

STATE OF NEW JERSEY,

Plaintiff-Movant,

v.

ZAK A. MISSAK,

Defendant-Respondent.

SUPREME COURT OF NEW JERSEY

Criminal Action

Docket No.: 091229

On Motion for Leave to Appeal From:  
Interlocutory Order of the Superior Court  
of New Jersey, Appellate Division.

Sat Below:

Hon. Jessica R. Mayer, P.J.A.D.

Hon. Lisa Rose, J.A.D.

Hon. Patrick DeAlmeida, J.A.D.

---

**BRIEF OF DEFENDANT-RESPONDENT ZAK A. MISSAK IN  
OPPOSITION TO MOTION FOR LEAVE TO APPEAL**

---

**MANDELBAUM BARRETT PC**

3 Becker Farm Road

Roseland, New Jersey 07068

973-736-4600 (p)

973-325-7467 (f)

agimigliano@mbawfirm.com

*Attorneys for Defendant,*

*Zak A. Missak*

Of Counsel:

Andrew Gimigliano (016792012)

Damian Conforti (020632001)

On the Brief

Andrew Gimigliano (016792012)

Stacey E. Zyriek (023592011)

**TABLE OF CONTENTS**

PRELIMINARY STATEMENT.....1

STATEMENT OF FACTS .....2

    A. The Charges .....2

PROCEDURAL HISTORY .....4

    B. The First Search Warrant and Supporting Affidavit.....4

    C. Motion to Compel Passcode and Cross-Motion to Quash the First  
    Warrant.....5

    D. The Appellate Division Quashed the First Warrant.....5

    E. The Second Search Warrant and Supporting Affidavit .....7

    F. Motion In Aid of Litigant’s Rights and Cross-Motion to Quash the  
    Second Warrant and to Stay the Court’s Order Compelling Production of the  
    Phone’s Passcode .....9

    G. The Appellate Division Affirmed the Trial Court Order Quashing the  
    Second Warrant.....11

LEGAL ARGUMENT .....12

    I. Leave to Appeal Should Be Denied Because This Case Presents No  
    Grave Damage or Injustice Warranting Interlocutory Review .....12

    II. The Appellate Division Properly Held the Second Warrant is  
    Unconstitutional Because the State Did Not Establish Probable Cause to  
    Search the Entire Contents of the Phone.....14

CONCLUSION.....22

**TABLE OF AUTHORITIES**

<b>Cases</b>	<b>Page(s)</b>
<u>Brinegar v. United States</u> , 338 U.S. 160 (1949).....	17
<u>Brundage v. Estate of Carambio</u> , 195 N.J. 575 (2008) .....	12, 13
<u>Burns v. United States</u> , 235 A.3d 758 (D.C. Ct. App. 2020).....	18
<u>Carroll v. United States</u> , 267 U.S. 132 (1925).....	17
<u>Commonwealth v. Snow</u> , 160 N.E.3d 277 (Mass. 2021).....	19, 20, 21
<u>DiMarino v. Wishkin</u> , 195 N.J. Super. 390 (App. Div. 1984).....	13
<u>Riley v. California</u> , 573 U.S. 373 (2014).....	15, 19, 20
<u>Stanford v. Texas</u> , 379 U.S. 476 (1965).....	15
<u>State v. Andrews</u> , 243 N.J. 447 (2020) .....	15, 19
<u>State v. Boone</u> , 232 N.J. 417 (2017) .....	16
<u>State v. Carter</u> , 247 N.J. 488 (2021) .....	16
<u>State v. Feliciano</u> , 224 N.J. 351 (2016) .....	15
<u>State v. Johnston</u> , 257 N.J. Super. 178 (App. Div. 1992).....	16

