FILED, Clerk of the Supreme Court, 19 Nov 2025, **091229**, **AMENDED**

Supreme Court of New Jersey
DOCKET NO. 091229

STATE OF NEW JERSEY,	:	CRIMINAL ACTION
Plaintiff-Movant,	:	On Motion for Leave to Appeal from an Interlocutory Order of the Superior Court of New Jersey, Appellate Division.
v.	:	
ZAK A. MISSAK,	:	Sat Below: Hon. Jessica R. Mayer, P.J.A.D.,
Defendant-Respondent.	:	Hon. Lisa Rose, J.A.D., Hon. Patrick DeAlmeida, J.A.D.

BRIEF ON BEHALF OF THE STATE OF NEW JERSEY

MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY
ATTORNEY FOR PLAINTIFF-MOVANT
RICHARD J. HUGHES JUSTICE COMPLEX
TRENTON, NEW JERSEY 08625

JEREMY M. FEIGENBAUM - Solicitor General (No. 117762014)
TIM SHEEHAN - Assistant Attorney General (No. 179892016)
LIZA B. FLEMING - Deputy Attorney General (No. 441912023)

WILLIAM P. COOPER-DAUB - Deputy Attorney General (No. 305072019)
Division of Criminal Justice, Appellate Bureau
P.O. Box 086
Trenton, New Jersey 08625
(609) 376-2400
cooperdaubw@njdcj.org

OF COUNSEL AND ON THE PETITION

October 8, 2025

TABLE OF CONTENTS

TABLE TO APPENDIX

TABLE TO APPENDIX CONTINUED

TABLE TO CONFIDENTIAL APPENDIX

[1] This document was included in an appendix submitted to the Appellate Division on October 18, 2024.

TABLE OF AUTHORITIES

PAGE

CASES

STATUTES

OTHER AUTHORITIES

RULES

TABLE OF CITATIONS

Ma - State's motion appendix, accompanying this brief
1T - Motion transcript, July 21, 2022
2T - Motion transcript, Feb. 21, 2024

PRELIMINARY STATEMENT

Police arrested defendant in 2021, and a State Grand Jury later indicted him for attempting to arrange a sexual liaison with a person he believed to be a fourteen-year-old girl. But the Appellate Division has twice stymied the State's efforts to recover evidence from defendant's cellphone. Diverging from settled precedent on the proper scope of search warrants, the Appellate Division—first in State v. Missak, 476 N.J. Super. 302 (App. Div. 2023) (Missak I), and again in the decision below—found a lack of probable cause to search anywhere on defendant's cellphone other than three specific applications defendant had used when messaging an undercover agent and for any time period outside the two days during which those messages occurred, effectively preventing the State from searching for any purpose other than confirming evidence the State already has. Its opinions are now impacting investigations across the state, as judges, prosecutors, and law enforcement struggle to reconcile the Appellate Division's novel standard with the realities of investigation and digital forensics. Leave to appeal is needed because the Appellate Division's decision diverges from settled precedent and will cause irreparable harm in this case and in others.

First, the Appellate Division's new test for probable cause for a cellphone search implicates a divide among state and federal courts; flouts longstanding precedent on search warrants; and is unworkable. The panel assumed, without

clear legal support, that even when there is probable cause that a phone contains evidence, the State must show distinct probable cause for each type of data that it seeks and each specific sub-location within the phone where it will be found. As a result, the panel limited any search to seeking that very specific evidence in those very specific places—contrary to longstanding precedent authorizing, on a showing of probable cause, a broader search for evidence of a crime in any location under a suspect's control where relevant evidence may be concealed. Requiring the State to establish precisely what it will find and where it will do so presents investigators with the impossible task of predicting the evidence and its locations, and conflicts as well with the realities of digital forensics and effective data extraction and preservation practices.

Second, if left to stand, Missak I and the Appellate Division's erroneous decision will cause the State irreparable harm for which it will have no recourse. Compliance with the panel's ruling will limit the State to applying for a warrant to confirm evidence it already has. And if the State proceeds to trial based only on evidence it already has and defendant is acquitted, double-jeopardy principles will preclude the State from ever seeking review from this Court of the panel's decision on this warrant. And the Missak decisions are causing irreparable harm in other cases too, as prosecutors and judges in this State struggle to apply their reasoning. This Court should grant leave to appeal.

