate fewer match results following a search. A lower threshold will require fewer similarities between the probe image and the images in the technology's database. In turn, the technology will then likely consider more database images to be a match with the probe image.

lower the threshold, the higher the likelihood that any given results will return false positives. The higher the threshold, the higher the likelihood you may get false negative results. The threshold setting is adjusted with those two outcomes in mind and whichever of those outcomes the user is more willing to accept. The larger a dataset gets, the more difficult it is to find a balance between false positives and false negatives. A large dataset and a low threshold—or no threshold at all—will always return false positives.

15. As a result, human interaction with FRT results is essential. And more specifically, in the context of the use of FRT in criminal investigations, the technology cannot be relied on to produce an accurate identification, but it is instead an aid to a human identification. Each of the expert witnesses here agreed that FRT can only be used to generate a lead[10] that requires further investigation and subsequent validation.[11]

16. Humans are generally bad at recognizing faces. This is especially true for strangers. One study of this phenomenon used commercial Cognitec software to search a large image database to return the eight highest ranking results for a probe photo.[12] Participants were presented with the probe photo and the results and asked to decide if the person in the probe photo was present in those results. The person was present only half of the time. When the probe individual was completely absent from the results, participants correctly concluded the probe individual was absent only 40-45% of the time. They identified the wrong person as the probe individual 30-

[10] Though only Dr. Rege attempted to define "lead," it is clear that what all the witnesses referred to was the narrowing down of a suspect list from a large set of possibilities to a much smaller number of possible suspects—maybe one or two. Dr. Rege said that explicitly. (Tr. at pgs. 50-51.)

[11] This conclusion is also supported by the National Academies of Sciences, Engineering, and Medicine ("NASEM"). *See* Ex. 16 at pg. 102 (FRT is best used by law enforcement as a component of developing investigative leads).

[12] *See* Ex. 10.

40% of the time. In other words, they produced false positives. The errors persisted across both conditions, regardless of whether the probe individual was absent or present.

17. Humans can be influenced by suggestions that a match has already been made. A study of that phenomenon involved three groups: (i) a control group who were simply presented with two faces and asked if they were a match, (ii) a human-source group who were told that a human source had already identified the images as a match/non-match, and (iii) a computer-source group who were told that a computer source had already identified the images as a match/non-match.[13] When participants were told that either a human or computer had already determined the images were a match, the false positive rate was 25% (compared with 19% when no information was provided). Participants were also much more confident in their conclusion that face pairs were a match when they were told either a human or computer had already determined they matched.

18. Various applications of FRT have been vetted by a peer-reviewed research process not dissimilar to what one would expect of scientific analysis. In addition, the National Institute of Standards and Technology ("NIST") is a third-party evaluator of various algorithms, including through its NIST Face Recognition Vendor Tests.[14] In these tests, a version of Cognitec's algorithm performed as well as other FRTs currently on the market. The specific algorithm that supports the IIT used in this case is not marketed as being NIST evaluated. The specific manner in which IIT was used here was not evaluated by NIST. However, both Dr. Rege and

[13] See Ex. 12.

[14] NIST sets benchmarking datasets and benchmarking evaluation. NIST acts as a judge of relevant scientific technologies and grades how reliable or accurate the evaluated technologies are functioning. NIST evaluates the technologies and then provides feedback on the strengths and weaknesses of that software.

Mr. Runyon—the experts who reviewed NIST data—agree that NIST's evaluation demonstrates that FRT, as tested, is generally reliable.

The use of IIT in this case.

19. Analyst Hughes demonstrated her use of the IIT program in court.[15] Simultaneously, she recorded her computer screen. That recording was offered and received as Exhibit 3.

20. In her demonstration, an image of the suspect from the HealthEast surveillance footage was imported into the system and used as the probe photo. She demonstrated how the program returns the results and includes a confidence score. The confidence score is the program's accuracy estimate that the result is the same individual as in the probe photo. Analyst Hughes noted that they do not consider this confidence score when analyzing the results. It is simply ignored.

21. Analyst Hughes demonstrated how she ruled individuals out. Despite being one of the top twenty results, some rule-outs are obvious because the individuals clearly do not resemble the probe. Others are not. For example, Analyst Hughes was only able to rule out the individual in Result 4 because she determined that the neck tattoo visible in the 2017 booking photo does not appear in the probe photo. (Tr. at 79.) That individual shares the same last name as the defendant in this case. Having potential family members show up in results generated by IIT is commonplace.[16] (Tr. at 48.)