<u>State v. Manning,</u> 240 N.J. 308 (2020) .....	16, 19
<u>State v. Mark,</u> 46 N.J. 262 (1966) .....	17
<u>State v. Missak,</u> 476 N.J. Super. 302 (App. Div. 2023) .....	<i>passim</i>
<u>State v. Missak,</u> No. A-2062-23 (App. Div. Sept. 3, 2025) .....	11, 13, 14
<u>State v. Muldowney,</u> 60 N.J. 594 (1972) .....	14
<u>State v. Smith,</u> 278 A.3d 481 (Conn. 2022) .....	20, 21
<u>State v. Wilson,</u> 884 S.E. 2d 298 (Ga. 2023) .....	18, 20
<u>United States v. Abboud,</u> 438 F.3d 554 (6th Cir. 2005) .....	20
<b>Constitutions</b>	
New Jersey Constitution .....	14, 15, 16
United States Constitution Fourth Amendment.....	<i>passim</i>
<b>Statutes</b>	
<u>N.J.S.A. 2C:5-1(a)(1)</u> .....	2, 3, 4
<u>N.J.S.A. 2C:5-1(a)(3)</u> .....	2
<u>N.J.S.A. 2C:13-6(a)</u> .....	2
<u>N.J.S.A. 2C:14-2(c)(4)</u> .....	2
<u>N.J.S.A. 2C:24-4(a)(1)</u> .....	2

## PRELIMINARY STATEMENT

This case has already been to the Appellate Division twice. Both times, the Appellate Division agreed with Defendant that the State's search warrant was unconstitutional. The first decision was issued in May 2023 and published in August 2023. The second opinion is unpublished and was issued in September 2025. This motion for leave to appeal is really a challenge to the opinion issued in 2023, not the current 2025 opinion that simply applied the earlier decision. The State's time to appeal the 2023 decision was in 2023, but it chose not to do so. The State should not be allowed to challenge that decision now, through a second appeal the State lost. Defendant is entitled to finality.

On the merits, the State disagrees with the Appellate Division's application of settled probable cause principles. The State's claim that the Appellate Division created a new legal test for cellphone searches is not true; the panel applied the long-established probable-cause standard to the search of digital devices. And the Appellate Division's rationale is consistent with other states around the nation that have considered cell phone searches. The State's position finds no similar support.

The offense conduct in this case allegedly occurred over thirty hours, via three messaging applications with an undercover State agent. So, the State has the communications, knows the dates and times of the communications, and knows the exact content of the communications. Yet, the State wants to search Defendant's

entire cell phone, with no temporal limitations and no limitations on the types of data searched. As the Appellate Division twice concluded, the State does not have probable cause for that broad search.

This motion is, at bottom, the State's attempt to revive an unconstitutional investigative method that would allow unfettered rummaging through cell phones without any judicial oversight. The Appellate Division has twice rejected the State's attempt to rely on a general warrant to search cell phones, and those decisions were correctly decided and consistent with the constitutional rules of search and seizure. The Court should deny leave to appeal.

## **STATEMENT OF FACTS**

### **A. The Charges**

Defendant was charged 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 N.J.S.A. 2C:5-1(a)(1). (Ma1-3).<sup>1</sup> On October 12, 2023, Defendant was indicted 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 N.J.S.A. 2C:5-1(a)(3), and third degree endangering the welfare of a child, N.J.S.A. 2C:24-4(a)(1) and N.J.S.A. 2C:5-1(a)(1). (Ma81-84).

The charges stem from an investigation conducted by Special Agent Laura Hurley ("Hurley") on December 8, 2021, and December 9, 2021. (Ma12 ¶ 8(a)).

---

<sup>1</sup> Ma1-3 refers to Movant's Appendix.

According to Hurley, she was operating undercover, posing as a 14-year-old female (the “Juvenile”). (Ma13 ¶ 8(b)).

On December 8, 2021, at approximately 2:06 p.m., Hurley alleges to have been using the mobile messaging application Skout, posing as the Juvenile. Ibid. Hurley alleges that she was contacted on Skout by an individual using the display name “Mark William,” who the State claims was Defendant. Hurley alleges that Mark William asked for her telephone number. Ibid.