STATEMENT OF FACTS AND PROCEDURAL HISTORY[2]

A. The Underlying Allegations.

On December 8, 2021, Homeland Security Investigations Special Agent Laura Hurley was undercover online, posing as a fourteen-year-old girl. (Ca10-12). She received an unsolicited message on Skout[3] from user "Mark William," saying, "Hey gorgeous I would love to be your sugar daddy and spoil you." (Ca12). "Mark" got Hurley's phone number and later sent text messages, again saying, "Hey gorgeous," and then, "I'm trynna get my dick sucked wya." Ibid. Hurley wrote that she was fourteen years old, and "Mark" responded with three messages: "[redacted]"; "[redacted]"; and "[redacted]" Ibid. That same evening, Hurley got an unsolicited message on Kik[4] from user "kazeblack," saying, "Hey sexy" and "What's up beautiful it's mark." Ibid. "Mark" asked for photos of the girl and sent a photo of a shirtless male. Ibid.

The next day, "Mark" arranged to meet the purported fourteen-year-old for sexual activity at 8:30 p.m. at a Franklin Township apartment complex,

---

[2] The statement of facts and procedural history are closely related and are presented together for the Court's convenience.

[3] Skout is a mobile application that allows users to locate, view profiles of, and chat with people near their geographical location. (Ca11).

[4] Kik is a mobile application that allows users to have private chats with each other, including sending pictures or videos. (Ca11).

where he believed she lived. (Ma5). At 8:11 p.m., defendant Zak Missak arrived at the complex. (Ca12). At the same time, "kazeblack" sent Hurley a Kik message reading, "I think I'm here what apartment are you in?" (Ma5). Two minutes later, he sent messages saying, "There's a park in the back" and "Meet me there." Ibid. At 8:15 p.m., members of the New Jersey Internet Crimes Against Children Task Force found defendant in the complex's rear parking lot, saw that he appeared to match the photo sent by "kazeblack," and arrested him. (Ma5; Ca12). Pursuant to a search incident to arrest, task-force members seized an Apple iPhone 12 Pro Max from defendant's person. (Ca4).

B. Initial Search Warrant and Decision.

On December 10, 2021, a complaint-warrant issued charging defendant with second-degree luring, N.J.S.A. 2C:13-6(a), and second-degree attempted sexual assault, N.J.S.A. 2C:14-2(c)(4) and 2C:5-1(a)(1). (Ma1-7). That day, the State applied for a search warrant/communications-data warrant to search the iPhone for evidence of luring and attempted sexual assault. (Ca1-6). The certification stressed the importance of having computer systems searched by a proficient examiner in a controlled environment to avoid inadvertently altering or destroying evidence. (Ca5-6). It explained the examiner must have access to search any part of the phone for, among other reasons, obtaining proof of who used or controlled the device and locating any concealed evidence. (Ca4-5).

The Honorable Michael J. Rogers, J.S.C., found probable cause and issued a warrant later the same day. (Ca7-8).

Upon arrest, defendant had told investigators the iPhone's passcode was "303030," but that passcode did not unlock the phone. (Ma61). On April 8, 2022, the State moved to compel defendant to provide the iPhone passcode to enable the warranted search. (Ma8). On June 24, 2022, defendant cross-moved to quash the warrant. (Ma9-10). On August 8, 2022, the Honorable Peter J. Tober, P.J. Cr., granted the motion to compel the passcode and denied the cross-motion to quash. (Ma11-29). Defendant appealed.

On May 25, 2023, the Appellate Division issued an unpublished opinion reversing Judge Tober's ruling. (Ma30-56). The court agreed that there was "probable cause to believe the phone found in defendant's possession contained some evidence of the crimes charged." (Ma51). Despite this, the panel held the warrant should be quashed because it authorized "searches of information and data within the phone for which [the] certification does not adequately establish probable cause." (Ma55). It found no probable cause to access information predating December 8, 2021—i.e., when the communications the State already possessed had begun. (Ma52-54). The court permitted the State to seek a new warrant but directed that any future warrant application should "allow the court to determine the locations within the data and information on the cellular phone

there is probable cause to believe relevant information concerning the crimes charged may be found." (Ma56). The court advised that a "certification should present facts enabling the court to determine the precise data for which probable cause has been established." (Ma52-53 n.7).

