PREPARED BY THE COURT

STATE OF NEW JERSEY Plaintiff, v. PAUL CANEIRO Defendant.	SUPERIOR COURT OF NEW JERSEY LAW DIVISION: CRIMINAL PART MONMOUTH Ind. No.: 19-02-283 Case No.: 18-4915 **ORDER**

THIS MATTER having been opened to the court on application of defendant Paul Caneiro (Monika Mastellone, appearing), and opposed by Raymond Santiago, Monmouth County Prosecutor (Christopher Decker and Nicole Wallace, Assistant Prosecutors, appearing), and the court having heard arguments of counsel and for good cause shown;

IT IS on this 10TH day of JULY, 2025;

ORDERED that Defendant's motion to suppress evidence seized pursuant to the search warrants executed on his electronic devices is **GRANTED IN PART** and **DENIED IN PART**.

HON. MARC C. LEMIEUX, A.J.S.C.

NOT FOR PUBLICATION WITHOUT THE
APPROVAL OF THE COMMITTEE ON OPINIONS

SUPERIOR COURT OF NEW JERSEY
COUNTY OF MONMOUTH

Ind. No.: 19-02-283
Case No.: 18-4915

Decided: July 10, 2025

STATE OF NEW JERSEY,

v.

PAUL CANEIRO

Defendant.

FINDINGS AND CONCLUSIONS OF THE COURT ON DEFENDANT'S MOTION TO SUPPRESS EVIDENCE SEIZED WITH A WARRANT

CHRISTOPHER DECKER, ESQ. and NICOLE WALLACE, ESQ., for the State of New Jersey Monmouth County Prosecutor's Office

MONIKA MASTELLONE, ESQ., for Defendant, PAUL CANEIRO

MARC C. LEMIEUX, A.J.S.C.

I. INTRODUCTION

This matter comes before the court by way of Defendant Paul Caneiro's motion to suppress evidence seized pursuant to several search warrants. The Defendant

challenges the validity of the searches conducted on his various digital devices, contending that certain warrants failed to establish probable cause for accessing the full contents and data stored within those devices. He argues that such broad searches amount to unconstitutional general warrants.

Residents of New Jersey enjoy a protected right to privacy under both the Federal and State Constitutions, and that right extends fully to a person's electronic devices. Today's cell phones, tablets, and computers contain the digital equivalent of thousands of pages of personal information. Accordingly, any search of such devices must be supported by a properly issued search warrant, or else must fall within a recognized exception to the warrant requirement.

The State of New Jersey has charged the Defendant with four counts of first-degree murder, two counts of first-degree felony murder, two counts of second-degree aggravated arson, one count of second-degree possession of a weapon for an unlawful purpose, one count of second-degree unlawful possession of a weapon, one count of third-degree possession of a weapon for an unlawful purpose, one count of fourth-degree unlawful possession of a weapon, one count of second-degree theft of movable property, one count of fourth-degree misapplication of entrusted property, and two counts of third-degree hindering the apprehension of oneself. At trial, the State intends to introduce evidence obtained through search warrants executed on

the Defendant's iPhone X, Apple Watch, iCloud Account, iPad, and MacBook laptop.

For the reasons set forth below, the court limits the information retrieved from the Defendant's iPhone X and Apple Watch which may be presented at trial to the data created within a time frame consistent with the probable cause articulated in the affidavits submitted in support of the search warrants for those devices. Additionally, the court finds insufficient facts within the affidavit to authorize a search of "[a]ny and all cellular telephones, computers, laptops, tablets and permission to search same" in the Porsche Cayenne as such affidavit failed to identify with particularity the specific devices expected to be found or articulate probable cause to believe those devices contained evidence of the alleged crimes. Without such particularity and articulable probable case for those devices, the contents of the devices found within the Porsche Cayenne are suppressed.

II. RELEVANT FACTUAL BACKGROUND

On November 20, 2018, at approximately 5:00 AM, police and emergency services responded to a fire at 27 Tilton Drive, Ocean, New Jersey, the home of Defendant Paul Caneiro. A second fire was discovered hours later, at approximately 12:30 PM, at 15 Willow Brook Road, Colts Neck, New Jersey, the home of Defendant's brother, Keith Caneiro. As firefighters worked to extinguish the flames and investigate the origin of the fire at Keith Caneiro's residence, they identified four

deceased victims at the scene: Keith Caneiro, Jennifer Caneiro, [redacted] and [redacted].

