State of New Jersey

OFFICE OF THE PUBLIC DEFENDER
MONMOUTH REGION
JOSHUA HOOD, DEPUTY PUBLIC DEFENDER
7 BROAD STREET
FREEHOLD, NEW JERSEY 07728
TEL :732- 308-4320
FAX: 732-761-3679
TheDefenders@OPD.NJ.GOV

PHIL MURPHY
Governor
TAHESHA L. WAY
Lt. Governor

JENNIFER N. SELLITTI
Public Defender
JOSHUA HOOD
Deputy Public Defender

May 7, 2025

The Honorable Marc C. Lemieux, A.J.S.C.
Monmouth County Courthouse
71 Monument Park, 3rd Floor
Freehold, NJ 07728

Re: State v. Paul Caneiro
Case No. 18-004915 / Indictment No. 19-02-283-I

Motion to Suppress Evidence Seized with an Overbroad Warrant

Dear Judge Lemieux:

Please accept this letter brief in lieu of a more formal brief in support of the defendant's motion to suppress evidence seized with an overbroad warrant.

STATEMENT OF FACTS

On November 20, 2018, at approximately 5:00 AM, a fire occurred at the home of the defendant, Mr. Paul Caneiro. Later that day, at approximately 12:30 PM, a second fire was discovered at the home of the defendant's brother, Mr. Keith Caneiro. Tragically, what was also discovered at that time was that Keith Caneiro, along with his family members (his wife, Jennifer Caneiro, and their two children, [redacted]) were all murdered at their home.

By the early morning hours of November 21, 2018, defendant was charged with Aggravated Arson for allegedly setting fire to his own home. About a week later, on November 29, 2018, the defendant was charged with Aggravated Arson, four counts of Murder, and additional related offenses in connection with the fire that occurred at his brother's home. Defendant was later indicted on these offenses in February 2019.

As part of the State's investigation, numerous warrants were obtained to search the various digital devices that were seized and alleged to belong to the defendant. Specifically, these devices include: (1) iPhone x; (2) apple watch; (3) iCloud account; (4) iPad; and (5) Apple MacBook laptop. As discussed below, there are issues with several of these warrants and/or the subsequent search and seizure of these digital devices.

iPhone

On November 21, 2018, Det. Andrea Tozzi submitted an Affidavit in support of an application for a Communications Data Search Warrant (CDW) for the **T-Mobile records** pertaining to Paul Caneiro's iPhone x (732-500-7902). (Exhibit A).

On November 21, 2018 at 3:37 PM, Judge Joseph Oxley, J.S.C. signed the CDW. The warrant permitted the following search:[1] (Exhibit B).

a. Subscriber information, to include the subscriber's address, date of birth, social security number, form of payment, contract initiation and alternate contact information **for the time period of November 6, 2018 up to and including November 20, 2018;**
b. Applicant forms;
c. Contract and payment information;

[1] Of significance, 5 days later, a second CDW for T-Mobile records for this same phone number (732-500-7902) was issued by Judge Oxley on November 26, 2018. (Exhibit C).

In this subsequent warrant, the information sought was almost identical to the first warrant, with two exceptions: (1) an additional paragraph was added (new para. "n") seeking "True Call" and other info for the time period of 11-19-20 through 11-20-20; and (2) **all of the 11-6-18 through 11-20-18 time frames were changed to 11-19-18 through 11-20-18.**

d. Any and all incoming and outgoing call detail records with cell sites/location information **for the time period of November 6, 2018 up to and including November 20, 2018.**
e. Incoming and outgoing text messages/short message service (SMS) detail messages and content with cell sites/location information **for the said period;**
f. Any and all multimedia messages (MMS) detail records with cell sites/location information **for the said period;**
g. Any and all email detail records with cell sites/location information **for the said period;**
h. Any and all Packet Data/Internet Protocol (IP) detail records with cell sites/location information **for the said period;**
i. Any and all other stored photographs and/or videos with location **information for the said period** (without audio);
j. AMA Record Searches and/or Call to Destination Reports to obtain all telephone facility numbers that called the captioned wireless telephone facility number **for the said period;**
k. Cell site antenna locations for all incoming and outgoing communication detail records (including text, email, multimedia messages and network communication events/registrations) and/or direct connect records for the said period, including interim cell site/locations information which may be available for locations during the course of phone calls **for the aforementioned time periods**;
l. Detailed location information (i.e. LAC/CID/switch/repoll/site/sector; latitude, longitude; azimuth; beamwidths, PN's (pseudo noises) etc.) and cell site list(s), RF (radio frequency) propagation maps/surveys, antenna/tower maintenance records, etc. for the involved data **for the aforementioned time period**;
m. Any and all "ranging data" (distance from antenna estimates) which may be available for any communication events with the target device, known as "per call measurement data (PCMD)," "range to tower/round trip time data (RTT)," etc, **for the aforementioned time period.**
n. Any and all other information contained therein regarding wireless telephone facility (732) 500-7902 **during the time period of November 6, 2018 up to and including November 20, 2018.**

(Emphasis added).

Also on November 21, 2018, Det. Brian Weisbrot submitted an Affidavit in support of an application for a search warrant for the **Apple iPhone x itself**, which was seized from the defendant's person at the time of his arrest. (Exhibit D – pages 6-11). This Affidavit was substantially similar to the Affidavit submitted in support of the T-Mobile

records (see ¶¶ a through p of both warrants) except that the Affidavit seeking T-Mobile records was more detailed than the Affidavit seeking a search of the iPhone itself (see ¶¶ q though w of Exhibit A).

Later that same date, on November 21, 2018 at 12:25 PM, Judge James McGann, J.S.C. signed the search warrant. (Exhibit E).