An amicus requested that the opinion be published. On August 4, 2023, after the period to seek certification had run and with approval of the Committee on Publications, the court reissued the decision as a published opinion. State v. Missak, 476 N.J. Super. 302 (App. Div. 2023) (Missak I); (Ma57).

C. Second Search Warrant and Decision.

The State applied again for a warrant to search the iPhone. (Ca9-16). The revised certification explained that full access to the phone was needed because (1) related data is generally dispersed throughout the device and appears in various locations; (2) data can be intentionally concealed by a user; (3) data deleted by the user may exist on the device and be recovered through forensic examination but may no longer have metadata reflecting associated dates; (4) navigating files, determining relevant dates, and properly opening files requires access to other data which may have widely ranging dates; (5) available date-and-time information varies among applications; (6) relevant evidence may not be severable from non-relevant information, such as logs of messages stored as one large database; and (7) date-and-time information related to certain data may

be altered by the user or the application. (Ca12-13). The certification outlined that relevant evidence includes data and information reflecting who used and controlled the device. (Ca13-14). It highlighted that a full forensic extraction is crucial to preserving the iPhone's memory as it exists at the time of examination so that it is available if some other challenge, such as software configuration or malware infection, is later raised as a defense. (Ca14). The certification also noted the increasing prevalence of methods for a user to hide items on a phone. (Ca14-15). The certification provided that, if evidence of another crime was discovered during the search, the search would stop until an amended warrant was obtained. (Ca15). The Honorable Julie M. Marino, J.S.C., issued a new search warrant on September 12, 2023. (Ca17-19).

On October 11, 2023, the State moved to compel defendant to produce his passcode. (Ma58-62). The next day, a State Grand Jury returned Indictment Number 23-10-00141-S, indicting defendant for second-degree luring, N.J.S.A. 2C:13-6(a), second-degree attempted sexual assault, N.J.S.A. 2C:14-2(c)(4) and 2C:5-1(a)(3), and third-degree attempted impairing or debauching the morals of a child, N.J.S.A. 2C:24-4(a)(1) and 2C:5-1(a)(1). (Ma63-67).

On November 3, 2023, defendant filed a cross-motion to quash the second warrant and to stay the order compelling passcode production. (Ma68-69). On March 5, 2024, Judge Tober issued a decision denying the State's motion and

granting the cross-motion to quash the warrant and stay the order for passcode production. (Ma70-84). The judge held that the revised certification failed to justify searching the cellphone because it failed to establish probable cause "'to believe relevant information concerning the crimes charged may be found' in places on the phone 'that either predate[] defendant's alleged commission of the crimes' or relates to his use of the phone after the crimes were committed." (Ma78). Judge Tober found the certification "failed to identify any precise data for which probable cause has been established." (Ma78).

The court rejected each justification for a full search of the phone. First, the judge held that the certification did not did not identify "precise data" that would reveal defendant's intent or where on the phone such data would be found. (Ma79). Second, he identified no factual basis to believe defendant was "guilty" of manipulating, hiding, or deleting pertinent data. (Ma79-80). Third, while the judge acknowledged evidence on the phone such as photographs of defendant or his family would be relevant to establishing ownership and control, he required more to show "that the massive amount of other data that would be accessed in a full search is connected in any way to the alleged criminality." (Ma80). Fourth, he treated the fact that data is often stored in separate locations as too hypothetical to establish probable cause to search the entire phone. (Ma91).