By the following day, November 21, 2018, law enforcement had charged the Defendant with aggravated arson, alleging that he had intentionally set fire to his Tilton residence. On November 29, 2018, the State filed additional charges against the Defendant, including aggravated arson, four counts of murder, and other related offenses in connection with the fire and deceased victims at the Willow Brook home. A grand jury subsequently indicted the Defendant on these charges in February 2019.

The State applied for, and obtained, multiple search warrants throughout this investigation. These warrants authorized the search of physical property, various electronic devices, and digital accounts alleged to belong to the Defendant, including an: (1) iPhone X; (2) Apple Watch; (3) iCloud account; (4) iPad; (5) Apple MacBook laptop; and (6) the Defendant's home and vehicles.

The Defendant contests the validity of some, but not all, of the issued warrants and the resulting searches. First, he asserts that the warrants for the iPhone and Apple Watch erroneously authorized law enforcement to seize "any and all" information from these devices without probable cause to support the search of the entire con-

tents. Next, with respect to the iPad and MacBook laptop, he asserts that these devices were erroneously searched under a broad authorization to search any computers or devices found in Defendant's home, cars, or businesses.

Finally, the Defendant challenged the iCloud warrant. During oral argument, however, the Defendant clarified that he does not challenge the validity of the iCloud warrant itself. However, he objects to the use of information obtained pursuant to that warrant that falls outside the temporal scope authorized. The parties and the court agree that any information obtained from the iCloud account that exceeds the temporal limitation of November 1, 2018, to November 20, 2018, as set forth in the warrant, is inadmissible at trial. Accordingly, there is no need to further address the filed challenge to the iCloud warrant in this opinion.

a. Warrants for Defendant's iPhone X

On November 21, 2018 Det. Brian Weisbrot submitted an affidavit ("Weisbrot affidavit") to the Honorable James McGann, J.S.C., in support of an application for a search warrant for the Defendant's home; his vehicles; the contents of any computers, phones, or tablets found during the search; and Defendant's iPhone X, which was in the Monmouth County Prosecutor's Office's possession at the time. Def. Exhibit D at 11. The Weisbrot affidavit described the make, model, and serial number of the Defendant's iPhone X, the location of Defendant's home, 27

Tilton Drive, and the makes, models, and registration numbers of the Defendant's family vehicles with particularity. Def. Exhibit D at 6.

The Weisbrot affidavit includes facts that "establish the grounds for this application and the probable cause of [his] belief" that 27 Tilton Drive, the Porsche Macan, the Porsche 911 Carrera, Jeep Wrangler, Porsche Cayenne, and iPhone X contained evidence of a crime. Def. Exhibit D, at 7. Paragraph a of part 8 of the Weisbrot affidavit details his professional background and experience. Paragraphs b and c detail the initial response to the fire at Defendant's home, the responding officer's reported first impressions of the scene, and the occupants of 27 Tilton Drive. The affidavit then details specific facts and evidence recovered at the scene:

> d) A red colored gasoline gas [sic] can was located on the driveway, in close proximity to a white colored Porsche Macan, bearing NJ registration [redacted]. The aforementioned vehicle had brown staining on the hood, indicative of likely spot pour burn patterns. A charred rubber glove was located on the ground in front of the aforementioned Porsche and garage door that was burned.
>
> e) Paul Caneiro was determined to be the operator of the white colored Porsche Macan bearing NJ registration [redacted], which was parked in the driveway. The vehicle was determined to be a loaner car from the Monmouth Porsche car dealership as Paul's vehicle was being serviced.
>
> f) A storage shed was located in the back yard of the property. The shed was determined to have a rear door, which was unlocked. Located inside the shed were three (3) gasoline cans. The first two gasoline cans were in line with a space separating them from the third gasoline can indicating that a fourth can had been there and was removed. The gasoline can located on the driveway is believed to be the can that was removed from the shed. Rubber gloves were also located inside and outside the shed.