[15] She noted that the database the program uses has grown since the original use in Mr. Archambault's case. But asserted that this change would not alter the accuracy of the mock run done during the hearing. Mr. Runyon believed that the algorithm being utilized by IIT was different during the mock run. Approximately five of the photographs that were produced by the Cognitec software during the mock run were not in the initial results to first identify Mr. Archambault in 2020.

[16] FRT algorithms work because they turn identifiable facial structures into data points. False positives often come up where people share facial similarities—especially if they share facial structure. Dr. King noted that this drives false positives, and Analyst Hughes confirmed that such false positives are commonplace.

22. Ultimately, Analyst Hughes presented a lead to the task force responsible for investigating the underlying crime here. This was done consistent with how law enforcement around the country uses FRT.[17] But a lead could include a suspect who is known to be out of state when a particular offense is committed. (Tr. at 80.) That lead would be included because the result of this process is not meant to be an identification.

PROCEDURAL POSTURE

23. Mr. Archambault challenges the admissibility of evidence derived from the use of FRT and, specifically, evidence derived from the use of IIT in this case. He asserts that the use of IIT cannot survive either prong of the *Frye/Mack* admissibility standard—that this novel technology is not foundationally reliable. He asserts that, absent that evidence, the allegation against him must be dismissed for lack of probable cause and/or because due process demands it. Additionally, Mr. Archambault asserts that even if the identification evidence derived by IIT is admissible per *Frye/Mack*, such evidence should be excluded as a violation of due process—in short, that the use of IIT amounts to an unnecessarily suggestive out-of-court identification. The State objects and asks this Court to determine that the use of IIT here is foundationally reliable as required by the *Frye/Mack* standard. It asserts that Sergeant O'Donnell's investigation provides probable cause independent of any use of IIT.

[17] While Dr. King agreed that the process utilized here was proper, Mr. Courtesis was particularly adamant about that conclusion. Mr. Courtesis noted that multiple steps were taken to generate the lead and that Analyst Hughes reviewed the FRT system processing and ruled out results consistent with the guidelines laid out by the Facial Identification Scientific Working Group. The probe image used in the IIT system was suitable. Additionally, Analyst Hughes ruled out any leads of those that were incarcerated at the time and date of the alleged crime. Mr. Courtesis suggested that this step went above and beyond baseline procedures. He believed that, because the probe image identifying Mr. Archambault as the suspect was corroborated by an independent crime tip, the FRT use in this case was "consistent with utilizing the totality-of-the-circumstances approach to lead verification." (T. 90).

CONCLUSIONS OF LAW

24. The experts who testified in this case all but agree that FRT has a place in the investigation of crimes. That role seems to be growing daily. All the experts agree that FRT can be used in a reliable and consistent way. That is because the underlying science that supports the use of FRT is generally accepted within the relevant scientific community. However, IIT—as an implementation of FRT—does not consistently and reliably produce accurate results as is required by law.

25. "Under Minn. R. Evid. 702, expert testimony is admissible if: (1) the witness is qualified as an expert; (2) the expert's opinion has foundational reliability; (3) the expert testimony is helpful to the jury; and (4) if the testimony involves a novel scientific theory, the proponent must show it is generally accepted in the relevant scientific community." *State v. Berry*, 982 N.W.2d 746, 755 (Minn. 2022). That fourth prong is the *Frye-Mack* analysis. "The *Frye-Mack* standard, which was incorporated into Minnesota Rules of Evidence 702 in 2006, governs the admissibility of expert testimony that involves a novel scientific theory or emerging scientific techniques." *State v. Garland*, 942 N.W.2d 732, 746 (Minn. 2020).

26. If evidence sought to be admitted at trial involves a novel scientific theory or technique, the district court must hold a *Frye-Mack* hearing to "determine whether the underlying science is generally accepted within the relevant scientific community and whether the particular scientific evidence in the case is shown to have foundational reliability." *Id.* Scientific evidence is considered novel when its admission has not been litigated before a district court. *Goeb v. Tharaldson*, 615 N.W.2d 800, 814 (Minn. 2000). Minnesota courts apply the two-pronged *Frye-Mack* standard to analyze the "admissibility of expert testimony that involves a novel scientific theory or emerging scientific techniques." *Goeb*, 615 N.W.2d at 814. "First, a novel

scientific technique must be generally accepted in the relevant scientific community, and second, the particular evidence derived from that test must have a foundation that is scientifically reliable." *Id.* at 809. The proponent of the evidence has the burden of satisfying these two prongs. *Id.* at 810.