The Appellate Division granted the State leave to appeal. (Ma85-86). On

September 3, 2025, the Appellate Division issued an unpublished opinion affirming. State v. Missak, No. A-2062-23 (App. Div. Sept. 3, 2025) (slip op.) (Missak II) (Ma87-116). The opinion built off of Missak I. (Ma91-106). The panel concluded the revised warrant certification "did not cure the deficiencies we found were sufficient to invalidate the first warrant." (Ma113). It found no probable cause that there would be relevant evidence on the phone "outside the two-day period the State alleges [defendant] engaged in criminal activity" or for any "information and data generated by applications the State does not allege defendant used in the commission of his crimes." (Ma113-14). While finding "no reason to doubt" that data can be hidden or deleted, the court found no facts showing defendant had done so. (Ma114). It held that any search beyond those limits "would effectively be a search for uncharged criminality not identified in the search warrant." (Ma115). This motion followed. (Ma117-24).

QUESTION PRESENTED

In seeking a warrant to search a cellphone in the investigation of a crime, whether it is enough that the State established a fair probability that the phone contains evidence relevant to the investigated crime, or whether the State instead must establish specific probable cause for every single type of digital evidence it expects to find on a cellphone and for every single sub-location in a cellphone where it expects to find relevant evidence.

ARGUMENT

POINT I

THIS COURT'S REVIEW IS WARRANTED SINCE THE DECISION BELOW IMPLICATES A DIVIDE AMONG COURTS, IS INCORRECT, AND IS TECHNICALLY UNWORKABLE WITH IMPACTS ON A SIGNIFICANT NUMBER OF CASES.

This Court should grant leave to appeal to correct the Appellate Division's imposition of new legal burdens before the State can establish probable cause to search a cellphone pursuant to a warrant. While that court acknowledged that there is probable cause to believe defendant's iPhone holds criminal evidence, it relied on a novel construction of probable cause requiring specific probable cause for each type of evidence sought and each sub-location on the phone to be searched. This legal rule implicates a growing divide among state and federal appellate courts on an important and recurring issue. This legal rule is wrong, diverging sharply from longstanding principles guiding the scope of warrants—including those for home searches. Finally, the test is unworkable, requiring near-perfect foresight on the part of investigators to obtain a warrant, virtually guaranteeing relevant evidence will be missed, and creating profound practical difficulties for forensic examination and preservation.

To understand the rule the panel adopted, and the problems necessitating further review, some background is helpful. The Fourth Amendment to the U.S.

Constitution and Article I, paragraph 7 of our Constitution of course require that search warrants (1) be supported by probable cause and (2) contain a particular description of the place to be searched and the things to be seized. See State v. Andrews, 243 N.J. 447, 464 (2020); State v. Marshall, 199 N.J. 602, 610 (2009). Because "[a] search warrant is presumed to be valid," the "defendant bears the burden of demonstrating that the warrant was issued without probable cause," State v. Evers, 175 N.J. 355, 381 (2003), and the reviewing court must "accord substantial deference to the discretionary determination resulting in the issuance of the search warrant," State v. Boone, 232 N.J. 417, 427 (2017). Probable cause rests on the "totality of the circumstances" established in the four corners of the affidavit, as well as recorded sworn testimony, if any, before the judge. Ibid. Despite constantly evolving technologies, affidavits should be "examined in a common-sense and not a hypertechnical manner." Evers, 175 N.J. at 385.

"[T]he scope of a lawful search is 'defined by the object of the search and the places in which there is probable cause to believe that it may be found.'" Maryland v. Garrison, 480 U.S. 79, 84 (1987) (quoting United States v. Ross, 456 U.S. 798, 824 (1982)). "A lawful search of fixed premises generally extends to the entire area in which the object of the search may be found and is not limited by the possibility that separate acts of entry or opening may be required to complete the search." Ross, 456 U.S. at 820-21; see also State v. Reldan, 100

N.J. 187, 195 (1985). "[A] warrant that authorizes an officer to search a home for illegal weapons also provides authority to open closets, chests, drawers, and containers in which the weapon might be found." Ross, 456 U.S. at 821.

This Court should grant review to determine how these principles govern a search warrant for a cellphone for at least three reasons.