The State alleges that, at approximately 2:55 p.m. on December 8, 2021, Hurley received a text message from the telephone number (732) 705-7395. Ibid. Hurley alleges that she asked the sender to identify himself, and the sender responded by identifying himself as “Mark.” Ibid. The State alleges that the conversation between Hurley and “Mark” became sexually explicit. Ibid. Hurley alleges that she told “Mark” that she was 14 years old and that he continued to chat with her in a sexually explicit manner. (Ma13 ¶ 8(c)).

On December 8, 2021, at approximately 7:17 p.m., the State alleges that Hurley received an unsolicited message on the mobile application Kik from username “Kazeblack.” Ibid. The State further alleges that “Kazeblack” was Defendant. Ibid.

On December 9, 2021, at approximately 8:11 p.m., Defendant reportedly arrived at Douglass Gardens in Franklin Park, New Jersey in a silver Toyota Prius

to meet the Juvenile. (Ma13 ¶ 8(d)). Members of the New Jersey Internet Crimes Against Children Task Force were at that location and arrested Defendant. Ibid. At the time of his arrest, Defendant was in possession of an Apple iPhone 12 Pro Max in a black Otterbox case (the “Phone”). (Ma13 ¶ 8(e)). The Phone was seized during Defendant’s arrest and was secured pending the approval of a search warrant. Ibid.

## PROCEDURAL HISTORY

### **B. The First Search Warrant and Supporting Affidavit**

The State applied for search warrants to search Defendant’s vehicle and the Phone. (Ma10 ¶ 1). The State’s applications relied on a certification made by Hurley, which stated that the warrants were sought to obtain evidence of the crimes of luring and attempted sexual assault (the “Specified Crimes”). (Ma13 ¶ 9).

Hurley certified that she had probable cause to believe the Phone contained evidence of the Specified Crimes. Ibid. Hurley supported her probable cause determination with a statement of facts that described the alleged communications with “Mark” and “Kazeblack” that were made expressly through text message, Skout, and Kik. (Ma13 ¶¶ 8(b)-8(c)).

The certification sought the “opportunity to access, search, forensically examine, and document all information contained within” the Phone. (Ma11 ¶ 4). The Certification further requested the “ability and opportunity to access all information contained within the [Phone].” Ibid. In other words, the State sought to

search the entire Phone without any temporal limitation and without any limitation to the specific applications and communications that the State alleges constitute evidence of the Specified Crimes. On December 10, 2021, a search warrant/communications data warrant (the “First Warrant”) was issued. (Ma8-9).

### **C. Motion to Compel Passcode and Cross-Motion to Quash the First Warrant**

The State moved to compel Defendant to provide the passcode to the Phone, and Defendant cross-moved to quash the First Warrant. State v. Missak, 476 N.J. Super. 302, 311 (App. Div. 2023). The trial court concluded that the First Warrant was presumptively valid and that Defendant did not overcome that presumption, concluding there was ample evidence in Hurley’s certification to find probable cause to search all information on the Phone. Ibid. “The court further determined the warrant was sufficiently particular because it authorized a search of the phone’s content and data, and Hurley’s certification supported that broad search.” Ibid. Finally, the trial court concluded that Defendant should be compelled to produce the passcode to the Phone. Ibid.

### **D. The Appellate Division Quashed the First Warrant**

Defendant moved for leave to appeal the trial court’s decision. Leave to appeal was granted, and this Court, in a published opinion, reversed the order and quashed the First Warrant. State v. Missak, 476 N.J. Super. 302, 312-23 (App. Div. 2023). (“Missak I”).

Defendant argued that the First Warrant was unconstitutional “because Hurley’s certification [did] not establish probable cause for a search of all the Phone’s contents, information, and data.” Id. at 317. Defendant further argued that the State obtained the First Warrant to search for evidence of the crimes of luring and attempted sexual assault that Defendant allegedly committed on December 8 and 9, 2021, but “the warrant’s authorization for the entirety of the phone’s contents is not supported by any facts establishing a reason to believe all the phone’s various contents, information, and data may include evidence of the crimes for which the warrant was sought.” Id. at 318. The State “sought to justify the request for the search of the phone’s entire contents by asserting individuals ‘may’ seek to alter computer files to disguise what they contain and ‘may’ thereby avoid the State’s recovery of information and data for which probable cause has otherwise been established.” Id. at 320-21.