[Paragraphs g and h detail the presence of exterior video surveillance cameras on Defendant's residence, and describe the last recorded activity found on the system's DVR. Because Defendant has challenged the admission of this evidence separately, the court does not include the verbatim contents of these paragraphs.]

[Paragraphs i and j detail the location of butane lighters found within the home, the points of origin of the fire, and the presence of unknown combustible liquids. Paragraph k) describes the vehicles owned by Defendant's family, their registration information, and a description of each. Paragraph l) describes the location of a gun safe and states that Defendant has multiple firearms registered in his name.]

m) Seized from the person of Paul Caneiro was one Apple iPhone X, black in color. The serial number is G6TWVEBLJCL8. The phone is currently located at the Monmouth County Prosecutor's Office located at 132 Jerseyville Avenue, Freehold, New Jersey 07728. Your affiant has probable cause to believe that evidence of the crime of Aggravated Arson and other related crimes exists within the phone.

[Def. Exhibit D at 7-10 (emphasis added).]

Paragraphs o and p follow shortly after paragraph m's mention of "other related crimes," and note that a vehicle was recorded leaving Defendant's home in the early morning hours, and that the Willow Brook Road fire was reported approximately 7 hours after the Tilton Drive fire:

o) Members of the investigative team traveled to 30 Tilton Drive and reviewed video surveillance recordings maintained at the home. A review of those recordings revealed that on November 20, 2018, at 2:07 AM, a white colored SUV believed to be a Porsche is observed driving past the residence heading towards Green Grove Road. A further review of those recordings revealed the same vehicle returning to Tilton Drive and driving towards [27 Tilton Drive] at 4:08 a.m. No vehicles are seen leaving the area at or around the time of the [27 Tilton Drive] fire.

p) It should also be noted that, at approximately 12:33 p.m. on November 20, 2018, Colts Neck Police were dispatched to a fire at 15 Willow Brook Road, Colts Neck. During the course of fire suppression efforts,

> four individuals were found deceased at the residence. These individuals were Paul Caneiro's brother, sister-in-law as well as his niece and nephew, ages 8 and 10. The deaths are currently pending autopsies, but significant trauma was noted.
>
> [Def. Exhibit D at 10.]

Paragraph r of the affidavit also references these "other related crimes" as follows:

> r) Your affiant has probable cause to believe that evidence of the crime of Aggravated Arson and other related crimes will be found within the residence and curtilage at 27 Tilton Drive, Ocean Township, NJ as well as within the vehicles, which were all located at the residence at the time of the fire. In addition, your affiant has probable cause to believe that evidence relating to these crimes is located within Paul Caneiro's Apple iPhone X. Your affiant knows that these devices contain a variety of information including but not limited to call history, text detail records, applications as well as significant information relating to location of the device at the time that it's being accessed.
>
> [Def. Exhibit D at 11. (emphasis added)]

The affidavit does not mention homicide as a specific "other related crime," but the warrant application mentions in several other places that they were seeking "evidence immediately apparent as being relevant to . . . the deaths at 15 Willow Brook Road, Colts Neck." Def. exhibit D at 3.

Judge James McGann, J.S.C. issued the search warrant on November 21, 2018, at 12:25 P.M. The search warrant issued by Judge McGann to search the electronic devices did not include a temporal limitation for the content to be seized within the electronic devices. Def. Exhibit E at 1-2.

Later that day on November 21, 2018, Det. Andrea Tozzi submitted an affidavit ("Tozzi 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. Def. Exhibit A. On November 21, 2018, Judge Joseph Oxley, J.S.C., signed the CDW. Def. Exhibit B. The warrant permitted investigators to search for the following types of data within the time period of November 6, 2018 to November 20, 2018: subscriber information; incoming and outgoing calls; SMS and MMS messages, email detail records and cell site/location information (CSLI) for same; IP detail records and packet data with CSLI for same; stored photographs and video with location information (without audio); and all other location information for the aforementioned data. Def. Exhibit B.

