**OFFICE OF THE COUNTY PROSECUTOR**
**COUNTY OF MONMOUTH**

132 JERSEYVILLE AVENUE
FREEHOLD, NJ 07728-2374

**(732) 431-7160**

RAYMOND S. SANTIAGO
MONMOUTH COUNTY PROSECUTOR

May 28, 2025

The Honorable Marc C. LeMieux, A.J.S.C.
Monmouth County Courthouse
71 Monument Park
Freehold, New Jersey 07728

Re: State of New Jersey v. Paul Caneiro
Indictment No. 19-02-0283; Case No. 18004915
Motion To Suppress Evidence Seized With a Warrant
Returnable: June 3, 2025

Dear Judge LeMieux:

Please accept the following letter in response to the above-captioned motion, by way of which the defendant seeks suppression of evidence searched pursuant to judicially-authorized warrants. In keeping with the law governing such motions, see infra, the State will rely upon the facts contained within the four corners of the challenged[1] warrants, incorporating the same herein by reference.

[1] Defendant also appends to his brief numerous communications data warrants (CDWs), the issuance of which he does not challenge. In fact, defendant appears to suggest that the CDWs are all in full compliance with the law because, in contrast to the search warrants at issue, the CDWs contain date ranges for the requested records. For the reasons and authorities contained herein, the State contests that the use of date ranges is a legal requirement for the issuance of valid electronics warrants. Nonetheless, the State agrees that the CDWs are valid and lawful and the evidence seized pursuant thereto is not subject to suppression.

In Riley v. California, 573 U.S. 373, 403 (2014), the United States Supreme Court answered the "simple" question "of what police must do before searching a cell phone" as follows: "get a warrant." Prior to searching this defendant's electronics, law enforcement heeded this advice. They did exactly what the Framers of the U.S. Constitution – and the authors of the "nearly identical" provision of the New Jersey Constitution – intended. State v. Feliciano, 224 N.J. 351, 366 (2016).

Detectives Brian Weisbrot and Patrick Petruzziello presented the evidence then compiled by law enforcement to "a neutral and detached magistrate," the Honorable James J. McGann, J.S.C., and the Honorable Joseph W. Oxley, J.S.C., respectively, each of whom, relieved from the "competitive enterprise of ferreting out crime" that plagues law enforcement, reviewed the nearly identical evidence and drew from it "the usual inferences which reasonable men draw from evidence." Riley, 573 U.S. at 381-82; State v. Marshall, 199 N.J. 602, 612 (2009) (quoting Johnson v. United States, 333 U.S. 10, 13-14 (1948)); see also DaD, I. The reviews conducted by Judges McGann and Oxley resulted in the conclusion that the constitutionality-mandated requirements for the issuance of a search warrant – probable cause and particularity – were met.

Defendant asks this Court to come to the opposite conclusion. In support thereof, defendant relies upon a plethora of non-precedential, unpublished opinions, see R. 1:36-3, and similarly non-binding out-of-state cases (some of which are supported solely by news reports, see Db23-24), as well as one federal district court case, all of which he claims lend support to what he contends is the conclusion of State v. Missak, 476 N.J. Super. 302 (App. Div.

2023): that warrants authorizing the search of electronic devices are per se overbroad and illegally "general" unless they limit the search temporally and by specific location within the device itself that can be searched.

Defendant's conclusion is not the law. It is the result of a self-serving overreading of both Missak, a case often untethered from its facts and actual holding, and Riley, 573 U.S. at 378, a case that did not address electronics search warrants, but "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested." (emphasis added). It is the result of an interpretation of the requirements of the Fourth Amendment expanded well beyond that envisioned by our Founding Fathers. Defendant's interpretation asks this Court to grant to electronic searches a level of protection not afforded to the home – the very location the Founding Fathers held so sacrosanct that its protection animated the Fourth Amendment's requirements.

In approving the electronics warrants at issue here, Judges McGann and Oxley did not authorize unconstitutional searches. The wealth of actual federal precedent – and not the unpublished, out-of-state law upon which defendant craftily relies – makes clear that this Court's review can and should come to the same conclusions made by Judges McGann and Oxley: that the search warrants were supported by sufficient probable cause and described the location to be searched and the items to be seized with sufficient particularity. See DaE, J. The State, therefore, respectfully requests this Court deny defendant's request for suppression.

