AMERICAN CIVIL LIBERTIES UNION FOUNDATION
New Jersey

P.O. Box 32159
Newark, NJ 07102

Tel: 973-642-2086
Fax: 973-642-6523

info@aclu-nj.org
www.aclu-nj.org

DILLON REISMAN
Staff Attorney

dreisman@aclu-nj.org
973-854-1718

November 24, 2025

Appellate Division Clerk's Office
Hughes Justice Complex, 5th Floor
25 Market Street
P.O. Box 006
Trenton, New Jersey 08625

Re: *State of New Jersey v. Sorah S. Tyner*
Docket No.: A-229-25 (AM-652-24)

Honorable Judges of the Appellate Division:

Pursuant to *Rule* 2:6-2(b), please accept this letter brief in lieu of a more formal submission on behalf of amicus curiae the American Civil Liberties Union of New Jersey ("ACLU-NJ") in the above-captioned matter.

TABLE OF CONTENTS

PRELIMINARY STATEMENT

If cell phones map the entirety of our private lives, then mobile device forensic tools ("MDFTs") are the powerful compasses law enforcement officers use to chart them. As with any new technology, these tools raise new dangers for our privacy rights requiring the careful application of our longstanding protections under Article I, Paragraph 7 and the Fourth Amendment.

Yet the State failed to heed these protections in its search of Ms. Tyner's phone. Amicus ACLU-NJ agrees with Ms. Tyner that the warrant authorizing the search of Ms. Tyner's phone was a "general warrant" requiring complete suppression. Here, amicus provides further arguments in favor of reversal.

STATEMENT OF FACTS AND PROCEDURAL HISTORY

Amicus relies on the Statement of Facts and Procedural History contained in the Brief on behalf of Defendant-Appellant Sorah S. Tyner, filed with this Court on October 15, 2025.

ARGUMENT

I. Warrants authorizing the inspection of data on a cell phone must cabin the scope of the search to data for which there is probable cause, not "any and all" data.

A warrant can never authorize the unbridled search a person's cell phone; like any warrant, it must cabin the scope of the search to only the

particular data connected by probable cause to the alleged crime. *State v. Marshall*, 199 N.J. 602, 633 (2009) (citing *Maryland v. Garrison*, 480 U.S. 79, 84 (1987)). This requirement goes back to the Founding:

> The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.
>
> [*Garrison*, 480 U.S. at 84.]

Yet a general warrant is precisely what the State obtained to search Ms. Tyner's phone. The State has claimed that it requires unfettered authority to rummage through "any and all" data on the phone for technical reasons, but that is not an excuse for giving officers limitless discretion contrary to our warrant requirement. Regardless of the technical obstacles that might face the process of a search, a warrant must nonetheless define with particularity the object of its search so that officers may delineate between responsive and unresponsive data. While the addition of a time period to limit the subject matter of the search may be necessary, it is not sufficient where it still leaves "any and all" data open to inspection regardless of its connection to the crime.

Cell phones often contain the entirety of our private lives within them. As the Court explained in *Riley v. California*,

> a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.
>
> [*Riley v. California*, 573 U.S. 373, 396-97 (2014).]

Our phones contain copies of most electronic communications or phone calls we have ever made and records of everywhere we have been. *See Carpenter v. United States*, 585 U.S. 296, 311 (2018) (explaining how phones "faithfully follow [their] owner" wherever they go). We use applications on our phones to track our health, discuss private family matters, share our political views, confer with doctors, clergy, or therapists, keep private photos, and much more. *See Lipsky v. N.J. Ass'n of Health Plans, Inc.*, 474 N.J. Super. 447, 473 (App. Div. 2023) (noting that phones often contain "confidential and even privileged information").

The requirement of "particularity" secures the privacies of our phones from indiscriminate searches by law enforcement and the threat of the dreaded general warrant. *Garrison*, 480 U.S. at 84; *see also Facebook, Inc. v. State*, 254 N.J. 329, 346 (2023). "Particularity" ensures that law enforcement be directed to search only the "specific areas and things for which there is probable cause to search," by ensuring that officers can "with reasonable effort identify the place to be searched" or the "items to be seized." *Marshall*, 199

N.J. at 611, 630; *State v. Muldowney*, 60 N.J. 594, 600 (1972). Warrants must provide "guidelines" that limit the discretion of executing officers and give officers a basis upon which to distinguish between the items subject to seizure and those that are innocuous. *Muldowney*, 60 N.J. at 600 (finding that a warrant was defective where it was not "sufficiently definite" and "delegated" to the executing officer the decision of what materials would meet the crime of obscenity). A warrant cannot give unfettered discretion without some definite statement or "descriptive fact" of the goal of the search. *Cf. State v. Sims*, 75 N.J. 337, 348, 351 (1978) (finding that a warrant must give a "descriptive fact" that provides the logical connection between the people or places to be searched and probable cause).