First Prong – General Acceptance

27. "The *Frye-Mack* standard asks first whether experts in the field widely share the view that the results of scientific testing are scientifically reliable." *State v. Roman Nose* 649 N.W.2d 815, 819 (Minn. 2002). "The results of mechanical or scientific testing are not admissible unless the testing has developed or improved to the point where experts in the field *widely share* the view that the results are scientifically reliable as accurate." *State v. Fenney*, 448 N.W.2d 54, 57 (Minn. 1989). "The scientific technique on which expert testimony is based must be scientifically reliable and broadly accepted *in its field*." *Fenny*, 448 N.W.2d at 58. Unanimity is not required. *Id.* Determining whether a scientific technique is generally accepted by the relevant scientific community is a question of law. *See State v. Dixon*, 822 N.W.2d 664, 672 (Minn. Ct. App. 2012). "Members of the relevant scientific community include those whose scientific background and training are sufficient to allow them to comprehend and understand the process and for a judgment about it." *United States v. Porter*, 618 A.2d 629, 635 (D.C. 1992).

Novelty

28. The first step of the first prong is to determine if a "novel" scientific technique exists. The court in *Roman Nose* held that while DNA testing was generally accepted and had been extensively litigated, the particular technique the State introduced was a method of analysis that had not been reviewed by the court. *Roman Nose*, 649 N.W.2d at 820-21. The court stated

that the previous analysis of RFLP DNA testing had already been determined to be generally acceptable but that the new PCR-STR DNA testing had not been litigated. *Id.* The novelty component for a *Frye-Mack* hearing is based on whether a court has reviewed the technology, not whether the technology has been in use for a particular period of time. *See id.* at 821 (stating that even though the PCR-STR testing had been in use by the Bureau of Criminal Apprehension, it had never been reviewed by a court, rendering it a novel scientific technique). The court in *Roman Nose* then stated that the *Frye-Mack* hearing should involve both a look at the DNA testing procedures used in the underlying case and also a review on the "general acceptance of the technique within the relevant scientific community . . . ." *Id.* at 822.

29. The experts who testified in this case all agree that FRT has been in use for decades (at least in some form). Algorithms such as that used by the IIT program are only around a decade old. Their use in courts is novel, though. Minnesota courts have not yet addressed the use of such algorithms in criminal investigations and before criminal juries.

Relevant Scientific Community

30. Members of the relevant scientific community on FRT were well represented at the *Frye/Mack* hearing in this case. Each of the witnesses is well qualified to speak to FRT, its various implementations, and the specific use of IIT in this case. None of the witnesses claimed that FRT had no place in law enforcement investigations. It seemingly does. Sans Mr. Runyon, they also agreed that IIT, even as used here, was the best-practice implementation of FRT.

31. While the more ubiquitous uses of FRT (unlocking your phone or having a social media site automatically tag your friends and families in photos) may not be wholly appropriate in a criminal investigation setting, the experts agree that there is value in a tool that can help narrow down the identity of an unknown, individual suspect to a smaller candidate list. Once that

candidate list has been created, a human must intervene. That person must then manually review the smaller list and make an independent determination as to whether a prospective lead exists. That lead requires further investigation, validation, and confirmation. That process—employing the general use of FRT and the specific use of IIT—is generally accepted amongst the experts who testified here and generally accepted in the applicable scientific community.

Despite its general acceptance, IIT is unreliable. It fails the second prong of the Frye/Mack analysis.

32. That a test enjoys general acceptance in its relevant scientific community does not mean that its results are admissible in criminal court.[18] While FRT plays a growing role in criminal investigations, it is not clear that IIT is foundationally reliable. The State has failed to meet its burden to show that, as used here, IIT can consistently produce accurate results. That is simply not what this version of the technology was designed to do. Instead of being designed to produce accurate results, it is designed to produce possibilities. And by Cognitec's own admission, this is evolving, unfinished, and unreliable technology that is, at best, hit-or-miss.