"A search based on a properly obtained warrant is presumed valid." State v. Sullivan, 169 N.J. 204, 211 (2001); State v. Valencia, 93 N.J. 126, 133

(1983). Reviewing courts should "accord substantial deference to the discretionary determination resulting in the issuance of the warrant." Sullivan, 169 N.J. at 211; State v. Marshall, 123 N.J. 1, 72 (1993), cert. denied, 507 U.S. 929 (1993). Any doubt as to the validity of a search warrant "should ordinarily be resolved by sustaining the search." State v. Keyes, 184 N.J. 541, 554 (2005); State v. Kasabucki, 52 N.J. 110, 116 (1968); State v. Missak, 476 N.J. Super. 302, 317 (App. Div. 2023). This is true even "'[w]hen the adequacy of the facts offered to show probable cause … appears to be marginal." Missak, 476 N.J. Super. at 317 (quoting Kasabucki, 52 N.J. at 116).

The burden to establish a warrant's invalidity rests with the defendant challenging it. State v. Keyes, 184 N.J. 541, 554 (2005); State v. Jones, 179 N.J. 377, 388 (2004); Valencia, 93 N.J. at 133. The defendant must "prove that there was no probable cause supporting the issuance of the warrant or that the search was otherwise unreasonable." Ibid.

A valid search warrant must be supported by "probable cause to believe ... that evidence of a crime is at the place to be searched." Sullivan, 169 N.J. at 210-11; State v. Evers, 175 N.J. 355, 381 (2003). Probable cause is "a fluid concept" that "eludes precise definition" and "cannot be defined with scientific precision." State v. Chippero, 201 N.J. 14, 26 (2009) (quoting Sullivan, 169 N.J. at 210); State v. Basil, 202 N.J. 570, 585 (2010) (quoting Evers, 175 N.J. at 381). This is so because probable cause "turn[s] on the assessment of probabilities in particular factual contexts – not readily, or even usefully, reduced to a neat set of legal rules.'" Basil, 202 N.J. at 585 (quoting Illinois v. Gates, 462 U.S. 213, 232 (1983); Sullivan, 169 N.J. at 211); Chippero, 201 N.J. at 27-28 (quoting United States v. Jones, 994 F.2d 1051, 1056 (3rd Cir.

1993)).

Nonetheless, "it is safe to say that a police officer has probable cause" "for the issuance of a search warrant" where there exists "'a fair probability that contraband or evidence of a crime will be found in a particular place.'" Ibid. This determination requires "a court ... look to the totality of the circumstances" as "viewed ... 'from the standpoint of an objectively reasonable police officer.'" Chippero, 201 N.J. at 27; Basil, 202 N.J. at 585 (quoting Maryland v. Pringle, 540 U.S. 366, 371 (2003)).

In Missak, 476 N.J. Super. at 310, 321-22, the Appellate Division found this standard – probable cause to believe evidence of a crime would be located where permission to search was sought, i.e., "all information contained within [the cell phone]" – not met where the facts contained in the supporting affidavit established only that defendant used two messaging applications and the text messaging function on two specific days in December to commit the sexually-motivated crimes. In so finding, the Appellate Division noted that it was undisputed the warrant "established probable cause permitting a search of the phone's contents and data limited to the text communications between the defendant and [undercover officer] allegedly exchanged through the Kik and Skout applications on December 8 and 9, 2021, and any alleged phone communications between defendant and the [undercover officer] on those two days." Id. at 320.

However, the Missak court could not find probable cause for "the expansive search warrant for all the data and information on the seized phone." Id. at 322. Significant to the court was that the search warrant allowed for the seizure of data "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;" for this data, the sole support was the affiant's representation that "individuals 'may' seek to alter … files to disguise what they contain." Id. at 320-21.

While it is true that, like in Missak, the much of the criminal conduct under investigation here occurred on a discrete date (November 20, 2018) and at specific times, the similarities end there. Detective Weisbrot's affidavit, submitted on November 21, 2018, established probable cause to believe that the 11 specifically-identified items of data relevant to two potentially connected crimes could be found in the defendant's electronics. DaD, E.

Detective Weisbrot's affidavit made clear that the crime under investigation was not merely the arson of defendant's residence; it also included "other related crimes." DaD. Of course these related crimes included the arson and murder of defendant's brother residence and the murder of the defendant's brother and his entire family, which was also discovered on November 20, 2018, and which was set forth in the four-corners of the affidavit. Thus, there was probable cause for the police to believe that evidence connecting these two sets of crimes could be found in the defendant's electronic devices. Cf. State v. Castagna, 400 N.J. Super. 164, 178-79 (App. Div. 2008) (discussing the importance and materiality of motive evidence).

The affidavit also set forth additional reasons to believe these two sets of crimes could be related: a vehicle matching the description of one of defendant's Porsches was seen on surveillance video leaving the area of defendant's residence in the early morning hours and returning before the fire at defendant's residence. The affidavit also connected defendant's electronic

devices to the crimes in ways beyond that which can generally be inferred, i.e., messages and calls between the defendant and his brother: defendant used a mobile application to access his own security cameras.