The panel rejected the State’s argument, holding that the State’s “justification [fell] short of the constitutional mark . . . because establishing probable cause for a search requires more than a showing of what ‘may’ have occurred.” Id. at 321. The panel noted that Hurley’s certification was missing “any facts establishing probable cause of an examination of data and other information, whatever it might be, that either predates defendant’s alleged commission of the crimes or does not constitute

evidence of his use of the phone around the time the crimes were committed.” Id. at 321-22.

The Court quashed the First Warrant and remanded the case to the trial court. The panel noted that the State was free to seek a new search warrant based on available **facts** that establish probable cause to search the data that the State believes contains evidence of the Specified Crimes.

#### **E. The Second Search Warrant and Supporting Affidavit**

On remand, the State applied for another warrant to search the Phone. The State again relied on a certification made by Hurley, which sought to obtain evidence of the same Specified Crimes.” (Ma68 ¶ 2). Hurley’s certification contained the same factual allegations as her certification in support of the First Warrant. Hurley recounted the same factual allegations about communications with “Mark” and “Kazeblack” that were made only through text message, Skout, and Kik on December 8 and 9, 2021. (Ma70–71).

Despite a factual basis for the new warrant that is identical to the factual basis to obtain the First Warrant, and the Appellate Division’s published opinion that the State’s factual basis failed to establish probable cause to search all the data on the Phone, Hurley’s second certification, once again, sought authorization to conduct a **full** forensic examination of **all** the data on the Phone. (Ma68 ¶4).

The only difference between Hurley’s first certification and her second certification was additional hypotheticals to support the State’s request to search all of the data on the phone:

- a) Data that represents an email or message may not be stored contiguously, but, instead may be split into chunks and disbursed widely through the storage medium. Moreover, the system itself may change that positioning over time with or without the knowledge of the user of the device.
- b) Data may be intentionally concealed by the device’s owner. For instance, data that would normally be interpreted by the device as an image file may be altered by the user to appear as though it is a different type of data.
- c) Data may be deleted by the user, but may still exist on the device. . . .
- d) Relevant data may need other data to be interpreted. . . . data stored by an app may be stored in a proprietary format . . . . In such a case, an examiner may need to recover both the application data and the program data . . . .
- e) Date and time information is often application specific and may not allow a straightforward assessment of time. For example, a messaging application may or may not store date and time information associated with each of the messages it stores.
- f) Data may not be capable of separation from other data. For instance, a messaging application may store all of its messages in a proprietary database that it maintains on the device. In such a case, it may not be possible to extract only a portion of the database . . . .
- . . . .
- j) The way certain data appears on its face may not be accurate. For instance, users of computing devices may

seek to hide contraband by altering the device to exhibit unexpected behavior. For example, a device may not report all of the files that are stored on it or may misreport their types, allowing the user to conceal data.

[(Ma71 ¶ 11(a) – Ma73 ¶ 11(j))]

On September 12, 2023, a search warrant/communications data warrant (the “Second Warrant”) was issued. (Ma65-67). The Second Warrant authorized the search of the entire Phone, without any limitations, but it did not identify the items that may be seized pursuant to the search. (Ibid.).

**F. Motion In Aid of Litigant’s Rights and Cross-Motion to Quash the Second Warrant and to Stay the Court’s Order Compelling Production of the Phone’s Passcode**

The State filed a motion in aid of litigant’s rights to enforce the trial court’s order compelling Defendant to produce the passcode to the Phone. (Ma76-77). Defendant cross-moved to quash the Second Warrant and to stay the order compelling production of the passcode. (Ma88-89). On March 5, 2024, the trial court issued a written opinion and order denying the State’s motion to enforce litigant’s rights and granting Defendant’s cross-motion to quash the Second Warrant and granting Defendant’s motion to stay the trial court’s August 8, 2022, order compelling him to provide the passcode to the Phone. (Ma90-104).