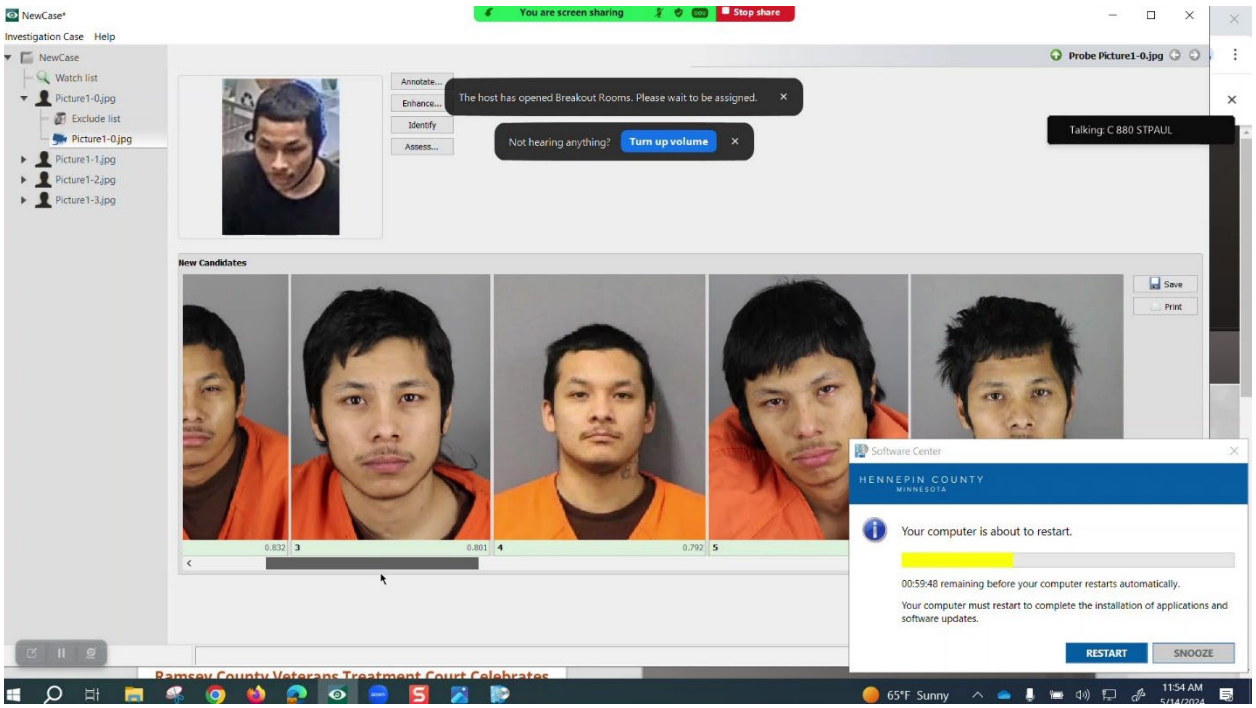
33. "The *Frye-Mack* standard asks . . . second whether the laboratory conducting the tests in the individual case complied with appropriate standards and controls." *Roman Nose*, 649 N.W.2d at 819. "Foundational reliability 'requires the proponent of a test [to] establish that the test itself is reliable and that its administration in the particular instance conformed to the procedure necessary to ensure reliability.'" *Goeb*, 615 N.W.2d at 814 (citing *State v. Moore*, 458 N.W.2d 90, 98 (Minn. 1990)); *see also Doe v. Archdiocese of St. Paul*, 817 N.W.2d 150, 165 (Minn.

[18] For example, polygraph tests are generally accepted in the communities in which they are used. The results of a polygraph test are not admissible in a criminal court as evidence, though. *State v. Opsahl*, 513 N.W.2d 249, 253 (Minn. 1994) ("It is well established that the results of polygraph tests, as well as evidence that a defendant took or refused to take such a test, are not admissible in Minnesota in either criminal or civil trials.") Polygraph testing does not have "such scientific and psychological accuracy, nor its operators such sureness of interpretation of results" as to justify submission of that evidence to a jury. *State v. Kolander*, 236 N.W.2d 458m 465 (Minn. 1952).

2012). "Without a foundation guaranteeing the test's reliability, the test result is not probative . . . and hence is irrelevant." *State v. Dille*, 258 N.W.2d 565, 567 (Minn. 1977).

34. In *Berry*, the defendant argued that the State "needed to offer data about accuracy, error rates, and peer-reviewed studies to establish the foundational reliability" concerning cell phone site tracking analysis. *Berry*, 982 N.W.2d at 757. The court disagreed, noting that *Harvey* was able to establish foundational reliability without the demanded types of evidence. *Id.* (citing *State v. Harvey*, 932 N.W.2d 792, 808 (Minn. 2019)). What the *Berry* court did confirm, though, was that the State must show that the test or mechanism that generates the evidence it offers is generally reliable, consistent, and accurate. *Id*. (citing *Doe*, 817 N.W.2d at 168).