Detective Petruzziello's affidavit, submitted approximately one month later, built on this already existent probable cause. See DaI, J. In support of its request to search for 11 specifically-identified items of data in defendant's Apple watch, the detective detailed evidence establishing that the interconnected finances of the defendant and his brother were unravelling. Detective Petruzziello's affidavit detailed how his brother believed defendant was stealing from him, how his brother was terminating recurring financial payments to defendant's wife, and how the brothers' shared businesses utilized financial accounting software that each accessed remotely. These interconnected, unravelling financial interests did not exist solely on the date of the arsons and homicides. The evidence presented in Detective Petruzziello's affidavit showed they existed for at least months to years prior. The continued investigation also confirmed that which Detective Weisbrot and Judge McGann had reasonably inferred – that the brothers had communicated with each other via their electronic devices.

The affidavits of Detectives Weisbrot and Petruzziello both provided sufficient probable cause to support a search defendant's electronics for 11 specifically identified items of data beyond the date and time of the arsons and homicides. The warrants here authorized searches well grounded in both the law and the facts contained in the detectives' affidavits, which established probable cause to believe that evidence relevant to the arsons and homicides – and importantly the connection between the two sets of crimes. Thus, unlike in

Missak, there was a factually-grounded basis for the State's requests, and for Judges McGann and Oxley's approval of those requests. This Court can and should come to this same conclusion and do that which the Appellate Division could not in Missak: uphold these judicially-authorized searches.[2]

Because the Missak Court found that the "fatal flaw in the warrant" was the absence of sufficient probable cause, it found it did "not need to reach" "defendant's argument the warrant should be reversed because it violates the federal and state constitutional requirement that warrants must state with particularity the place to be searched." Missak, 476 N.J. Super. at 311, 322-23. The appellate court nonetheless offered the following comment:

> The warrant is very particular – it allows a search without limitation of all the phone's contents, information, and data. It therefore satisfies the "mandat[e] that [a] warrant specifically describe the search location so that an officer can reasonably 'ascertain and identify the place intended' to be searched, as authorized by the magistrate's probable cause finding." [State v. Bivins, 226 N.J. 1, 11 (2016) (quoting Marshall, 199 N.J. at 611[]).

Id. at 322 (emphasis added). It is to this finding, and this finding alone, the State submits Missak provides a sufficient guide and warrants the same conclusion. Compare ibid. with DaD, E, J, I.

"The particularity requirement is uncomplicated." Marshall, 199 N.J. at 611. Added to the Bill of Rights by the Framers "to prevent [the] 'wide-

[2] The State would be remiss in not noting for the Court that much of the data located within these electronic devices was also located in the records associated with iCloud account(s) obtained via communication data warrant(s), see, e.g., DaK, L, providing an "independent source" for the seized data. See State v. Holland, 176 N.J. 344, 353-65 (2003).

ranging, exploratory searches'" conducted by the Crown and reviled by the colonists, it "general[ly] mandates that a warrant sufficiently describe the place to be searched so 'that the officer with a search warrant can with reasonable effort ascertain and identify the place intended.'" State v. Feliciano, 224 N.J. 351, 366 (2016) (quoting Marshall, 199 N.J. at 611; Maryland v. Garrison, 480 U.S. 79, 84 (1987)). "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." Marshall, 199 N.J. at 611 (quoting Garrison, 480 U.S. at 84; United States v. Ross, 456 U.S. 798, 824 (1982)); see also Ross, 456 U.S. at 824 ("Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase").

"To be sufficiently particular … , a warrant must satisfy three requirements:" 1) it "must identify the specific offense for which the police have established probable cause;" 2) it "must describe the place to be searched;" and, 3) it "must specify the items to be seized by their relation to designated crimes." United States v. Ulbricht, 858 F.3d 71, 99 (2d Cir.), cert. denied, 585 U.S. 1033 (2018) (quoting United States v. Galpin, 720 F.3d 436, 445 (2d Cir. 2013)). These requirements are to be applied "with practical accuracy rather than absolute precision." United States v. Tompkins, 118 F.4th 280, 287 (2d Cir. 2024); see also United States v. Blakeney, 949 F.3d 851, 862 (4th Cir. 2020) ("When it comes to particularity, we construe search warrants in a 'commonsense and realistic' manner, avoiding a 'hypertechnical' reading

of their terms"); United States v. Bradley, 644 F.3d 1213, 1259 (11th Cir. 2011) (the particularity "requirement does not necessitate technical perfection; instead it is applied with 'a practical margin of flexibility'").