1. For one, courts across the country have demonstrated confusion as to the warrant requirements in this context—and they have divided on the question. Many state courts and federal courts of appeals have rejected attempts to demand that cellphone searches be tied only to specific forms of digital evidence or sub-locations within the phone, thus diverging from the decision of the Appellate Division here. See, e.g., United States v. Tompkins, 118 F.4th 280, 287-91 (2d Cir. 2024); United States v. Bishop, 910 F.3d 335, 336-38 (7th Cir. 2018); United States v. Bass, 785 F.3d 1043, 1048-50 (6th Cir. 2015); State v. Goynes, 927 N.W.2d 346, 354-57 (Neb. 2019); Commonwealth v. Green, 265 A.3d 541, 552-55 (Pa. 2021); Planck v. State, 264 N.E.3d 718, 2025 WL 1779552, at *6-7 (Ind. Ct. App. July 27, 2025) (Ma130-31); People v. English, 32 N.Y.S.3d 837, 840 (N.Y. Sup. Ct. 2016). Meanwhile, courts in other States have narrowed the scope of warranted phone searches, although many rested on particularity, distinguishing them from the decision below. See, e.g., People v. Carson, __ N.W.3d __, 2025 WL 2177501, at *9-11 (Mich. July 31, 2025); Terreros v. State,

312 A.3d 651, 666-69 (Del. 2024); State v. Wilson, 884 S.E.2d 298, 300-01 (Ga. 2023). The final word on the governing standards for such warrants in New Jersey should therefore come from this Court.

2. For another, this Court's review is needed because the decision below announced the wrong legal standard—on this tremendously important, recurring issue. The panel declared that a warrant must show distinct probable cause for each item of evidence sought, and concluded that the State did not establish that evidence would be found on the iPhone in locations other than the messaging applications defendant used during the crime and in data generated outside the two-day period when defendant messaged Agent Hurley. (Ma113-14). Instead, the question is whether there is "a fair probability that contraband or evidence of a crime will be found in a particular place," State v. Chippero, 201 N.J. 14, 28 (2009)—here, the cellphone—and not whether specific probable cause exists for each type of digital evidence and each type of sub-location. Compare Missak I, 476 N.J. Super. at 320, 323; (Ma113-14).

As a general matter, the rule has long been that probable cause to believe a location holds criminal evidence sweeps in any parts of that location over which a suspect exercises control and where evidence could be concealed. See, e.g., Ross, 456 U.S. at 820; Reldan, 100 N.J. at 195; State v. Sheppard, 46 N.J. 526, 529-30 (1966). In Sheppard, this Court reversed an order suppressing a

warrant authorizing a search of all areas of an apartment building under the immediate control of the suspect superintendent even though the only place police had seen him retrieve contraband was the apartment where he resided. 46 N.J. at 529. The Court added that, "[w]hen law enforcement officials learn that an individual is engaged in criminal activity in one part of a building, it is reasonable for them to assume that similar activity may be uncovered in other areas of the building over which that individual has control." Id. at 529-30. So too in a traditional home search, where investigators are looking for the weapon, or contraband, or other evidence of the crime: the warrant need only establish that evidence is likely in the home, not whether in the bedroom or living room.

That principle applies equally to digital searches, including of cellphones. Like the search of an apartment, there is often no way for officers to know all the places on a defendant's phone that particular evidence might be stored. See, e.g., Tompkins, 118 F.4th at 289 (computer searches "may sometimes need to be as broad as searches of residences pursuant to warrants"); United States v. Cobb, 970 F.3d 319, 329 (4th Cir. 2020) (upholding warrant to search entire computer because police "could not foretell the murder evidence that was located on the computer or the location of that evidence within the contents of the computer"); Bishop, 910 F.3d at 336-38 (upholding search of entire phone, reasoning search may include "everywhere" that "contraband may be hidden");

Bass, 785 F.3d at 1049-50 (upholding warrant to search cellphone because "officers could not have known where this information was located in the phone or in what format"); United States v. Meek, 366 F.3d 705, 716 (9th Cir. 2004) ("The prohibition of general searches is not to be confused with a demand for precise ex ante knowledge of the location and content of evidence related to the suspected violation."). That is logical: "as with filing cabinets, the incriminating evidence may be in any file or folder." Bishop, 910 F.3d at 337.