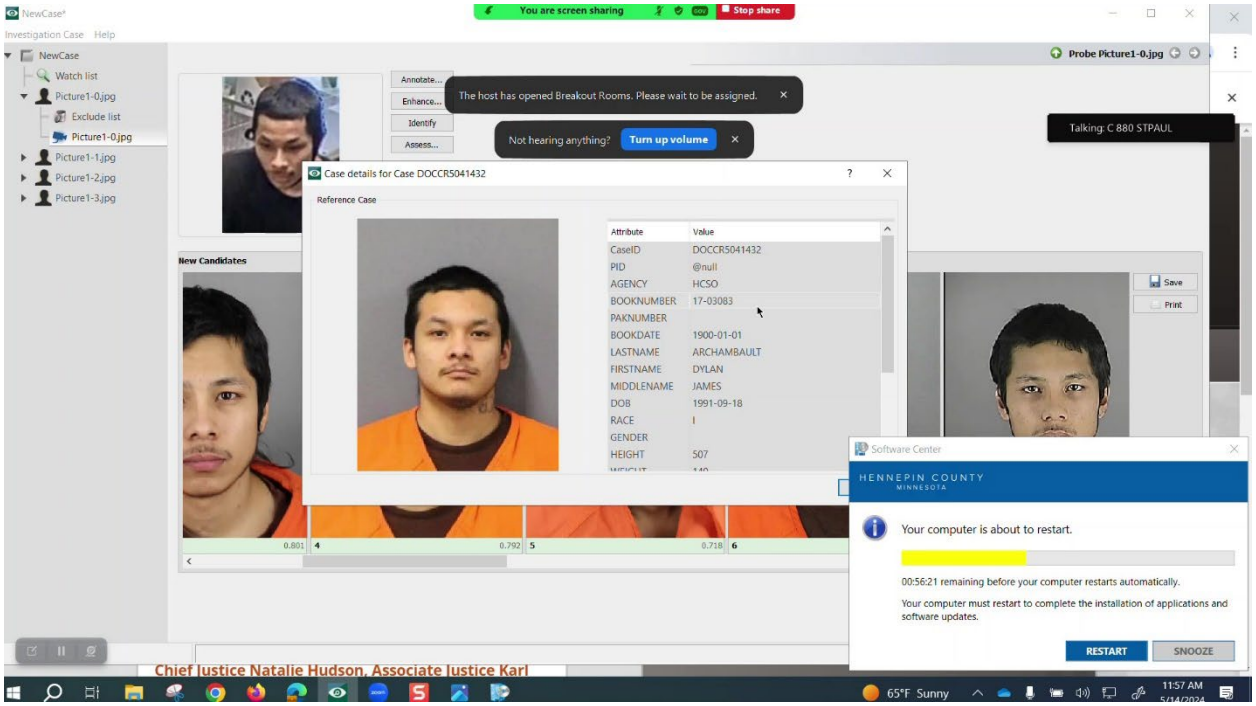
35. FaceVAC's IIT is designed to display its "top" results without regard to whether those results would otherwise meet an acceptable threshold of accuracy. This is problematic for at least two reasons. First, and most important, the "test" is designed to produce and display results that are clearly inaccurate and unreliable. Ms. Hughes demonstrated that through her testimony and through the demonstration conducted at the May hearing.



Ex. 3. Screenshot at 7m00s showing Candidate 4.

The IIT used in this case returned Candidate 4 as a result with a confidence score of 0.792—that is, it calculated with 79% certainty that the individual in that picture matched the probe photo. That individual is not Gerald Archambault. If you believe the State's assertions that Mr. Archambault is the suspect here, then the IIT returned an inaccurate result.