This Court applied these principles in *State v. Missak* to quash an expansive warrant covering a phone's "entire contents." 476 N.J. Super. 302, 321-22 (App. Div. 2023). That warrant failed to limit its search to only those particular data and information on the phone for which there was probable cause to believe contained "evidence of the crimes for which [the] defendant has been charged." *Id.* at 322. Although the Court in *Missak* noted that it wasn't considering this through the lens of "particularity," since the warrant sought was "specific" to the entirety of the phone, this is just a matter of frame of reference. The Court suggested it would likely find probable cause to search

through a smaller subset of data on the phone had the warrant been more particularized (in that case, data covering a more limited time period and only the communication apps that the defendant was known to have used in the commission of the alleged crime). *Id.*; *see also id.* at 321 n.7 ("[T]he certification should present facts enabling the court to determine the precise data for which probable cause has been established and to authorize a search of that data with the requisite particularity.").

Other courts have found that "any and all" data warrants are unconstitutional general searches precisely because they lack any sort of principle to limit the scope of the search to particular data for which there is probable cause. *See Wheeler v. State*, 135 A.3d 282, 306-07 (Del. 2016) (finding that a warrant allowing the search for any device data, even though the aim of the State's investigation was only written communications, was an impermissible general warrant). As the Oregon Supreme Court found, a cell phone search's "enhanced risk of extensive governmental intrusion into a defendant's privacy interests" should require warrants to "identify, as specifically as reasonably possible in the circumstances, the information to be searched for" and describe the target of the search to "permit law enforcement, exercising reasonable effort, to identify the information sought with a reasonable degree of certainty." *State v. Turay*, 532 P.3d 57, 74 (Or. 2023).

Such an approach also enables courts to review "whether the forensic steps of the search process were reasonably directed at uncovering the evidence specified in the search warrant." *People v. Hughes*, 958 N.W.2d 98, 119 (Mich. 2020) (providing criteria that reviewing courts must have sufficient information to apply when evaluating the reasonableness of a phone search); *see also State v. Smith*, 278 A.3d 481, 496-97 (Conn. 2022) ("[A] warrant for the search of the contents of a cell phone must be sufficiently limited in scope to allow a search of only that content that is related to the probable cause that justifies the search.").

By these lights, the warrant in this case plainly "vest[ed] executing officers with unbridled discretion." *Taylor v. State*, 260 A.3d 602, 617 (Del. 2021). It contained no descriptive fact to limit the search of the phone to any particular category of evidence; the bare statement that the phone would be searched for evidence of "VEHICULAR HOMICIDE N.J.S.A. 2C:11-5, MANSLAUGHTER N.J.S.A. 2C:11-4" supplies no nexus between probable cause and the particular information to be sought after. (DCa17).[1] For example, this general warrant authorizes forensic analysts to look at Ms. Tyner's entire camera roll, any application data, and entire communications

[1] DCa refers to the Confidential Appendix to the Defendant's Brief. SMa refers to the appendix to the State of New Jersey's brief opposing the motion for leave to appeal.

without any "descriptive fact" binding the officers to inspect only that data which pertain to the alleged crime of distracted driving. In this case, even if we assume that there was probable cause that the use of the cell phone played a role in a distracted driving incident, it is simply not true that "any and all" data on the phone would constitute evidence of this crime. Why, for example, would data from a private Notes app tend to prove distracted driving?[2] The warrant lacks limiting language that would allow such data to be ruled in or out of bounds.

The warrant's few attempts to justify its breadth are based on generic information concerning how cell phone forensics may be complicated by the fact that cell phone data are stored in "complex interconnected structures," that timestamps may be misleading, and that some users "can conceal evidence within the device." *See, e.g.*, DCa11-12. But this is a red herring and should have no bearing on particularity.

First, *Missak* already concluded that warrants require more than unsupported theories about what "may" have occurred on a cell phone. *Missak*, 476 N.J. Super. at 320-21. But even if law enforcement has definitive reason that a search might encounter difficulties, an affidavit still must include the definite facts or criteria that define the objective of the search. *See Marshall*,

[2] *See* Point III for further discussion of what may constitute relevant evidence.