The trial court held that the State lacked probable cause to support a search of the entire Phone. (Ma98). The trial court, following the holding of this Court in Missak I, noted that the State did not provide “information to allow the court to find

that “there is probable cause to believe relevant information concerning the crimes charged may be found” 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 to justify the full search the State is seeking.” Ibid. Furthermore, the trial court held that the State failed to identify any precise data for which probable cause has been established, as this Court required in Missak I. Ibid.

The court also found that Hurley failed to identify any precise data or information that would reveal evidence of Defendant’s intent and that Hurley was again relying on hypothetical scenarios that defendants generally may try to conceal or destroy evidence, which this Court held fell short of establishing probable cause. (Ma99-100). The court therefore found the Second Warrant to be overbroad because it sought access to the entire Phone and not just the applications related to the charged offenses. Ibid.

Accordingly, applying Missak I to the Second Warrant, the trial court found that “without any showing that the State has probable cause to search outside of the specific applications used by the Defendant to commit the charged crimes or outside of the relevant time period when the crimes were alleged to be committed,” a warrant to search the entirety of the Phone was unconstitutional. (Ma101).

### **G. The Appellate Division Affirmed the Trial Court Order Quashing the Second Warrant**

The State moved for leave to appeal the trial court's decision. Leave to appeal was granted, and the Appellate Division, in an unpublished opinion, affirmed the order and quashed the Second Warrant. State v. Missak, No. A-2062-23 (App. Div. Sept. 3, 2025) (slip op. at 11). (“Missak II”) (Ma106-35).

The State argued that Hurley's certification established probable cause that relevant data may be located anywhere in a cell phone, and thus, it “makes no sense to limit a search within the place to be searched.” (State Br. at 24). The State argued that it is impracticable in cases where a digital examination of a cell phone is sought to limit the examination to certain applications and time frames as data on cell phone “may not always correlate to a specific date range or type of file.” (Id. at 24-25).

Defendant argued that the Second Warrant was unconstitutional “because in support of its request to conducted an unlimited search of the phone, the State relies on hypotheticals relating to storage, manipulation, and deletion of information and data on cellular phones in general.” (Id. at 25). Therefore, according to Defendant, “Hurley identified no facts establishing a fair probability evidence related to the two crimes identified in the warrant would be found on his phone outside the information and data generated during the two-day period he is alleged to have committed those crimes or by applications the State does not allege he used to commit those crimes.” (Ibid.).

The Appellate Division concluded that Hurley’s second certification did not cure the deficiencies from the First Warrant. (Ma132). The court noted, “the State identified no facts establishing probable cause defendant engaged in criminal activity outside the two-day period or with applications other than those used to communicate with Hurley.” (Ibid.). It concluded that “absent probable cause to the contrary, a search of the information and data on defendant’s phone outside those limited confines would effectively be a search for uncharged criminality not identified in the search warrant.” (Ma133).

The court therefore quashed the Second Warrant and remanded the case to the trial court. (Ibid.). The panel declined to offer an “opinion with respect to the scope of an appropriate search warrant in this matter, should the State elect to make a third application to search defendant’s cellular phone.” (Ma134).

## **LEGAL ARGUMENT**

### **I. Leave to Appeal Should Be Denied Because This Case Presents No Grave Damage or Injustice Warranting Interlocutory Review**

The Supreme Court may grant interlocutory review when necessary to prevent irreparable harm. R. 2:2-2(1). “[T]he standards governing grants of interlocutory review are stringent” and “leave is sparingly granted.” Brundage v. Estate of Carambio, 195 N.J. 575, 607 (2008). A movant must show “that the desired appeal has merit and that ‘justice calls for [an appellate court’s] interference in the case.’” Id. at 599.

The standard does not call for the correction of “minor injustices,” but rather, there must exist the “possibility of ‘some grave damage or injustice’ resulting from the trial court’s order.” Ibid. Only an “exceptional case” warrants interlocutory review. DiMarino v. Wishkin, 195 N.J. Super. 390, 394-95 (App. Div. 1984).