Indeed, cellphones present an even greater likelihood than physical spaces that relevant evidence will be found in various locations throughout the device, as digital files "are not maintained, like files in a file cabinet, in discrete physical locations separate and distinct from other files," and are instead "'fragmented' on a storage device, potentially across physical locations." United States v. Ganias, 824 F.3d 199, 213 (2d Cir. 2016); see also United States v. Richards, 659 F.3d 527, 538 (6th Cir. 2011) (holding warrant to search computer server was not overbroad because law-enforcement officers could not know precisely how evidence would be stored). Cellphones may also store "unseen information about any given 'file'—not only metadata about when the file was created or who created it, but also prior versions or edits that may still exist 'in the document or associated temporary files on [the] disk'—further interspersing the data corresponding to that 'file' across the physical storage medium." Ganias,

824 F.3d at 213 (citation omitted) (alteration in original). The "features unique to digital media as a whole and to those relevant in a particular case—features that simply do not exist in the context of paper files" thus cut against demanding probable cause on a datum-by-datum or location-by-location basis. Ibid.

Moreover, as courts have found, "in the context of electronic devices such as computers and cell phones, 'criminals can—and often do—hide, mislabel, or manipulate files to conceal criminal activity [such that] a broad, expansive search of the [device] may be required.'" Bass, 785 F.3d at 1049-50 (brackets in original); see also United States v. Stabile, 633 F.3d 219, 239 (3d Cir. 2011) (finding decision to view contents of particular computer file "was objectively reasonable because criminals can easily alter file names and file extensions to conceal contraband"). Although the Appellate Division accepted that this could occur, it declined to find probable cause to search the entire phone because it found "no facts establishing defendant engaged in such manipulation or deletion of data." (Ma114). But courts have not required such a showing of manipulation before authorizing searches of places in which evidence could be hidden. See Bass, 785 F.3d at 1049-50; Stabile, 633 F.3d at 239. Were that required, "a warrant to search filing cabinets for evidence of drug activity" would often be restricted to "'file cabinets in the basement' or to file folders labeled 'Meth Lab' or 'Customers.'" United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir.

2009). Such limitations have never been our law.

And the limitations the Appellate Division imposed here were particularly egregious. The panel concluded that probable cause only existed to search for defendant's specific messages with Agent Hurley during the two-day period that the State already possessed—and declared that the State had not identified any other precise data or information to support a search for evidence beyond those messages. But probable cause has never been limited to evidence that is already known to the prosecution; it requires only a "fair probability that contraband or evidence of a crime will be found in a particular place.'" Marshall, 199 N.J. at 610. Indeed—as the State's certification made crystal clear, (Ca13-14)—other evidence on the phone beyond the messages to Agent Hurley would be relevant to proving the crime, including (among other things) as to defendant's intent to commit these crimes and as to his ownership and control of the phone. To take just one example, investigating law enforcement officers cannot know whether defendant will argue that (1) he did not in fact intend to engage in sexual conduct or (2) missed the message from the undercover stating she was fourteen. There is a fair probability the phone contains other evidence that could refute those defenses by showing a proclivity for pedophilia or ephebophilia, which could include messages (whether on the same or other messaging applications), photographs, internet activity, or deleted files. The State also bears the ultimate

burden of proving who was using this phone, and other evidence, in a range of other sub-locations, will reveal who controlled or had access to the phone.

The date range runs into all the same problems. The Appellate Division's refusal to permit a search of the cellphone for any content outside the two days in which defendant exchanged messages with Agent Hurley failed to account for the fact that digital files can be mislabeled or mis-timestamped so that a time-limited search does not recover all relevant evidence. See English, 32 N.Y.S.3d at 840 (refusing to limit scope of cellphone search to date and time of offense, as doing so would "give criminals the ability to evade law enforcement scrutiny by utilizing coded terms in their files or documents, or placing such documents in areas of the computer that would not normally contain such files/documents"). Moreover, it again ignores that the phone likely contains evidence of intent or bearing on potential defenses, which could include messages, photographs, internet activity, or deleted files beyond those two days. Although law enforcement did not yet have specific knowledge of those pieces of evidence, it had a "fair probability" that these pieces of evidence existed on the phone—the standard at the investigative stage.