In contrast to the T-Mobile warrant signed by Judge Oxley, which delineated a clearly defined time frame of 11-6-18 through 11-20-18, this warrant permitted the following search:

1. **Any information** relative to the identity of the service provider and/or cell service subscriber;
2. The assigned phone number of the cell phone;
3. Attached or electronically stored serial numbers, including the ESN, MIN and SIM card number;
4. Preference, system and security settings, including passwords and PIN numbers;
5. Call histories of incoming, outgoing and missed calls and direct connections, including all associated information recorded in connection therewith, such as telephone numbers, date and time of call, etc.,
6. Calendar or planner information, address book and contact information and programmed phone numbers;
7. **All text and email messages**, including sent, unsent, read, unread and draft messages and memos;
8. Digital images and video;
9. Installed applications;
10. Viewed and/or saved Web sites;
11. **All saved tasks** and digital copies of handwritten notes

(Emphasis added). That is, the search warrant for the iPhone x itself contained **no limitations by date, time frame, application or otherwise**. Rather it simply stated that "any" and "all" data could be searched, and in fact, failed to include for certain items any time frame at all.

Additionally, the warrant stated:

YOU ARE FURTHER COMMANDED *to execute this warrant within ten (10) days from the issuance hereof . . . and forthwith make return thereof, to me, with your report of the execution of this warrant and the written inventory of the property seized hereunder by you.*

Despite the Court's order to execute the search warrant within ten days, this was not done. In a report dated 2/19/19, Det. Petruzziello of the MCPO explains that as of November 27, 201[8], "Detective Migliorisi had made arrangements to bring Paul Caneiro's Apple iphone to Burlington County Prosecutor's Office for the purposes of extracting the data utilizing the GrayKey Device, which should provide more information than the Cellebrite UFED device."[2]

The inferred reason why the device needed to be further extracted is because on November 21, 2018, Det. Migliorisi attempted to extract data from the device only to learn that its data was encrypted. As a result, Det. Migliorisi needed to perform additional steps to successfully extract the information. Curiously, Det. Migliorisi never makes any mention of making arrangements with the Burlington County Prosecutor's Office (BCPO) and only notes, "The last step (#4) was not performed by me, I instead connected the device to the Cellebrite UFED and performed another Advanced Logical extraction with the iTunes backup file encryption password removed."

It is unclear what, if any, evidence was extracted during that subsequent attempt as the report does not indicate same – and it is likewise unclear when this attempt was made. However, the defense is left surmising that the attempts using the Cellebrite UFED device were unsuccessful, therefore leading to the use of BCPO's GrayKey extraction device. Again, no mention of this is contained in Migliorisi's report. Likewise, the defense has not received any supplemental reports from BCPO documenting the date/ time/ location/ or circumstances of this extraction.

[2] On April 27, 2025, the defense requested that the State provide any reports authored by BCPO and/ or authored by Det. Migliorisi related to the extraction performed at BCPO using GrayKey. The defense followed up regarding this request on May 1, 2025. To date, the defense has not received any reports related to this request.

However, it was not until March 8, 2019 that Det. Weisbrot signed and dated the "Return of Search Warrant" for the Apple iPhone x. (Exhibit F). Without any reports memorializing the date and time of the extraction, it can be inferred that the successful extraction using BCPO's GrayKey device was performed on or about this date – over 3 months after the 10-day time frame permitted in the warrant.

Apple Watch

On December 19, 2018, Det. Patrick Petruzziello submitted an Affidavit in support of an application for a search warrant for the **T-Mobile records** pertaining to Paul Caneiro's Apple watch (848-459-0431). (Exhibit G).

On December 19, 2018 at 9:32 AM, Judge Joseph Oxley, J.S.C. signed the search warrant. The warrant permitted the following search: (Exhibit H).

a. Subscriber information, to include the subscriber's address, date of birth, social security number, form of payment, contract initiation and alternate contact information **for the time period of November 19, 2018 up to and including November 20, 2018;**
b. Applicant forms;
c. Contract and payment information;
d. Any and all incoming and outgoing call detail records with cell sites/location information **for the time period of November 19, 2018 up to and including November 20, 2018.**
e. Incoming and outgoing text messages/short message service (SMS) detail messages and content with cell sites/location information **for the said period;**
f. Any and all multimedia messages (MMS) detail records with cell sites/location information **for the said period;**
g. Any and all email detail records with cell sites/location information **for the said period;**
h. Any and all Packet Data/Internet Protocol (IP) detail records with cell sites/location information **for the said period;**
i. Any and all other stored photographs and/or videos with location **information for the said period** (without audio);
j. AMA Record Searches and/or Call to Destination Reports to obtain all telephone facility numbers that called the captioned wireless telephone facility number **for the said period;**

k. Cell site antenna locations for all incoming and outgoing communication detail records (including text, email, multimedia messages and network communication events/registrations) and/or direct connect records for the said period, including interim cell site/locations information which may be available for locations *during* the course of phone calls **for the aforementioned time periods**;
l. Detailed location information (i.e. LAC/CID/switch/repoll/site/sector; latitude, longitude; azimuth; beamwidths, PN's (pseudo noises) etc.) and cell site list(s), RF (radio frequency) propagation maps/surveys, antenna/tower maintenance records, etc. for the involved data **for the aforementioned time period**;
m. Any and all "ranging data" (distance from antenna estimates) which may be available for any communication events with the target device, known as "per call measurement data (PCMD)," "range to tower/round trip time data (RTT)," etc, **for the aforementioned time period.**
n. All "True Call" or Timing Advance Information for 848-459-0431 **for the time from of November 19, 2018 through November 20, 2018**. Additionally, all Internet Protocols, (IP), Logs, Internet Activity, and Data Transactions, to include cell site if available **for the time frame of November 19, 2018 through November 20, 2018**.
o. Any and all other information contained therein regarding wireless telephone facility (732) 500-7902 **during the time period of November 19, 2018 up to and including November 20, 2018.**

(Emphasis added).

On December 19, 2018, Det. Patrick Petruzziello submitted an Affidavit in support of an application for a search warrant for the **Apple watch itself**. (Exhibit I). The paragraphs contained in this Affidavit were exactly the same as the Affidavit submitted in support of the T-Mobile records pertaining to the Apple watch. (See ¶¶ a through qq in both warrants).