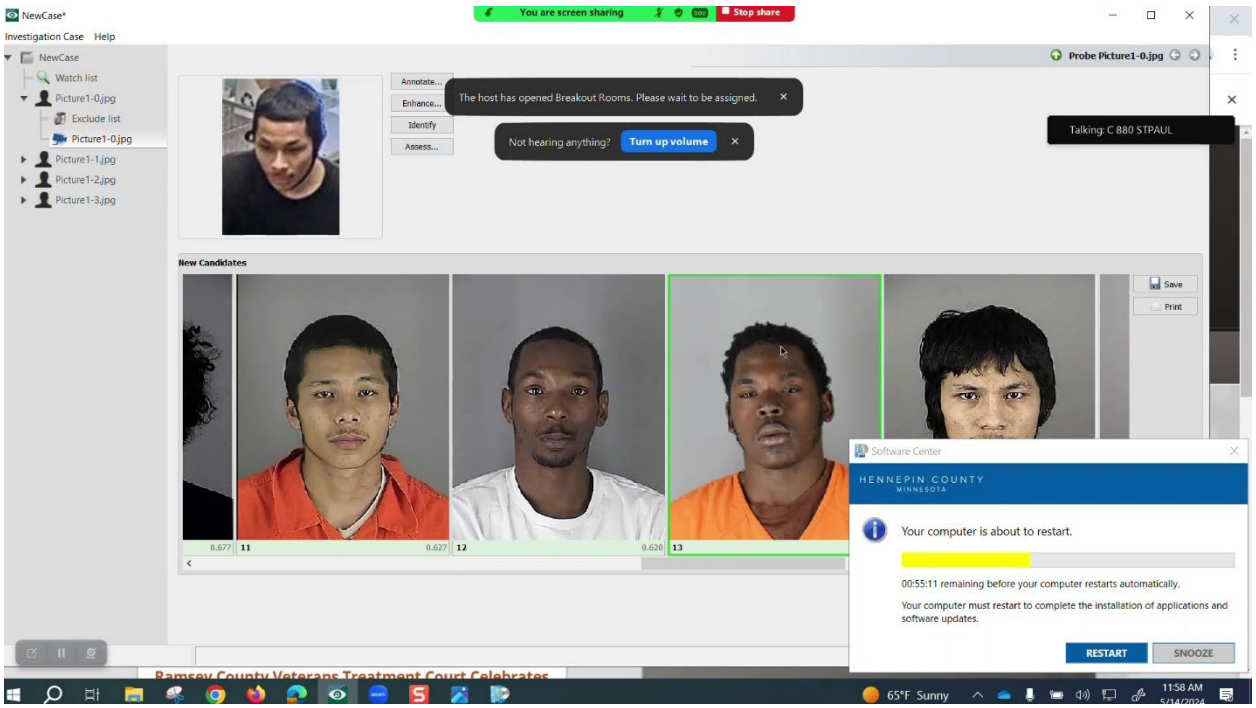
36. And in this specific instance, that inaccurate result might be understandable. That's because Candidate 4 shares the same last name as Mr. Archambault.



Ex. 3. Screenshot at 10m27s showing the case details for Candidate 4.

This is precisely that type of misidentification that some of our testifying experts were wary of. And apparently this is common. Analyst Hughes testified in November of 2023 that "among the results, there was another person, even, with the same last name, but that is common. I have seen family members show up because they have similar bone structures." (Tr. at 48.) At the end of the day, this type of inaccurate result appears to be commonly and reliably produced using IIT.

37. In addition, the existing software produces results that are woefully and obviously inaccurate. One need look no further than the rest of the run results generated in this case.



Ex. 3. Screenshot at 11m37s showing the mock run results.

The likelihood that an analyst would have selected Candidates 12 and 13 as leads is low. But the fact that the IIT used here generated those individuals as results in this investigation is either testament to how poorly it performs its job or evidence that it is not designed to produce results that are genuinely accurate. The parties disagree on whether the State need provide error rates, but what the law is clear on is that the State must show that the test or mechanism that generates the evidence it offers is generally reliable, consistent, and ***accurate***. That showing has not been made here, and this Court is not aware of any other tests or systems that form the basis for admissible evidence in which the underlying test or program produces results that are so wholly wrong and inaccurate—certainly none that produce inaccurate results by design.

38. Furthermore, because the IIT used here does not utilize a threshold to better discern more accurate results, nothing precludes an analyst from using a probe photo to generate a run result

of individuals who "match" the probe with a confidence score of less than 60%[19] (displayed as 0.60 and below)—that is, the IIT generates results where no individual is better than a 60% match to the probe. Analyst Hughes explained that it is her office's policy to ignore those scores and to plow ahead regardless, and if a lead is developed, it is passed along just like a lead was passed along in this case. That lack of discernment means that this technology cannot consistently, reliably, or accurately produce results. But then, it isn't trying to do that. Otherwise, it would employ the same protection utilized in other operational uses of FRT: the threshold. When accuracy and reliability matter, those who implement this technology do so in a way that utilizes a threshold. That such an implementation is missing here is telling.

39. Instead, the IIT is designed to winnow down a much larger dataset of "suspects" to a list of twenty potential matches. At best, any one of those results is potentially a false positive. At worst, all results are undeniably false positives. The IIT cannot differentiate. It produces this cascade of inaccurate, false positives by design. Because of this a human analyst is required to sort through the muck to find the hidden treasure.