Here the Court should decline to grant interlocutory review because the State has not shown that “grave damage or injustice” will result from the Appellate Division’s decision. The State claims that leave to appeal is warranted because the Appellate Division “announced a new legal test” for cellphone search warrants that is both unprecedented and unworkable. (State Br. at 1). That assertion is false. The Appellate Division applied the same probable cause analysis that has governed search warrants for decades to the search of Defendant’s cell phone. The law has not changed, and the decision was correct.

The Appellate Division also applied the law of the case (Missak I) to the Second Warrant (Missak II). Both times, the court addressed the same legal question and resolved it consistently, thus, leaving no conflict to resolve. What the State seeks now is an opportunity to litigate Missak I through the lens of Missak II.

When the Appellate Division issued Missak I, the State had undeniable notice of the decision it now claims is incorrect. If the State believed Missak I conflicted with precedent, it had the opportunity to request this Court’s review. It chose not to. A motion for leave to appeal now should not be permitted as a mechanism to evade

the consequences of failing to pursue timely review. Moreover, the State's efforts to reopen a decision it ignored two years ago would unfairly prejudice Defendant, who is entitled to finality and the benefit of the decision in Missak I.

At bottom, this motion for leave to appeal is an attempt by the State to resuscitate an unconstitutional investigative method so it can rummage through cell phones without any judicial oversight and without any concerns about the constitutional rights of the citizens of New Jersey. The State's position is that it can search all of the data on a cell phone by relying on generic probable cause supported by hypotheticals about what may or may not occur with cell phone data. But two panels of the Appellate Division already issued an interlocutory decision in this case rejecting the State's attempt to generate probable cause with hypotheticals. The State does not pose any new or novel questions that would warrant interlocutory review. The Court should reject the State's attempt to evade the well-reasoned holding in the Missak decisions and should deny the motion for leave to appeal.

**II. The Appellate Division Properly Held the Second Warrant is Unconstitutional Because the State Did Not Establish Probable Cause to Search the Entire Contents of the Phone**

The Fourth Amendment of the United States Constitution and Article I, Paragraph 7 of the New Jersey Constitution prohibit "general searches and unrestrained seizures by officers acting under the unbridled authority of a general warrant." State v. Muldowney, 60 N.J. 594, 600 (1972). The Fourth Amendment and

Article I, Paragraph 7 provide, in nearly identical language, that “no warrant shall issue except upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the papers and things to be seized.” N.J. Const. art. I, ¶ 7; State v. Andrews, 243 N.J. 447, 464 (2020) (stating the United States and New Jersey Constitutions require search warrants to “describe with particularity the places subject to search and people or things subject to seizure.”).

The “Fourth Amendment was the founding generation’s response to the reviled ‘general warrants’ and ‘writs of assistance’ of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.” Riley v. California, 573 U.S. 373, 403 (2014). “Opposition to such searches was in fact one of the driving forces behind the Revolution itself.” Ibid.

Indeed, “[v]ivid in the memory of the newly independent Americans were those general warrants known as writs of assistance under which officers of the Crown had so bedeviled the colonists.” State v. Feliciano, 224 N.J. 351, 366 (2016) (quoting Stanford v. Texas, 379 U.S. 476, 481 (1965)). “The hated writs of assistance had given customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws.” Ibid. “The warrant requirement is predicated upon the premise that the necessity and reasonableness of a search can best be determined by a neutral and detached magistrate instead of . . .

[a police] officer engaged in the often competitive enterprise of ferreting out crime.”  
State v. Johnston, 257 N.J. Super. 178, 188 (App. Div. 1992).

Further, and significantly, “[c]ompliance with the warrant requirement is not a mere formality but—as intended by the nation’s founders—an essential check on arbitrary government intrusions into the most private sanctums of people’s lives.” State v. Manning, 240 N.J. 308, 328 (2020). And, of course, it is critical to note that the “New Jersey Constitution ‘affords our citizens greater protection against unreasonable searches and seizures’ than the Fourth Amendment does.” State v. Carter, 247 N.J. 488, 529 (2021) (citing cases identifying greater protections under New Jersey Constitution, including “cell phone location data”; “internet subscriber information”; “bank records”; and “hotel-room telephone toll or billing records”).