199 N.J. at 616 (noting that even if law enforcement might have justification for not being able to be more specific in which of two apartments to search, they still must specify that the search is limited to "the premises occupied by [the defendant]"). *See also People v. Herrera*, 357 P.3d 1227, 1233-34 (Co. 2015) ("If we were to hold that any text message folder could be searched because of the abstract possibility that it might have been deceptively labeled, we would again be faced with a limitless search . . . .").

Second, even if the affidavit had limited the responsive data to six days as the motion court suggested, it could not have saved the warrant from being a general warrant. Six days of "any and all" data on a person's cell phone, without any additional limitations or statements limiting law enforcement discretion to only that data connected to the alleged crime, does not change the fact that law enforcement had essentially unfettered access to a wide, undefined swath of Ms. Tyner's private life far beyond what would constitute evidence of phone usage in the minutes leading up to a car accident. Where this failure of particularity occurs—in other words, where a warrant authorizes the indiscriminate search of multiple people, places, or things without limitation—our courts suppress the entire fruits of the warrant as violations of our constitutional protections against unreasonable searches and seizures. *See, e.g.*, *Marshall*, 199 N.J. at 618 (finding a warrant deficient in its entirety when

it lacked particularity); *Sims*, 75 N.J. at 351 (reversing the convictions of two individuals arrested and charged with gambling because they were found via an unconstitutional general warrant).

II. An officer's generic "training and experience," without additional explanation, cannot be allowed to justify a phone search.

Phones are pervasive features of daily life. *Riley*, 573 U.S. at 385. Wherever there are people, there are cell phones. It is only natural, then, that police officers will encounter cell phones, even if just incidentally, in virtually every police investigation they undertake. But this alone does not constitute probable cause to believe that the phone will actually contain evidence of the crime. Placing undue weight on an officer's generic "training and experience" to show probable cause for a phone search, especially without explication in the affidavit, would erode our Article I, Paragraph 7 and Fourth Amendment protections by granting police access to our innermost lives for generic reasons that will apply for virtually any crime and in any case.

As Ms. Tyner notes, the affidavit of probable cause offered no factual statements sharing any nexus with her cell phone. For example, the supporting affidavit recounts in cursory fashion how cars are equipped with "event data recorders" ("EDRs"), but fails to include information on what the EDR in *this* case revealed or how that leads to a "fair probability that contraband or

evidence of a crime" will be found on Ms. Tyner's phone. *State v. Moore*, 181 N.J. 40, 46 (2004) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). Likewise, while the affidavit recounts how a child in the car was improperly restrained in their car seat, that fact has no nexus to the State's theory that cellular phone usage while driving caused distracted driving. And perhaps most egregiously, the affiant supplied an incomplete version of a key witness statement that would have tended to show that the incident may not have been caused by a cell phone, but rather because Ms. Tyner was distracted by a child in her car. Such an omission, had it been included, may have "militated against issuance of the search warrant." *State v. Sheehan*, 217 N.J. Super. 20, 25 (App. Div. 1987).

But of particular concern is the State's overreliance and the court's improper crediting of the officer's "experience and training" to support the search of a cell phone. Amicus does not dispute that "in some situations a police officer may have particular training or experience that would enable him to infer criminal activity in circumstances where an ordinary observer would not." *State v. Demeter*, 124 N.J. 374, 382 (1991). But in those cases, "when an officer's experience and expertise is relevant to the probable cause determination, the officer must be able to explain sufficiently the basis of that opinion, so that it 'can be understood by the average reasonably prudent

person.'" *Id.* (quoting 4 Wayne R. LaFave, *Search and Seizure*, § 3.2(c) (2d ed. 1987)).

Here, the lower court gave substantial credit to the affiant's training and experience in its probable cause determination. But despite the limited leeway that officers are entitled to, *State v. Kasabucki*, 52 N.J. 110, 117 (1968), the absence of any hint of logic or explanation connecting the fact of the accident to Ms. Tyner's cell phone is simply too glaring to ignore. As courts have found in similar situations, an affiant's "training and experience" cannot substitute for particularized facts, contained within the affidavit's four corners, that actually provide the connective tissue between the crime alleged and the cell phone to be searched. For example, in a robbery and capital murder investigation in Texas, the state's highest court for criminal appeals found that an officer's generic knowledge of cell phones drawn from boilerplate "training and experience" cannot constitute probable cause without case-specific facts connecting the device to the alleged offense. *See State v. Baldwin*, 664 S.W.3d 122, 134-35 (Tex. Crim. App. 2022) (Officer's reliance on his "training and experience" that co-conspirators in a robbery were likely to use their cell phones around the time of the crime was insufficient to support probable cause for the issuance of a warrant to search a phone).