Having an analyst review, rule-out, and otherwise process a "lead" does not make the test and this process any more reliable or accurate.

40. Notwithstanding the design flaws inherent in the IIT, the State asserts that the test is saved by human involvement. The experts who provided their opinion on this issue mostly seem to agree as well that the best-case use of FRT in criminal investigations involves the use of a human to review results produced by the technology to produce a lead. But this Court disagrees,

[19] The Court uses 60% only because the run results demonstrated by Analyst Hughes suggest that even at that "high" of a confidence score, the results are subject to significant variance. You could imagine a run result where no confidence score got above 50% or 40% or even lower. The fact remains that, without the use of a threshold, such returns are entirely possible.

especially with regards to whether evidence derived from the use of IIT is admissible pursuant to our rules of evidence.

41. Of the experts who testified in this case, only one opined that the use of IIT here did not comport with best practices. The outlier was Thomas Runyon. He also happened to be the only individual who testified about his review of studies on bias and on how poorly a human being performs when asked to verify whether a result "matches" a probe—the type of search done in this case. Of specific note, Mr. Runyon testified—and the defense late submitted the relevant text—that, in a somewhat similar use of FRT, participants performed poorly. The study used commercial Cognitec software to import a probe photo and return the highest ranking eight results. The software in this study compared the probe photo against a large image database. Participants were presented with the probe photo and the results and asked to decide if the person in the probe photo was present in those results. The probe individual was intentionally omitted from the results half of the time. Participants correctly concluded the probe individual was absent only 40-45% of the time, and they identified the wrong person as the probe individual 30-40% of the time. The errors persisted across both conditions, regardless of whether the probe individual was absent or present.

42. Another study involved three groups:

    - a control group who were simply presented with two faces and asked if they were a match,
    - a human-source group who were told a human source had already identified the images as a match/non-match, and
    - a computer-source group who were told that a computer source had already identified the images as a match/non-match.

When participants were told that either a human or computer had already determined the images were a match, the false positive rate was 25% (compared with 19% when no information was provided). Participants were also much more confident in their conclusion that face pairs were a match when they were told either a human or computer had already determined they matched.

43. Mr. Runyon opined that these studies demonstrate that humans are likely to be influenced by a computer's determination that a probe photo and another photo have "matched." He concluded that the use of IIT to suggest matches or identifications would unduly influence the human being asked to weed through the findings. The veracity of these studies and their conclusions were not challenged by the State, nor were they refuted by any of the other expert witnesses. The issues identified would seem to indicate that there is a real problem with FRT, and IIT specifically, influencing a human reviewer.

44. This Court imagines that one of the reasons Analyst Hughes and her team ignore the confidence scores is to avoid the influence problem noted above. However, as they go about their work, the analyst still knows that the program has indicated some kind of "match," even if it is with a low confidence score. The analysts know that these are the top results generated after an exhaustive search of a very large database of individuals. And while Analyst Hughes and her team are armed with information[20] that should make the job of ruling out a result easier, this case—like others could be—came down to her determination that a matched image generated by the softward showed an individual who best matched the probe photo. There is a process for that, but per Analyst Hughes's own testimony, that determination could result in the

[20] Analyst Hughes testified to being able to access demographic information about an individual present in the results. She demonstrated such access at the May hearing. Similarly, she can determine if someone was in custody on any relevant dates and can also determine when a particular photo was generated or taken.

production of a "lead" even if the individual suspect could not have committed the alleged offense:

> "Once I've ruled out as many as I can and if I think that -- after doing analysis for assessing the photo, doing comparisons from an unknown to many, I find a more recent photo that may not be among the booking pictures in here. It could be from another agency. It could be from social media. But I then compare that known party and their scars, marks, tattoos, hairstyle, height, weight as close as I can determine was known compared -- in reference to the day of the photo. And that's when I provide a lead to an investigator: "Here's who I think it could be. You should investigate further. Here's why." And if there are things like hair, scars, marks -- such as that -- or they were out of custody at the time or geographically, um -- if I can't rule them out of being in town at the time. ***If I saw something on social media putting them out of state, I would probably hesitate and say, "Please investigate further before" -- but everything that I'm providing after that point is just a lead.***"

(Tr. at 79-80.) (Emphasis added).

If nothing in this process prevents the relay of an, at best, approximate lead when there is evidence that the person could not have committed the alleged offense, then the process is not reliable, nor is it accurate. It is flawed and may be inherently so.