Although a warrant is “presumptively valid,” a reviewing court should look at the totality of the circumstances to determine whether adequate facts support finding probable cause or whether the intended search “was otherwise unreasonable.” State v. Boone, 232 N.J. 417, 427 (2017).

Here, the Second Warrant suffers from the same constitutional flaw as the First Warrant; it is not supported by probable cause to search the entire contents of the Phone. Instead of presenting additional **facts** to establish probable cause to search the entire Phone, as the panel in Missak I suggested would be appropriate, the State relies on additional hypotheticals of what **may** be true to establish probable cause.

See Missak, 476 N.J. Super. at 323 (“The State is free to seek a new search warrant based on whatever facts are available to it that establish probable cause to believe the various information and data the State requests to search contain evidence pertaining to the criminal charges pending against defendant.”). Relying on what may have occurred is not sufficient for the State to carry its constitutional burden to establish probable cause. Ibid.

Probable cause means “more than bare suspicion.” Brinegar v. United States, 338 U.S. 160, 175 (1949). “Probable cause exists where ‘the facts and circumstances within their (the officers’) knowledge and of which they had reasonably trustworthy information (are) sufficient in themselves to warrant a man of reasonable caution in the belief that’ an offense has been or is being committed.” Id. at 175-76 (quoting Carroll v. United States, 267 U.S. 132, 162 (1925)). In short, probable cause requires “less than legal evidence necessary to convict though more than mere naked suspicion.” State v. Mark, 46 N.J. 262, 271 (1966). Put simply, “establishing probable cause for a search requires more than a showing of what ‘may’ have occurred.” Missak, 476 N.J. Super. at 321.

Here, Hurley’s certification in support of the Second Warrant contains the exact same facts that supported the First Warrant, that is, specific information about three communication threads allegedly between Defendant and an undercover officer that form the basis of the Specified Charges. Hurley identified the

applications used, the usernames, phone numbers, and times associated with the alleged communications. In other words, the State already has copies of and, therefore, knows the exact information and communications it is looking for to support the Specified Charges. Yet it seeks to search the entire Phone based solely on speculation about where data might be stored. That approach is constitutionally insufficient. See Burns v. United States, 235 A.3d 758, 767 (D.C. Ct. App. 2020) (holding that warrant was not supported by probable cause where law enforcement sought to review entire contents of cell phone “even though the warrants were supported by affidavits that established probable cause for only three narrow and discrete items of data”).

The State cannot rely on hypotheticals to manufacture generic probable cause that could apply to any criminal investigation. Missak, 476 N.J. Super. at 320-21; see also State v. Wilson, 884 S.E. 2d 298, 306 (Ga. 2023) (Pinson, J., concurring) (“As far as I can tell, that warrant allowed the search and seizure of the data from two cell phones on the theory that (1) they were found in the suspect’s van, and (2) criminals commonly use cell phones to talk about crimes. And the scope of the authorized search and seizure looks unlimited: police could search and seize the entire contents of the phones, with no apparent restrictions on the type or category of data or information that could be seized, or on how any of that data or information could be used. A warrant supported by such generic “probable cause” to search

someone’s house and seize the entirety of its contents, with no restrictions on their use, would never fly.”). Therefore, the State should obtain a warrant that seeks to search the specific apps and files, during the relevant time period, that it has probable cause to search. And the probable cause cannot rest on what may be true about cell phone data.

The State’s claim that it may search the entire Phone just as it could search an entire house is constitutionally unsound. Digital and physical searches are fundamentally different. As the Supreme Court explained, comparing the two is like comparing “a ride on horseback” to “a flight to the moon.” Riley v. California, 573 U.S. 373, 393 (2014). Because of that difference, the scope of any cell-phone search must be limited to areas where the sought evidence “might reasonably be found.” Commonwealth v. Snow, 160 N.E.3d 277, 285-86 (Mass. 2021).<sup>2</sup>

Cell phones contain not only vast quantities of data but information that is “qualitatively different” from anything found in a home, such as information related to medical conditions or “a wealth of detail about...familial, political, professional, religious, and sexual associations.” Riley, 573 U.S. at 395-96; see also State v.