On that same date, December 19, 2018 at 9:36 AM, Judge James Oxley, J.S.C. signed the search warrant. (Exhibit J).

In contrast to the T-Mobile warrant signed by Judge Oxley, which delineated a clearly defined time frame of 11-19-18 through 11-20-18, this warrant permitted the following search:

1. **Any information** relative to the identity of the service provider and/or cell service subscriber;
2. The assigned phone number of the **cell phone**;
3. Attached or electronically stored serial numbers, including the ESN, MIN and SIM card number;
4. Preference, system and security settings, including passwords and PIN numbers;
5. Call histories of incoming, outgoing and missed calls and direct connections, including all associated information recorded in connection therewith, such as telephone numbers, date and time of call, etc.,
6. Calendar or planner information, address book and contact information and programmed phone numbers;
7. **All text and email messages**, including sent, unsent, read, unread and draft messages and memos;
8. Digital images and video;
9. Installed applications;
10. Viewed and/or saved Web sites;
11. **All saved tasks** and digital copies of handwritten notes

(Emphasis added). That is, the search warrant for the Apple watch itself contained no limitations by date, time frame, application or otherwise. Rather it simply stated that "any" and "all" data could be searched, and in fact, failed to include for certain items any time frame at all.

iCloud Account

On November 28, 2018, Det. Andrea Tozzi submitted an Affidavit in support of an application for a CDW for records pertaining to Paul Caneiro's Apple iCloud account. (Exhibit K).

On that same date, November 28, 2018 at 9:42 AM, Judge Joseph Oxley, J.S.C. signed the search warrant. The warrant permitted the following search: (Exhibit L).

a) Device Registration including customer name, address, email address, and telephone number at the time of device registration;
b) Customer Service Records including records of suppo1i interaction, information regarding the device, waITanty and repairs **for the time period of November 1, 2018 to November 20, 2018;**

c) iTunes subscriber information, connection logs with IP addresses, purchase/download transactions, update/re-download connections, and iTunes Match connections **for the time period of November 1, 2018 to November 20, 2018**;
d) Apple Online Store Purchases associated with the email · address pcaueiro(a),mac.com and/or pcaneiro@me.com **for the time period of November 1, 2018 to November 20, 2018;**
e) **Any and all iCloud data** including but not limited to music, photos, documents, subscriber information, mail logs, email content (pcaneiro@mac.com and/or pcaneiro@me.com or any other email contained in the iCloud), contacts, calendars, bookmarks, safari browsing history, maps search history; messages, iOS device backups including photos and videos in the camera roll, device settings, app data, iMessage, business chat, SMS and MMS messages and voicemail **for the time period of November 1, 2018 to November 20, 2018**;
f) Find My iPhone transactional activity including remote requests to access all connected devices and what actions were taken on the associated **device for the time period of November 1, 2018 to November 20, 2018;**
g) Any and all MAC addresses associated with the above identified serial number for the time period of November 1, 2018 to November 20, 2018;
h) Any and all connected devices associated with the WIFI address 74:9e:af:6f:bf:f4 and Bluetooth device address 74:9e:af:6c:b5:4a **for the time period of November 1, 2018 to November 20, 2018;**
i) Any and all sign-on activity to Apple services including the connection logs with IP addresses **for the time period of November 1, 2018 to November 20, 2018;**
j) Any and all My Apple ID and iForgot logs including connection logs with IP addresses and transactional records **for the time period of November 1, 2018 to November 20, 2018;**
k) Any and all FaceTime call invitation logs **for the time period of November 1, 2018 to November 20, 2018;**
l) Any and all iMessage capability query logs **for the time period of November 1, 2018 to November 20, 2018.**

(Emphasis added).

iPad & Apple MacBook laptop

On November 21, 2018, Det. Brian Weisbrot submitted an affidavit in support of an application for a warrant to search Paul Caneiro's vehicle, a Porsche Cayenne. (Exhibit D – pages 5-6).

Later that same date, on November 21, 2018 at 12:25 PM, Judge James McGann, J.S.C. signed the search warrant. (Exhibit M). This warrant permitted the search of:

> (3) **Any and all** cellular telephones, computers, laptops, tablets and **permission to search same** pursuant to this warrant;

(Some emphasis added; some emphasis in original). As a result of this search, police located a backpack alleged to belong to Mr. Caneiro. Inside, police located the (1) Apple MacBook laptop, (2) iPad, and (3) Apple Watch. Based on this warrant, data extractions were then performed on the Apple MacBook and iPad, while a separate search warrant was obtained for the search of the Apple Watch (Exhibit J).

LEGAL ARGUMENT

The digital age has required courts throughout our nation to reevaluate the Fourth Amendment to ensure that privacy survives modern advances in technology. As recognized by our United States Supreme Court, "[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans the privacies of life. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." Riley v. California, 573 U.S. 373, 403 (2014), (internal citations omitted). The judiciary is obligated to ensure that technological advances do not erode the Fourth Amendment protections. Carpenter v. U.S., 138 S. Ct. 2206, 2223 (2018).

Indeed, "a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record." Riley, 573 U.S. at 394. Moreover, "a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet." Ibid. "[T]he data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket

a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone." Ibid.

In light of these privacy rights, search warrants may not authorize the search and seizure of **all** data in a cell phone. As recently recognized in State v. Missak, 476 N.J. Super. 302 (App. Div. 2023), such a warrant is an unconstitutional general warrant. As such, the search warrant must be limited in scope by date range, category of data, and/ or other filter that is factually related to the probable cause alleged in the affidavit. Because the warrants issued here are general warrants allowing for the search and seizure of the defendant's entire devices, all of the evidence seized therefrom must be suppressed. Since New Jersey does not recognize the good faith exception to the warrant requirement, all data seized must be suppressed, without regard to a post execution finding that the general warrant issued could have been limited in scope, but was not.