And finally, while the Appellate Division acknowledged the State's need to prove who was using the phone, its decision permitting only a narrow search for evidence on the two days was error. A search beyond the two days in which

the conduct occurred is needed to assess whether any other individuals also had access to the cellphone, bearing on defendant's own culpability. E.g., Bass, 785 F.3d at 1048–50 (finding probable cause based on suspect's use of phone and approving search for evidence including "indicia of use, ownership, or possession"); Goynes, 927 N.W.2d at 354-57 (finding phone warrant supported by probable cause where affidavit explained that data "provides insight for criminal investigations on the motivation, method, and participants," "who owns or was using the cell phone," and "an individual's level of culpability and knowledge"). Sound investigation is not achieved by narrowly limiting warrants to searches for evidence confirming the initial theory of a case. In unreasonably limiting this search, the Appellate Division departed from well-settled principles of probable cause underpinning the scope of search warrants. And it prescribed a rule that will ultimately deprive the State and the courts of pertinent evidence, both inculpatory and exculpatory.

3. Finally, not only does the decision below err as a matter of law on an issue that has divided state appellate courts and is of tremendous importance, but the panel adopted a standard that is unworkable in practice—underscoring the importance of this Court's review. See Ganias, 824 F.3d at 213 (noting "in assessing the reasonableness, for Fourth Amendment purposes, of the search and seizure of digital evidence, we must be attuned to the technological features

unique to digital media as a whole and to those relevant in a particular case—features that simply do not exist in the context of paper files").

First, the digital nature of cellphones makes it difficult to define particular "places" because files are often "'fragmented' on a storage device, potentially across physical locations." Ibid. So it makes little sense to treat data stored on a cellphone, where bits are scattered to fill free space, as existing in a discrete physical location. (Ca12-13); Scientific Working Group on Digital Evidence, Considerations for Required Minimization of Digital Evidence Seizure, 2 (Aug. 5, 2024) (Considerations) (Ma137). Although particular sub-locations could appear as folders within a phone's file system, asking investigators to identify in advance specific file paths to be searched is unrealistic given how these vary depending on the operating system, particular user, applications used, and other variables. See Considerations at 4 (Ma139); Bass, 785 F.3d at 1050 ("At the time of the seizure, ... the officers could not have known where this information was located in the phone or in what format."); Burgess, 576 F.3d at 1093 ("It is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename or extension or to attempt to structure search methods—that process must remain dynamic."). Accessing or understanding a file located in one virtual folder may also require accessing data located in another file, and recovering deleted or concealed information will depend on the ability to search

broadly. (Ca13); Considerations at 2, 5 (Ma137, 140); see also United States v. King, 737 F. Supp. 3d 1020, 1031-32 (D. Nev. 2024) (examiner explaining that recovering erased data requires extracting the full contents of the phone).

That difficulty extends to date ranges. Even accepting that evidence in a certain case might be confined only to a narrow date range, attempting to limit a search to those dates poses its own obstacles. Date and time conventions vary among applications and can be unreliable for various reasons, including nested files, subsequent modification, or intentional manipulation. (Ca13); Considerations at 3-4 (Ma138-39). Deleted files, while potentially recoverable, may no longer have dates. (Ca15); Considerations at 4-5 (Ma139-40). And a number of messaging applications log messages in non-severable database files that may contain years of messages, meaning the whole file must be accessed just to locate one message from a concrete date. (Ca13).

Second, limiting a cellphone search to specific locations and date ranges is incompatible with forensic methods and impairs forensic examiners' effective preservation of evidence. For one, mobile data forensic tools (MDFTs) do not enable the requirements the Appellate Division imposed. MDFTs are tools, used by expert forensic examiners, to ensure digital evidence is securely preserved and to locate and recover relevant data. A full digital extraction of a phone by MDFT is the best practice for both evidence preservation and accuracy and is a

necessary prerequisite to attempts to recover deleted information. See (Ca14-15); Considerations at 2-6 (Ma137-41); Fed. R. Crim. P. 41(e)(2)(B) (assuming initial copying of digital evidence followed later by review). An MDFT can pull together data from different parts of the phone to help a forensic examiner locate and review, for example, photographs or messages from common applications.