---

<sup>2</sup> This is the approach followed by the trial court in Andrews, 243 N.J. at 464. In Andrews, the Supreme Court acknowledged that the trial court had heard arguments regarding the scope of the search warrants and had entered an order curtailing the State’s access to the contents of the phone. 243 N.J. at 460. The order limited the scope of the search to information contained within (1) the “Phone” icon and application, and (2) the “Messages” icon and/or text messaging applications used by the defendant with regard to the communications at issue. Ibid.

Manning, 240 N.J. 308, 316 (2020) (“Cell-phone records can reveal intimate details about people’s lives and relationships -- the persons and groups with whom they associate, the doctors they choose, the religious services they attend, the stores they patronize, the recreational places they visit, and much more.”). Moreover, cell phone apps “offer a range of tools for managing detailed information about all aspects of a person’s life.” Riley, 573 U.S. at 396 (noting existence of apps for political associations, addictions, religion, tracking pregnancy, and “for every conceivable hobby or pastime”). A cell phone search therefore “expose[s] to the government far more than the most exhaustive search of a house.” Ibid. In short, cell phone searches are not like physical searches, and current Fourth Amendment law accounts for that difference. See, e.g., Riley, 573 U.S. at 373-74; Commonwealth v. Snow, 160 N.E.3d 277, 288-89 (Mass. 2021); State v. Smith, 278 A.3d 481, 497 (Conn. 2022); Wilson, 884 S.E. 2d at 299-300.

In a final attempt to support its motion for leave to appeal, the State argues that a limited search of a cell phone is not feasible given how cell phones store information. (State Br. at 19-22). The State fails to offer any explanation how other law enforcement agencies throughout the country are able to conduct searches of cell phones based on constitutional limitations, but the New Jersey Attorney General’s Office cannot follow suit. See, e.g., United States v. Abboud, 438 F.3d 554, 576 (6th Cir. 2005) (holding warrant was not sufficiently particular because it

was not limited to time period for which magistrate had probable cause to believe fraud had occurred); Smith, 278 A.3d at 497 (holding warrant was not constitutionally particular where “it included no time parameters to cabin the scope of the search but, rather, allowed for the entire contents of the phone to be searched for all time.”). Snow, 160 N.E.3d at 288-89 (holding warrant was not sufficiently particular because it lacked any temporal limitations, noting “[t]he magnitude of the privacy invasion of a cell phone search utterly lacking in temporal limits cannot be overstated.”).

The well-worn constitutional principles governing search and seizure can be applied to digital searches in a manner to ensure that the State does not trample individual rights by rummaging unfettered through cell phone data. The lynchpin of those principles is probable cause. The State must establish it has probable cause to conduct any search, digital or physical, and to do that, the State must assert facts to demonstrate it will find evidence of the offense conduct. The State, however, cannot generally allege conduct or posit theories about why it may find evidence. That does not clear the probable cause hurdle.

The State is trying to make New Jersey a constitutional outlier by ginning up concerns about data. The State’s logic that hypotheticals establish probable cause not only would make New Jersey an outlier on cell phone searches but also would render Fourth Amendment protections for cell phones meaningless. The State could

produce a generic affidavit filled with the same hypotheticals to justify the search of any phone, no matter the charges or facts of the case. The Constitution forbids that approach.

### **CONCLUSION**

Leave to appeal is rarely granted and only in the most deserving cases. Here, the State's motion does not meet the standard for interlocutory review because the State's motion is a thinly veiled attempt to relitigate an issue already decided by two panels of the Appellate Division. This motion presents nothing new or novel that requires this Court's immediate supervision. Instead, the panel in Missak I issued a precedential opinion governing the Fourth Amendment issues in this case, and the panel in Missak II properly applied those principles. The State's motion for leave to appeal should be denied.

Respectfully submitted,  
**MANDELBAUM BARRETT PC**

Dated: December 1, 2025

By: /s/ Andrew Gimigliano  
Andrew Gimigliano