POINT I

THE WARRANTS CONCERNING THE SEARCH OF THE IPHONE, APPLE WATCH, MACBOOK, AND IPAD ARE INVALID AND ILLEGAL GENERAL WARRANTS.[3]

Our courts have recognized that 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. Opposition to such searches was in fact one of the driving forces behind the Revolution itself. Riley v. California, 573 U.S. at 403.

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,

[3] The defense is not challenging the iCloud Warrant at this time; it is only included to demonstrate the limited time frame for which police had probable cause.

60 N.J. 594 (1972). The Fourth Amendment and Article I, Paragraph 7 instead 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, para 7; State v. Andrews, 243 N.J. 447, 464 (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 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) (quoting State v. Malik, 221 N.J. Super. 114, 118 (App. Div. 1987).

The purpose of the particularity requirement “was to prevent general searches[,]” and to prevent such “wide-ranging exploratory searches.” Feliciano, 224 N.J. 351, 366 (2016) (quoting Mayland v. Garrison, 480 U.S. 79, 84 (1987)); see, e.g. Importantly, “[t]he progress of two-hundred-thirty-two years since the ratification of the Bill of Rights has not tempered these provisions’ denunciation of general searches.” Missak, 476 N.J. Super. at 316. In United States v. Riccardi, 405 F. 3d 852, 862-63 (10th Cir. 2005), for example, the court held that a warrant which “permitted the officer to search for anything from child pornography to tax returns to private correspondence,” was “precisely the kind of wide-ranging exploratory search that the framer intended to prohibit.”

The recent case of State v. Missak. supra, is illustrative of the New Jersey courts finally recognizing that a warrant to search the entire contents of a cell phone is in fact a prohibited general warrant. In Missak, the defendant was arrested for luring a “minor” he made arrangements to meet through text messages and mobile chats. Upon his arrest, his cell phone was seized and a warrant was obtained authorizing a search of the entire cellular device. The detective who authored the Affidavit in support of the warrant “sought the search warrant for the express purpose of ‘obtaining evidence of the crimes of’ luring and attempted sexual assault allegedly committed by defendant on December 8 and 9, 2021. Id. at 310. And yet, the detective applied for, and received, a search warrant that

allowed law enforcement "to access and examine ALL of the data" on the phone. Ibid. (Emphasis in original). More specifically, the detective requested that the "warrant authorize the State to 'access, search, forensically examine, and document all information contained within [the cellular phone], for evidence relating to offenses involving the exploitation of children' specifically involving the crimes of luring and attempted sexual assault defendant allegedly committed on December 8 and 9, 2021.'" Ibid. In response to this application, the court found the detective's certification established probable cause to believe the cellular phone "will yield evidence of the crimes of" luring and attempted sexual assault. Id. at 311.

On appeal, and after reciting the history of our nation's prohibition against general warrants, the Appellate Division held that "the search warrant is constitutionally **invalid**." Id. at 315. (Emphasis added). The Appellate Court explained that because the detective's affidavit "sought a search warrant for evidence pertaining only to the crimes of luring and attempted sexual assault defendant allegedly committed on December 8 and 9, 2021[,]" there was absolutely no justification for allowing the search of the phone to fall outside of that date range or beyond the messaging applications. Id. at 320-222. The court stated, "[f]or example, the record lacks facts establishing probable cause the phone's text messages, calls communications, GPS data, or other data created or existing prior to defendant's alleged initial communication with [the detective] posing as the juvenile on December 8, 2021, contain evidence of the two crimes for which [the detective] expressly sought the search warrant." Ibid.

The Appellate Court further explained, "What is missing from [the detective]'s certification are any facts establishing probable cause for 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. Accordingly, the Appellate Court concluded, "in our view, [the detective]'s certification does not provide sufficient facts supporting the expansive search warrant **for all the data and information** on the seized cellular phone." Id. at 322. (Emphasis added).

Of significance, the Appellate Court found unpersuasive the detective's sworn statements that a search of the entire phone was necessary because individuals "may" seek to hide or alter data in other areas of the phone. The Appellate Court reasoned that the "justification falls short of the constitutional mark, however, because establishing probable cause for a search requires more than a showing of what 'may' have occurred." Id. at 321.

Thus, while recognizing that the detective's affidavit might have established probable cause to believe the phone contained evidence of the messages exchanged between the defendant and the undercover posing as a child on two specific dates, it did not provide a basis for searching all of the data and information seized on the phone. Id. at 322.

Missak cited with approval the case of State v. Smith, 344 Conn. 229 (2022), where the Connecticut Supreme Court found unconstitutional a search warrant for all the data on a cellular phone. Missak, 476 N.J. Super at 320. In Smith, the court concluded that "a warrant for the search of the contents of a cell phone must be sufficiently limited in scope to allow a search of only that content that is related to the probable cause that justifies the search." Id. at 250. (Emphasis added). The Smith court explained that the warrant was invalid because:

> The warrant . . . failed to provide the type of information sought by its authorization. **The warrant authorized a search of a "data extraction," which allowed for a search of the entire contents of the cell phone.** The warrant failed to list types of data this particular device or cell phones in general contain, and the types of data on the phone the affiants sought to search and seize, such as cell phone call logs, text messages, voice messages, photographs, videos, communications via social media, or other evidence of the crime of aggravated assault. Further, 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.

Id. at 251. (Emphasis added). As such, the Smith court further concluded "that the search warrant did not comply with the particularity requirement because it did not sufficiently

limit the search of the contents of the cell phone by description of the areas within the cell phone to be searched, or by a time frame reasonably related to the crimes. Therefore, the trial court improperly denied the defendant's motion to suppress the evidence obtained with respect to the cell phone search warrant." Id. at 252.

In fact, other courts have issued similar opinions with similar reasoning. In Commonwealth v. Broom, 52 N.E.3d 81, 89 (Mass. 2016), the Massachusetts Supreme Court held that a warrant was "general" and "conclusory" and not supported by probable cause. The Broom Court noted that it is insufficient for the affiant to blanketly assert that "cellular telephones contain multiple modes used to store vast amount of electronic data" in the hopes that such "vast" data would contain evidence of a homicide. Id. at 495-96. Rather, the warrant must contain "a substantial, particularized basis" to expect that certain data would reveal evidence of a certain particular offense, in that case, a homicide.