The Tozzi affidavit included the grounds for the application and facts necessary to determine probable cause. Def. Exhibit A at 4. Paragraph a establishes Det. Tozzi's qualifications and experience before and after joining the MCPO. Paragraphs b through l are identical to the Weisbrot affidavit. Starting with paragraph m, the facts attested differ. In pertinent part, the Tozzi affidavit states the following:

> m) Seized from the person of Paul Caneiro was one Apple iPhone X, black in color. The serial number is G6TWVEBLJCL8. During the course of this investigation, the cellular telephone number for the aforementioned phone was identified as [redacted], whose service provider was identified as T-Mobile. The phone is currently located at the Monmouth County Prosecutor's Office located at 132 Jerseyville Avenue, Freehold, New Jersey 07728.

[. . .]

[Paragraph o details the information gathered from viewing the surveillance camera footage at the nearby residence of 30 Tilton Dr. It attests that a "white colored SUV" believed to be Defendant's vehicle can be seen departing from and returning to Defendant's residence. Paragraphs p through u detail the discovery and subsequent investigation of the homicides and fire at Keith Caneiro's residence, and specifically state that the victims suffered gunshot and stab wounds. Paragraph v asserts that Defendant and Keith owned two businesses together.]

[Def. Exhibit A at 4-9.]

Based upon the above information, Det. Tozzi submitted that she had probable cause to believe:

> w) ...that the phone records maintained by T-Mobile for [redacted] and/or the phone records maintained by T-Mobile for [redacted] contain evidence of the crimes under investigation, specifically murder, aggravated arson, possession of a firearm, possession of a firearm for an unlawful purpose, unlawful possession of a weapon and possession of a weapon for an unlawful purpose, contrary to the provisions of N.J.S.A. 2C: 11-3, 2C: 17-1, 2C:39-4, and 2C:39-5. As noted above, the records will assist in determining whether Paul Caneiro and Keith Caneiro had any relevant/significant communications and/or contact in the weeks leading up to and including November 20, 2018. Additionally, the information contained in the records of WYZE and Nest surveillance systems will assist detectives in determining what transpired both inside and outside of the residence of 15 Willow Brook Road at the time of and leading up to the homicides.
> [Def. Exhibit A at 8 (emphasis added).]

The CDW entered by the court, after review of the Tozzi affidavit, stated the following:

> There has been and now is located certain property pertaining to account activity which constitutes evidence of a crime or tends to show a

violation of the penal laws of the State of New Jersey, including but not limited to the following:

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;

1. 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 [redacted] during the time period of November 6, 2018 up to and including November 20, 2018.

[Def. Exhibit B at 1-2.]

A second CDW was obtained on November 26, 2018, for more detailed data from the same phone number. Def. Exhibit C at 1. This CDW covers the smaller time frame of November 19, 2018 to November 20, 2018. Def. Exhibit C at 1-2.

b. Apple Watch

On December 19, 2018, Det. Patrick Petruzziello submitted an affidavit in support of an application for a CDW for the T-Mobile records pertaining to cell phone number, [redacted]. Def. Exhibit G at 1. Det. Petruzziello's affidavit makes specific mention of Paul Caneiro's Apple Watch. This affidavit requested a warrant for the following:

> [. . .]
>
> 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, Internet activity, and data transactions 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;
1) 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 "pel 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 [redacted] 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 [redacted] during the time period of November 19, 2018 up to including November 20, 2018.

[Det. Exhibit G at 1-2.]

Det. Petruzziello's affidavit lists the following regarding the Apple Watch:

m) Additionally, during the search of the aforementioned Porsche Cayenne, an Apple watch more specifically described as a black 42 millimeter series 3 watch, with a black band, was located in the center console of the vehicle.

[Def. Exhibit G at 5.]

Judge Oxley signed the CDW on December 19, 2018. Def. Exhibit H at 2. The warrant authorized a search and seizure of data from November 19, 2018 to November 20, 2018. Def. Exhibit H at 1-2.

On December 19, 2018, Det. Petruzziello also applied for and was granted a search warrant for the Apple Watch itself, based on an affidavit containing the same facts as the CDW. Def. Exhibit I at 1. The affidavit requested a warrant to search the Apple Watch for and subsequently seize the following evidence:

> 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 drat 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.
>
> [Def. Exhibit I at 1-2.]