Even though modern-day cell phones are "minicomputers that also happen to have the capacity to be used as a telephone," see Riley, 573 U.S. at 393, this "focus on practical accuracy, as opposed to technical precision … extends to warrants authorizing the search of electronic devices." Tompkins, 118 F.4th at 287-88. "The Fourth Amendment does not require a perfect description of the data to be searched and seized." Ulbricht, 858 F.3d at 100. "The Fourth Amendment does not prohibit law enforcement from seizing … electronic devices that are likely to contain evidence of a crime simply because that evidence is likely intermingled with other non-criminal and private information." United States v. Ray, 541 F.Supp.3d 355, 394 (S.D.N.Y. 2021). "[I]t is precisely because computer files can be intermingled and encrypted that the computer is a useful criminal tool." Ibid. (citations omitted).

"[D]igital information is 'not maintained, like files in a file cabinet, in discrete locations,' but instead is often 'fragmented' on a storage device, potentially across physical locations.'" Tompkins, 118 F.4th at 287. The particularity requirement, like the searches it authorizes, necessarily can be broad enough to address this reality:

> Search warrants covering digital data may contain 'some ambiguity … so long as law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant.

Ulbricht, 858 F.3d at 100 (quoting Galpin, 720 F.3d at 446); United States v. Ivey, 91 F.4th 915, 917-18 (8th Cir. 2023) ("Evidence of the offense could have been found anywhere in the phone, and 'a warrant need not be more specific than knowledge allows").

To this end, the particularity requirement does not mandate that a search of an electronic device for data be conducted in a manner different from a search of a home for paper records: "Since a search of a computer is 'akin to [a search of] a residence … , searches of computers may sometimes need to be as broad as searches of residences pursuant to warrants." Ulbricht, 858 F.3d at 100; United States v. Richards, 659 F.3d 527, 538-39 (6th Cir.). cert. denied, 566 U.S. 1043 (2012). It is well recognized that "[w]hen a search requires review of a large collection of items, such as papers, 'it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.'" United States v. Williams, 592 F.3d 511, 519-20 (4th Cir.), cert. denied, 562 U.S. 1044 (2010) (quoting Andresen v. Maryland, 427 U.S. 463, 482 (1976)). So too for "electronic data," which "may entai[l] the exposure of records that are not the objects of the search to at least superficial examination in order to identify and seize those records that are." Ray, 541 F.Supp.3d at 394 (quoting Ulbricht, 858 F.3d at 100). "[A] search warrant does not necessarily lack particularity simply because it is broad." Ulbricht, 858 F.3d at 100. Broadness, and the realities of executing a broad warrant, does not "necessarily turn[] a search warrant into a prohibited general warrant." Ibid.

Even if one could characterize Detectives Weisbrot and Petruzziello's affidavit, with their 11 identified items of data to be seized and the locations in

which this data could be located on defendant's cell phone, see DaD, E, J, I, as broad, they cannot be said to lack in particularity. In identifying the specific data to be located and where it could be located, and limiting the seizure to only that data relevant to the arson and related crimes under investigation, the warrants here provided significantly more particularized details than the sufficiently-particular warrant in Missak, which allowed for "a search without limitation of all the phone's contents, information, and data." Missak, 476 N.J. Super. at 322. The search warrants authorized by Judges McGann and Oxley, bear no identity to the generalized warrants so hated by the Founders. The search warrants here did not run afoul of the particularity requirement of the Fourth Amendment, or New Jersey's similar constitutional protections, and, therefore, can and should be affirmed by this Court through the denial of defendant's request for evidence suppression.

In addressing defendant's myriad of attacks on the electronics warrants obtained and executed[3] here, the State respectfully requests this Court be guided by the course already set by our federal courts – the courts tasked with setting forth the parameters and meaning of the Fourth Amendment – and hold the electronic search warrants at issue here to nothing more or less than the standards long-established and applied to the most-venerated of private

[3] Defendant appears to suggest on pages five to six of his brief that the State's warrant execution on his Apple iPhone X occurred outside of the permitted 10-day window provided for in the warrant because the State needed the assistance of the Burlington County Prosecutor's Office's GrayKey Device due to encryption. Defendant's argument fails to appreciate that the continuation of a search appropriately started is permitted under the reasonable continuation doctrine. See Facebook, Inc. v. State, 254 N.J. 329, 367-68 (2023); State v. Finesmith, 406 N.J. Super. 510, 519-20 (App. Div. 2009).

locations – one's home, see Payton v. New York, 445 U.S. 573, 596-97 (1980). Richards, 659 F.3d at 538-40; Ulbricht, 858 F.3d at 99-100.

Respectfully submitted,

RAYMOND S. SANTIAGO
MONMOUTH COUNTY PROSECUTOR

/s/ Monica do Outeiro

By: Christopher J. Decker, 038272003
Deputy First Assistant Prosecutor and

Nicole D. Wallace, 037582008
Trial Team Leader
Assistant Prosecutor
Of Counsel and

Monica do Outeiro, 041202006
Assistant Prosecutor
Director, Appellate Section
On the Letter

c Monika Mastellone, A.D.P.D.