In a similar vein, the Massachusetts Supreme Court, in Commonwealth v. White, 59 N.E.3d 369 (Mass. 2016) held that "probable cause to search or seize a person's cellular telephone may not be based solely on an officer's opinion that the device is likely to contain evidence of the crime under investigation[.]" Id. at 371-72. In White, police obtained a warrant based on the purported common-sense notion that people communicate and conspire with others about their crimes using their cellular devices. The White Court held that although "[i]t may well be the case that many of [those] ... who own a cell phone [in effect] keep on their person a digital record of nearly every aspect of their lives, including, presumably, communications with their coventurers[,]" this notion does "not, alone, furnish the requisite nexus between the criminal activity and the places to be searched or seized." Id. at 375 (quoting Riley v. California, supra) (internal quotations omitted). And thus, does not amount to probable cause. Ibid.

In State v. Mansor, 363 Or. 185 (2018), the Oregon Supreme Court disagreed with the State's position that if a search warrant authorizes the seizure of a digital device such as a computer, then law enforcement is "free to examine it as they see fit." Id. at 208. In fact, the Mansor Court noted that the State's position "is not well taken." Ibid. The Mansor Court held that, "the fact that police have a warrant, based on probable cause, to search

for and seize 'things,' including computers, does not necessarily mean that they may conduct a comprehensive forensic examination of a computer that they seize, and then use at trial anything they find on the computer, without limit." Ibid. The Mansor Court reminded that, a "computer or other digital device is a repository with a historically unprecedented capacity to collect and store a diverse and vast array of personal information" and thus "the lawful seizure of defendant's computer does not, by itself, permit the state to analyze and use all of the information found on the computer." Id. at 208-211.

Importantly, the Mansor Court also explained a significant distinction between two related, but separate concepts – specificity and overbreadth. That is, "[a] warrant must be sufficiently specific in describing the items to be seized and examined that the officers can, with reasonable effort ascertain those items to a reasonable degree of certainty. But, *even if the warrant is sufficiently specific, it must not authorize a search that is broader than the supporting affidavit supplies probable cause to justify*." Id. at 212 (quoting State v. Reid, 319 Or. 65, 71 (1994)) (internal quotations omitted). Thus, "the warrant must identify, as specifically as reasonably possible in the circumstances, the information to be searched for, including, if relevant and available, the time period during which that information was created, accessed, or otherwise used." Id. at 218.

Returning to New Jersey jurisprudence, since the Missak decision was issued in 2023, our higher courts have followed suit. Most recently, in State v. Summers, 2024 WL 5252023 (Dec. 31, 2024), our Appellate Division relied on Missak to reverse a denial of the defendant's suppression motion in a Homicide case. (**DA1-7**). In Summers, the defendant moved to suppress evidence seized from the contents of his cell phone because the warrant was an overbroad, general warrant that permitted a search of the entire cell phone. In fact, in Summers, similar to the instant case, there were two related warrants:

First, on April 11, 2019, detectives applied for, and obtained, a CDW for defendant's cell phone carrier records. This CDW was limited to the time frame of April 5, 2019 to April 11, 2019. (The alleged murder occurred on April 6, 2019).

Second, on May 17, 2019, detectives applied for, and obtained, a search warrant for the defendant's cell phone itself. Unlike the first warrant, this warrant for the phone itself was for **"any an all"** of the information contained in the phone. Thus, the Summers court noted that unlike the first warrant, this second warrant "did not include a temporal limitation, or any other limitation, restricting the search of any and all data on the phone. The warrant stated simply that law enforcement was authorized to search the cell phone." Id. at *1-2. (Emphasis added).

The Summers court also noted that the two Affidavits submitted in support of these two warrants were substantially similar in that the second Affidavit "expressly incorporate[d]" the contents of the first Affidavit. Id. at *2.

The defendant challenged the second warrant on the grounds that it was an overbroad, general warrant failing to satisfy the particularity requirement. Id. at *1. However, the trial court denied the defendant's motion. Id. at *3.

On appeal, the Appellate Division reversed and suppressed the evidence. Id. at *7-8. The Appellate Court emphasized: "As technological advances introduce '[s]ubtler and more far-reaching means of" privacy invasion, the judiciary is obligated 'to ensure that [advance] does not erode Fourth Amendment protections.'" Id. at *3, 6. (quoting Missak, 476 N.J. Super. at 316) (Emphasis added). In this context, the Summers Court further noted, "The use of open-ended, general warrants has been condemned as "the worst instrument of arbitrary power," Boyd v. United States, 116 U.S. 616, 625 (1886) (internal quotation omitted), and "was a motivating factor behind the Declaration of Independence," Berger v. New York, 388 U.S. 41, 58 (1967)." Id. at *4. Indeed, "Even in the context of a cellular phone search, a valid warrant requires 'probable cause to believe that a crime has been committed, or is being committed, at a specific location or that evidence of a crime is at the place sought to be searched.'" Id. at *4 (citing State v. Sullivan, 169 N.J. 204, 210 (2001)). (Emphasis added).