45. The human intervention here cannot save those flaws. The human analyst is subject to the influence that IIT has produced a "match"—that is, the human analyst could produce a lead not because the results produced by IIT are accurate, but because the results *were* produced. And without a threshold, the system is designed to produce inaccurate results. Additionally, even once a human intervenes, the process outlined here allows an analyst to suggest a lead even in the face of evidence that would prevent that potential suspect from committing the crime.

46. Like the polygraph test before it, this Court has little doubt that FRT may be valuable in the course of investigative work. It could very well lead to arrests and the remedy of cases that would otherwise have gone unsolved. And much like polygraph testing, the State has not demonstrated that inaccuracies built into the use of IIT are saved by the interpretation and

intervention of a human analyst—not when humans are so easily influenced by indication that a "match" has been made and not when leads produced by this process could be produced even when evidence suggests that the potential suspect could not have committed the alleged crime. That is not a process designed to consistently and reliably produce accurate results. It cannot form the basis for admissible evidence of an individual's identification because it does not meet the requirements under *Frye/Mack*.

47. Because the Court has determined that the evidence derived directly from the use of IIT in this case is not foundationally reliable and is not admissible, it need not address the due process concerns articulated by Mr. Archambault and his counsel.

48. Similarly, because the discovery violations alleged exclusively relate to information about the technology used in this case, this Court need not articulate a response now that the evidence derived from that technology is not admissible. The Court does note that the most egregious issue raised by the defense relates to the failure of the State to preserve the initial run results. Those results could have had exculpatory value, but the failure to preserve them was not done in bad faith.

The investigation done by Sergeant O'Donnell provides enough probable cause for this case to continue.

49. Mr. Archambault asserts that the "facial recognition 'lead' provided by Analyst Hughes is the sole evidence with which the State seeks to prove the identity of the perpetrator." If so, then he argues that there is not probable cause to charge him with a crime. The assertion and conclusion are based wholly on the premise that there is no other reliable evidence that could support a finding of probable cause. That premise is incorrect.

50. A person may be charged with a crime only where there is probable cause to believe that the person is guilty[21]—that is, where facts have been submitted to the district court showing a reasonable probability that the person committed the crime. Minn. R. Crim. P. 2.01; *State v. Lopez*, 778 N.W. 2d 700, 703 (Minn. 2010); *and see State v. Florence*, 239 N.W.2d 892, 896 (Minn. 1976).[22] Probable cause determinations are fact-intensive determinations that must be made on a case-by-case basis. *State v. Knoch*, 781 N.W.2d 170, 180 (Minn. Ct. App. 2010). Unlike proof beyond a reasonable doubt or preponderance of the evidence, "probable cause requires only a probability or substantial chance of criminal activity, not an actual showing of such activity." *State v. Harris*, 589 N.W.2d 782, 790-91 (Minn. 1999) (quoting *Illinois v. Gates*, 462 U.S. 213, 244 n. 13 (1983). "The district court must view the evidence in the light most favorable to the State and may not assess the relative credibility or weight of conflicting evidence." *State v. Barker*, 888 N.W.2d 348, 353 (Minn. Ct. App. 2016) (citations and quotation omitted).

51. Probable cause is not a high bar to meet. It only requires that the State show a probability or substantial chance of criminal activity. That burden has been met here. Seemingly independent of the work of Analyst Hughes, Sergeant O'Donnell received a tip that the suspect they were looking for was Gerald Archambault. She conducted her own review and compared the images from the surveillance video with images of Mr. Archambault that she pulled. She determined that Mr. Archambault was the suspect they were looking for.

[21] Upon a defendant's motion to dismiss for lack of probable cause, the "court must determine whether probable cause exists to believe that an offense has been committed and that the defendant committed it." Minn. R. Crim. P. 11.04, subd. 1(a).

[22] The test of probable cause is whether the evidence worthy of consideration brings the charge against the defendant within reasonable probability.

52. While the defense is correct that an unverified anonymous tip cannot itself support a finding that probable cause exists, *see for e.g.*, *Olson v. Comm'r of Pub. Safety*, 371 N.W.2d 552, 556 (Minn. 1985) (finding an anonymous tip without indicia of reliability insufficient to establish reasonable suspicion to initiate a traffic stop), we don't have an unverified tip in this case. Sergeant O'Donnell followed up on the tip. It was investigated. Her work is the verification needed. Viewing that evidence in the light most favorable to the State, the Court must conclude that there is a substantial probability that Mr. Archambault has been linked to criminal activity. Probable cause exists for this case to continue to trial.

Dated: September 13, 2024

BY THE COURT:

Andrew S. Gordon
Judge of District Court