But MDFTs are not magic wands enabling law enforcement officers to automatically sift evidence from innocuous information. Forensic examiners must confirm that MDFT results are accurate and discern when other evidence may be present, including any deleted or hidden files or data from less-common applications. (Ca15); Considerations at 3 (Ma138); see Burgess, 576 F.3d at 1094 ("[T]here may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders ....). Performing a proper forensic examination of a cellphone simply is not possible with the bright-line distinctions the lower courts have wrongly assumed. See Ganias, 824 F.3d at 213 (explaining digital files' "interspersion throughout a digital storage medium, moreover, may affect the degree to which it is feasible, in a case involving search pursuant to a warrant, to fully extract and segregate responsive data from non-responsive data"). The decisions below do not seriously grapple with these problems, but the burdens that they impose on investigators in the digital age further compel review.

POINT II

LEAVE TO APPEAL IS WARRANTED IN ORDER TO PREVENT IRREPARABLE HARM.

Not only did the Appellate Division gravely err in announcing a new legal test for cellphone search warrants that implicates a divide among federal courts and state appellate courts, conflicts with first principles, and is unworkable in practice, but this Court's immediate intervention is warranted. Leave to appeal is appropriate when "necessary to prevent irreparable injury," R. 2:2-2(1), which is "similar" to asking whether the appeal is "in the interest of justice," Brundage v. Est. of Carambio, 195 N.J. 575, 599 (2008). That standard can be satisfied in multiple ways, including if "there is the possibility of some grave damage or injustice resulting from the trial court's order." Ibid. Ultimately, the question is whether the "appeal has merit" and "justice calls" for review. Ibid.

First, leave to appeal is the State's only recourse to prevent irreparable harm from the Appellate Division's decision. Without granting review on this interlocutory posture, this Court will be unable to review the important questions this case presents. In its decision, the panel signaled that it would not approve a warrant unless restricted to the "limited confines" of confirming defendant's "connection to evidence already in the State's possession." (Ma115). So if the panel's decision stands without review, the State will be limited to applying for a warrant only to confirm evidence it has. And if the State proceeds to trial

based only on the evidence it has and defendant obtains an acquittal, double-jeopardy principles will preclude the State from "the chance to seek a ruling from a higher tribunal which it would have had under slightly different circumstances." State v. Sims, 65 N.J. 359, 373 (1974). That means the fundamental legal questions that this appeal presents can be reviewed only in an interlocutory posture. And because leave to appeal is the only vehicle to ensure this Court can provide guidance on the proper search-warrant standard for cellphones, that is a particularly compelling basis to grant this motion.

Second, the interests of justice also warrant immediate review because the Missak decisions are causing irreparable harm in other cases. Deputy attorneys general and assistant prosecutors around the State are reporting that, due to these rulings, many judges now feel bound to deny phone search warrants unless they include narrow restrictions as to either date range, or application or sub-location within the phone, or both. This has led to denial of some warrant applications and curtailment of others in attempts to comply with these newly narrowed rules, which will likely lead to the permanent loss of relevant evidence. The effect is particularly problematic in domestic-violence cases and those involving ongoing conduct, where precise dates and evidence may be impossible to perfectly define in advance. This Court's immediate attention is warranted.

Finally, at least one petition and one other motion for leave to appeal are

pending before this Court raising similar questions as to cellphone searches. See State v. Tarte, No. 091185 (Notice of Petition filed Sept. 8, 2025); State v. Bonora, App. Div. Docket No. A-1602-24 (paper motion filed Sept. 19, 2025). But this case offers a particularly strong candidate in which to take up these questions, because it arises from the case involving the Appellate Division's published opinion on the subject, and because it involves a recurring fact pattern—involving the use of a phone in furtherance of child sex-abuse offenses—that regularly requires cellphone searches.

CONCLUSION

This Court should grant leave to appeal. If this Court does grant leave, the State requests an opportunity to submit supplemental merits briefing due to the complexity of the subject matter.

Respectfully submitted,

MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY
ATTORNEY FOR PLAINTIFF-MOVANT

BY: /s/ *William P. Cooper-Daub*
William P. Cooper-Daub
Deputy Attorney General
cooperdaubw@njdcj.org

DATED: October 8, 2025