Next, citing to Missak, the Appellate Division further acknowledged, "'[d]iscerning where evidence of a crime may be found on a cellular phone is a function of complex

technology ....'" Id. at 6 (Citing Missak, supra. at 319). While stating, "We note the voluminous amount of private information that is stored on a cellular phone[,]" the Summers Court concluded:

> Applying the applicable standard of review and legal principles, we are persuaded that the evidence derived from the search made pursuant to the May 17, 2019 search warrant must be suppressed. **We reach this determination based on the breadth of the express language of the warrant, which authorized law enforcement officers unfettered and unrestricted access to search defendant's phone for any and all information, data and the like, for which the State had failed to establish probable cause. In fact, the warrant granted authority to search defendant's phone without any limitations, temporal or otherwise, at all.**
>
> We note the complexity of the digital landscape "presented by data contained in cellular phones, the manner in which such data may be searched and retrieved, and the constitutional issues presented by law enforcement's efforts to traverse the landscape in search of evidence." Missak, 476 N.J. Super. at 319. And, irrespective of the fact that the affidavit in support of the warrant application "described in sufficient detail how cell phones are used and how [a search of the cell phone] can result in data which is relevant to a criminal investigation," **the warrant itself must identify the location on the phone where data and information possibly stored on defendant's phone may be found based on the probable cause established in the search warrant affidavit**. Marshall, 199 N.J. at 611 (stating "the description [of where to find the information sought by the warrant] is such that the officer with a search warrant can with reasonable effort ascertain and identify the place intended").
>
> We are further persuaded that the May 17, 2019 warrant is not supported by probable cause for the authorized expansive and limitless search of defendant's phone and data. We note that by May 17, 2019, law enforcement knew the timeframe of Harvey's murder and had the surveillance footage of defendant leaving Harvey's residence using his cell phone. With this information, law enforcement officers and the court had, at a minimum, the facts necessary to properly limit the temporal scope of the May 17, 2019 warrant. See Jones, 179 N.J. at 388. They did not.

> Although a search warrant enjoys a presumption of validity, Bivins, 226 N.J. at 11, **because the warrant in this case authorized a search for all data from defendant's cell phone, we are convinced it is constitutionally invalid**. See, e.g., Winn, 79 F. Supp. 3d at 922 (finding a CDW "had no valid portions" because the description of the search — "any and all files" — was broader than the evidence over which the police had probable cause); Burns v. United States, 235 A.3d 758, 774 (D.C. 2020) (finding invalid warrants that broadly "authorized the seizure of 'any evidence' on the phones and listed, by way of examples, generic categories covering virtually all of the different types of data found on modern cell phones").

Summers, supra. at *6-7. (Emphasis added).

Notably, a case that the defendant in Summers, and ultimately the Summers Court itself, relied upon is Illinois v. Winn. 79 F. Supp. 3d 926 (2015). In Winn, the defendant was charged with public indecency for touching his genitals while taking photos and videos of teen girls in their swimsuits. Id. at 910. Detectives sought and obtained a search warrant for the defendant's cell phone, with the warrant permitting a search of:

> ***any or all*** *files on said cell phone and its SIM Card or SD Card to include but not limited to the calendar, phonebook, contacts, SMS messages, MMS messages, emails, pictures, videos, images, ringtones, audio files, all call logs, installed application data, GPS information WiFi information internet history and usage, any system files on phone, SIM Card, or SD Card, or any data contained in the cell phone, SIM Card or SD Card to include deleted space.*

Id. at 911 (emphasis added). The Winn Court held that this warrant was an unconstitutional "general warrant." Id. at 904. The Winn Court explained that there was probably evidence to believe that only two categories of data – photos or videos – would have evidence of criminality. Id. at 922. Specifically, the court explained that "the warrant did not limit the scope of the seizure to only that data or describe that data with as much particularity as the circumstances allowed." Ibid. "Instead, the warrant contained an unabridged template that authorized the police to seize the entirety of the phone and rummage through every conceivable bit of data, regardless of whether it bore any relevance whatsoever to the criminal activity at issue." Ibid. The Winn Court therefore

concluded, "Simply put, the warrant told the police to take everything, and they did. As such, the warrant was overbroad in every respect and violated the Fourth Amendment." Ibid.

Two additional recent New Jersey cases that have been decided since the Missak decision are State v. Halgas, 2024 WL 4563241 (Oct. 24, 2024) and State v. Saal, 2024 WL 5036721 (Dec. 9, 2024). (**DA8-15** and **DA16-20**, respectively).

In State v. Halgas, the Appellate Court found that the detective's Affidavit in support of its application for a warrant to seize and search "**any and all electronic devices**" from the defendant's marital home was deemed invalid. Id. at *9. Specifically, in Halgas, police obtained a warrant to search the defendant's home along with any and all electronic devices found therein. As a result of the warrant, police seized and searched phones belonging to the defendant's wife and daughters. Id. at 2.

After searching the wife's phone, and finding evidence therein, the defendant moved to suppress the evidence. Id. at *3. After confirming that the defendant had standing to challenge the evidence seized from his home, the court found that while there was probable cause to support the search of the home, there was not sufficient probable cause to support the search of the phones. Id. at *7-9. The court reasoned:

> In this case, we need not reach the scope of search issue addressed in Missak because **the warrant application does not set forth facts sufficient to support a finding of probable cause to seize and search the cell phones**. The warrant application does not set forth any factual basis to find a nexus between the alleged crimes and information that might be located on cell phones. **The crimes themselves do not involve cell phones or electronic communications**, **and there is nothing in the warrant application to create a reasonable belief that relevant evidence would be located on the cell phones used by Rosemary or the daughters**. The only mention of cell phones in the application is the unremarkable statement that "numerous cellular phones are known to be inside the residence ...." The application does not provide any other information about the cell phones or even specify where in the residence they were located.

Id. at *8. Ultimately, the court held that while the police had probable cause to search the premises (the defendant's home), this was "not including authorization to search the cell phones." Id. at *9. The Court explained, "According to the Detective, he wanted to seize the phones to see [a]ny communications which might assist us in the investigation to understand what happened.'" Id. *8. However, "That is not an adequate factual basis for probable cause to search a cell phone. The State must do more than assert a 'mere hunch or bare suspicion.'" Ibid.

In State v. Saal, the Appellate Divion reviewed the denial of a suppression motion concerning a search warrant issued for the defendant's cell phone. Although the defendant argued that the search warrant was overbroad pursuant to Missak, the Appellate Division disagreed. However, the reason the Appellate Division disagreed because the warrant, in fact, did contain language that limited the search to "**around the time of the murder**." Id. at *5. (Emphasis added). Therefore, the Appellate Court found that, "the warrant neither lacked particularity, nor was it overbroad.'" Ibid.