Similarly, the affidavit here did not use case-specific facts to connect the officer's "training and experience" to a particularized rationale for the phone search. Even if we grant that Ms. Tyner may have been distracted, there is not a hint of a rationale for what Detective Carrington's experience teaches him about how prevalent phones are in distracted driving cases or what sort of data on the phone would constitute evidence of distracted driving.

The bare-bones recitation of the affiant's experience cannot be credited where there is no connection between that experience and the actual facts. Exposing this data to law enforcement, simply because a single law enforcement officer thinks that it's the right thing to do in an investigation with zero explanation, would undermine the entire reason for requiring warrants to search cell phones. *See Riley*, 573 U.S. at 403. Such indiscriminate deference would necessarily lead to no effective limitations on cell phone searches and the concomitant gross invasion of privacy.

III. Mobile device forensic tools allow law enforcement to conduct limited phone searches with greater particularity.

Finally, the State's contention that it requires a broad phone search fails as a simple matter of fact. Despite the State's suggestions otherwise, law enforcement operates from a position of strength, not weakness, when it comes to conducting cell phone searches. "Mobile device forensic tools" ("MDFTs") can glean a wealth of information from phones, including valuable metadata

that normally would not be available to the average phone user, without exposing irrelevant, private data to human forensic analysts. Had the probable cause affidavit represented the true power of MDFTs and how they work, it would have been plain that there was no patent technical need for an "any and all" data warrant.

First, the State conflates the "data acquisition" or "extraction" stage of phone analysis, where forensic analysts download a partial or complete copy of the phone's contents for preservation and data integrity reasons, with the "data reduction" phase, where a human forensic analyst analyzes the copy of the phone's contents to filter and narrow the data down to what is responsive.[3] *State v. Mansor*, 421 P.3d 323, 332-33 (Or. 2018). A complete download of the phone's contents may be required in some (but not necessarily all) cases to locate deleted files or access certain kinds of system data. Logan Koepke et al., Upturn, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* 21-22 (2020)[4]. But the latter "data reduction step," in which private data are exposed to investigators, does not require analysts to *query* for or *view* every file beyond the goal of their investigation (e.g., data within a specified time range, data pertaining to a certain application, etc.).

[3] *See, e.g.*, DCa11 ("Therefore, in order to view the data in a readable format the device in its entirety must be opened and downloaded.").
[4] Amicus includes this report in its attached appendix.

This is where the rubber meets the road for how warrants must apply for forensic phone searches: the probable cause and particularity specified in the warrant must limit the discretion of the human analyst to only aim their queries and analysis towards responsive data (*see* Point I).

Second, MDFTs are built to recognize the structure of a variety of phone operating systems and organize the data contained within their file systems into searchable categories for the human analyst, saving the human analyst from having to piece much of the information together themselves. *See, e.g.*, *Smith*, 278 A.3d at 501 n.14 ("Cellebrite software was used to extract data from the defendant's cell phone and categorized it into separate 'container file[s]' by placing, for example, text messages into a text messages folder and call logs into a call logs folder. Once the data is categorized, the police can then search the files to 'see what's on the phone.'"). MDFTs also surface databases usually hidden to the user, including information on when the user interacts with their phone. *See* Koepke et al., *supra*, at 22.

The hidden metadata within a phone is a "digital forensics goldmine" while also constituting a very limited subset of phone data. *Id.* In a distracted driving case, where the State's theory is that a defendant interacted with their phone and caused an accident, this metadata may in fact be one of the only sources of data it needs.

In this case, the State appears intent on relying on precisely this sort of data, which it could have predicted would be central to their investigation before seeking the warrant. (SMa2). It should have shared that knowledge in its warrant application so that the court might have better understood the target of the search and whether the warrant's scope was actually necessary. The State's ongoing failure to adequately explain its tools creates an unnecessary mystique around the "complexity" of cell phone searches that stands in the way of our Article I, Paragraph 7 and Fourth Amendment rights.

CONCLUSION

For the above reasons, amicus ACLU-NJ urges the Court to order complete suppression of the search of "any and all" data on Ms. Tyner's phone.

Respectfully Submitted,

Dillon Reisman (374142021)
Brian Lozano (510002025)
Ezra D. Rosenberg (012671974)
American Civil Liberties Union
of New Jersey Foundation
[redacted]
P.O. Box 32159
Newark, New Jersey 07102
(973) 854-1718
dreisman@aclu-nj.org

Counsel for amicus curiae