With respect to remedy, the Summers Court rejected the State's suggestion that "when a portion of a search warrant is constitutionally infirm, 'primarily due to a lack of particularly or probable cause, it is separated from the remainder and the evidence seized under the valid portion admitted[.]'" Summers, supra. at *7 (citing, among other cases, U.S. v. Sells, 463 F.3d 1148 (10th Cir. 2006)). Thus, the Summers Court held, "Because we have found the warrant here invalid in its entirety *based on a lack of probable cause supporting its unbridled breadth*, and the warrant does not distinguish between the clearly invalid search authorization from any portion of it the State claims is valid, we need not further address the State's severability arguments under Sells. Ibid. (Emphasis added).

Nevertheless, when presented with this same Missak issue, New Jersey trial courts have elected to perform judicial surgery, separating the time-frame for which there is probable cause from the rest of the warrant. In Burlington County, a trial court in State v. Sam Gore decided to perform judicial surgery on the overbroad search warrant to limit the evidence that was admissible at trial. Specifically, while the warrant permitted the search of 'any and all' information contained in the phone, the court limited the evidence

to the time frame supported by probable cause, which was a 4-day period from 9-17-19 to 9-20-19. (**DA43-44**). Thus, all information taken outside of that time frame was precluded. It should be noted that the defendant sought leave to appeal this Order on the basis that the trial court improperly performed judicial surgery, however, that motion was denied.[4]

In Mercer County, a trial court in State v. Kahiree Peterson[5] likewise performed judicial surgery in a case where the police obtained an overbroad, general search warrant for the search of the defendant's entire iPhone. (**DA22-42**). Like the Burlington Court, the Mercer Court limited the admission of evidence to that which fell within a specific time frame supported by probable cause while the rest of the evidence was excluded. The State was therefore precluded from using any content found on the phone outside of a 60-day window (30 days pre-Murder; 30-days post-Murder). In its written opinion, the court explained:

> Since Detective Johnston's certification did not establish probable cause to believe that evidence relating to Mr. Abdullah's murder would be found in every file or application contained on the Defendant's phone, **the warrant's authorization to search and forensically examine 'all stored electronic data' amounted to a general warrant that does not pass constitutional muster, just like the one quashed in Missak.**

(**DA37**).

Ultimately, the protection over one's cell phone data is critical because "a cell phone search would typically expose to the government far more than the most exhaustive search of a house." Riley v. California, 573 U.S. 373, 396 (2014). (emphasis in original). "Data on a cell phone can contain information related to medical conditions or "a wealth of detail about . . . familial, political, professional, religious, and sexual associations." Id. at 395-96 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)). Moreover, cell phone apps "offer a range of tools for

[4] The issue never reached direct appeal because the defendant was acquitted at trial.
[5] This case is still pending with the trial court.

managing detailed information about all aspects of a person's life." Id. at 396 (noting existence of apps for political associations, addictions, religion, tracking pregnancy, and "for every conceivable hobby or pastime"). A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form[.]" Id. at 396-97. Thus, general warrants permitting the search of a person's entire cell phone are, without question, overbroad, illegal warrants.

Moreover, although a seizure may deprive an individual of control over his cell phone, it does not reduce his reasonable expectation of privacy in the contents contained within his phone. Cf. U.S. v. Carey, 172 F.3d 1268 (10th Cir. 1999) (noting that although "electronic storage" makes "tempting targets in searches for incriminating information[,]" law enforcement must still limit their searches to what is supported by probable cause). Additionally, safeguards must be taken to protect an individual's personal information and data stored within his cell phone the same way safeguards are taken to protect physical property. Not only does this provide protection to the accused, but also to innocent third parties whose personal information and communications can be contained within the accused's phone. Ibid. A warrant that fails to include such limitations as to content and time may therefore render the warrant insufficiently particular and thus invalid.

In fact, a prime example of this principle can be found in the present-day high-profile case currently being re-tried, Massachusetts v. Karen Read. In that case, where Ms. Read is accused of murdering her boyfriend, the lead detective, Det. Proctor performed a search (pursuant to an extraction) of her cell phone. While doing so, he evidently was texting other law enforcement officers discussing how he was looking for nude photographs of her on her phone and was disappointed that he had not yet found any.[6] Likewise, after searching through her phone and finding content related to her

[6] *https://www.the-independent.com/news/world/americas/crime/karen-read-murder-trial-boston-b2536524.html*

https://nypost.com/2025/03/19/us-news/trooper-michael-proctor-fired-for-conduct-during-karen-read-murder-case/;

Crohn's disease, he made insensitive, vulgar, and crude comments about her medical condition in a text thread with others.[7] While this serves as an extreme example where police misconduct occurred, it does not take away from the fact that even the accused, and even those accused of murder, have privacy rights that must be protected by our Constitution. Whether the search for an individual's private photographs or personal health information is intentionally located or inadvertently stumbled upon during a broad search of their cell phone, either way, the person's privacy interests have been violated. Our jurisprudence now recognizes this and requires that search warrants for cell phones and other digital devices be limited in scope by timeframe and application.

Accordingly, it should not be forgotten that the Fourth Amendment of the United States Constitution and Article I, Paragraph 7 of the New Jersey Constitution prohibit general searches. See e.g., State v. Feliciano, 224 N.J. 351, 366 (2016) ("The Framers added the particularity requirement to the Bill of Rights to prevent such 'wide-ranging exploratory searches.'"). As the above courts, including New Jersey's Missak Court, have realized, these critical rights protecting against general warrants are not eliminated, and in fact must be upheld, in the digital age. The law must "evolve in response to changes in technology." State v. Earls, 214 N.J. 564, 588 (2013). See Facebook, 471 N.J. Super. at 464. Carpenter v. United States, 138 S.Ct. 2206, 2223 (2018).

Here, in the instant matter, the warrants in issue – the search warrants for the physical iPhone and Apple Watch devices as well as for the iPad and Apple MacBook – are the precise type of overbroad warrants that Missak and these other courts have identified as constituting an illegal general warrant.

---

https://www.rollingstone.com/tv-movies/tv-movie-news/karen-read-case-officer-joked-searching-phone-nudes-1235296877/;

https://nypost.com/2025/03/19/us-news/trooper-michael-proctor-fired-for-conduct-during-karen-read-murder-case/

7 Ibid.

First, with respect to the warrants for the iPhone and watch, these warrants erroneously authorized law enforcement to seize 'any and all' information from these devices without any probable cause to support the search of the entire devices. In fact, the T-Mobile records that were sought for these devices contained clear temporal restrictions. The T-Mobile records for the phone were initially limited to a 15-day time frame of 11-6-18 through 11-20-18, however, 5 days later limited even further to only 11-19-18 through 11-20-18. Likewise, the T-Mobile records for the watch were limited to the 2-day time frame of 11-19-18 through 11-20-18. And yet, the warrants obtained for the actual physical devices – obtained the same day as their respective T-Mobile warrants using almost identical Affidavits of PC – did not in any fashion limit the scope of the search, either by timeline or by application. As demonstrated in the Summers case, supra, this disparity in the T-Mobile warrants versus the physical device warrants is constitutionally unacceptable.

To be sure, the fact that the T-Mobile warrants for the same devices were limited to a 6-day and even a 2-day time period using the same Affidavits as used for the devices themselves, clearly demonstrates a concession that the warrants should have been limited in scope. That is, there was no PC to support a search of the devices beyond those 6-day and/ or 2-day time frames. There was absolutely no probable cause to support an unfettered, limitless search of the entire devices. In fact, while the iPhone warrants (T-Mobile and physical device) were obtained on November 21, 2018, the same date of defendant's arrest, the iCloud warrant was obtained 7 days later, on November 28, 2018 and even still, despite an additional 7 days of investigation, the warrant was limited in scope to a 2-day period of 11/19/18 to 11/20/18. Then, another month later, the Apple Watch T-Mobile records were sought for the same two-day period. As such, there was no legal basis to justify warrants for the search of the entire devices, wherein the information/ data could date back weeks, months, years, or even decades.

With respect to the iPad and Macbook, these devices were erroneously included in search warrants for defendant's home, car, and business address. As the Court in Halgas, supra, made clear, throwing a generalized, overbroad provision into the warrant

pertaining to the search and seizure of "any and all" phones or electronic devices – without any regard to what they are or who they belong to – is unacceptable because there was not sufficient probable cause to support same. For instance, there is nothing in the Affidavit of PC "to create a reasonable belief that relevant evidence would be located on the cell phones used by [Susan Caneiro] or their daughters." See Halgas, supra at *8. Moreover, pursuant to Missak, supra, this catch-all provision renders the warrant an unconstitutional, overbroad warrant.

Thus, to be clear, the language in these warrants renders them deficient because it granted the police unfettered authority to search the seized devices. Compare with State v. Ulrich, 265 N.J. Super. 569, 575-76 (App. Div. 1993) (discussing anticipatory warrants). There are absolutely no restrictions, parameters, or restraints qualifying this search. No time-frame, no limitation as to the types of data or information to be searched (e.g. text messages, photos, applications, etc), and no restriction as to the content contained within these applications whatsoever. As a result, this warrant permitted the exact type of "wide-ranging exploratory searches" that our Fourth Amendment and New Jersey Constitution expressly forbid. See Feliciano, 224 N.J. 351, 366 (2016) (quoting Mayland v. Garrison, 480 U.S. 79, 84 (1987)); United States v. Riccardi, 405 F. 3d 852, 862-63 (10th Cir. 2005).

As in Missak, the warrant here improperly authorized the search of the entire device, specially "ALL of the data." 476 N.J. Super. at 310. Thus, as in Missak, the search warrant here "is constitutionally invalid." Id. at 315. Likewise, as in Missak, the detective's application for the search warrant "does not provide sufficient facts supporting the expansive search warrant **for all the data and information** on the seized cellular phone." Id. at 322.

The warrants at issue here are also comparable to the warrant described in the Smith case, supra, where the "warrant authorized a search of a 'data extraction,' which allowed for a search of the entire contents of the cell phone." Smith, 344 Conn. at 251. The Missak Court agreed with the Smith Court's ruling that the search warrant was unconstitutional because the warrant "did not comply with the particularity requirement because it did not sufficiently limit the search of the contents of the cell phone by

description of the areas within the cell phone to be searched, or by a time frame reasonably related to the crimes." Id. at 252. Likewise, here, no such descriptions as to content and time were provided in the warrant.

Additionally, as the Mansor Court, supra, explained, "the warrant must identify, as specifically as reasonably possible in the circumstances, the information to be searched for, including, if relevant and available, the time period during which that information was created, accessed, or otherwise used." Id. at 218. This is because our law also recognizes that the police should not be given the discretion to decide, on their own, what to search. See State v. Marshall, 199 N.J. 602 (2009). However, here, the warrants at issue contained no such specifications. Instead, the police relied on their general warrant to conduct a full forensic examination of the phone/ watch/ iPad/ laptop without any nexus whatsoever tying the probable cause to ***all*** of the content contained within these devices for ***all*** of the time that such devices' content has been in existence.

There is no question that the warrants issued here were illegal general warrants. As a result, and because New Jersey does not have a good-faith exception, all evidence obtained must be suppressed. State v. Novembrino, 105 N.J. 95 (1987).

CONCLUSION

For the foregoing reasons and authorities cited in support thereof, the defendant respectfully requests that the evidence seized with a warrant be suppressed as well as any evidence flowing therefrom.

Respectfully Submitted,

/s/ Monika Mastellone
Monika Mastellone, Esq.
Attorney ID No. 122942014

CC: AP Chris Decker; AP Nicole Wallace