The Petruzziello affidavit states the facts and grounds for a determination of probable cause as follows: Paragraph a details Det. Petruzziello's qualifications and experience prior to and after joining the Monmouth County Prosecutor's Office. Paragraphs b though k are identical to the Tozzi affidavit supporting the initial CDW for Defendant's iPhone. Compare Def. Exhibit I with Def. Exhibit A. From there, the affidavits diverge: Det. Petruzziello's affidavit incorporates information gathered during the earlier search of the Defendant's residence, vehicles, and devices. It specifically mentions the Apple watch in two paragraphs:

m) Additionally, during the search of the aforementioned Porsche Cayenne, an Apple watch, more specifically described as a black 42 millimeter series 3 watch, with a black band, was located in the center console of the vehicle.

. . .

qq) Additionally, upon review of the aforementioned cell phone extraction of Paul Caneiro's cell phone, four incoming text messages from Keith Caneiro's cell phone to Paul Caneiro's cell phone were revealed. All were sent between the hours of 3:14 a.m. and 3:18 a.m. on November 20, 2018, approximately four minutes after the report of shots fired in Colts Neck. A review of the previously obtained records for Keith Caneiro's cell phone identified several entries that were listed as both incoming and outgoing with Paul Caneiro's telephone number [redacted] Keith Caneiro's telephone number [redacted] and a third number identified as [redacted] for the time period listed above. On December 17, 2018, your affiant issued a grand jury subpoena to T-Mobile to obtain subscriber information for [redacted]. The results indicated that the aforementioned number is associated with Paul Caneiro, and was effective July 4, 2018. Additionally, the subscriber information identified the rate plan as being associated with an Apple watch. Your affiant reviewed the previously obtained records associated with Paul Caneiro's Apple ICloud account, which identified an Apple watch that was purchased on July 4, 2018 in the name of Paul Caneiro. The watch was more specifically identified as a series three, which has a built in cellular feature.

[Def. Exhibit I at 5, 11-12.]

The affidavit further detailed that Det. Petruzziello was aware that "computers, cell phones, and other electronic storage devices . . . generally can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file

names." Def Exhibit I at 12. It noted that "in order to fully retrieve data from a computer or other digital communications system, the analyst will need access to all storage media and devices that were or may have been used by the suspect." Def. Exhibit I at 12.

Based on Det. Petruzziello's December 19th affidavit, a search warrant for the Apple Watch was issued by Judge Joseph W. Oxley, J.S.C. Def. Exhibit J at 2. It contained no temporal limitations. Def. Exhibit J at 1-2.

c. iPad and MacBook Laptop

The Weisbrot affidavit, submitted on November 21, 2018, was submitted in support of a search of Defendant's Porsche Cayenne. Def. Exhibit D at 5. In this warrant, the State sought to seize, and subsequently search, certain property located within the Porsche Cayenne including:

> 3) Any and all cellular telephones, computers, laptops, tablets **and permission to search same** pursuant to this warrant;
>
> [Def. Exhibit D at 6 (emphasis in original).]

A search warrant for the Porsche Cayenne was issued on November 21, 2018, by the Honorable James J. McGann, J.S.C. Def. Exhibit M at 2. This warrant permitted the search of "[a]ny and all cellular telephones, computers, laptops, tablets and permission to search same pursuant to this warrant." Def. Exhibit M at 1. After

searching the Porsche Cayenne, police officers found an Apple MacBook laptop, an iPad, and an Apple Watch[1].

III. SUMMARY OF ARGUMENTS

a. Defendant's Position in Support of Suppression

The Defendant asserts that search warrants may not authorize the unrestricted search and seizure of all data on a cell phone. He contends that a warrant must be "limited in scope by date range, category of data, and/or other filter that is factually related to the probable cause" asserted in the supporting affidavit.

According to the Defendant, the evidence obtained from the iPhone X, Apple Watch, iPad, and Apple MacBook laptop must be suppressed because the warrants issued were impermissibly general and authorized an unrestricted search of each device's entire contents. He further argues that all such data must be excluded because New Jersey does not recognize a good faith exception to the warrant requirement.

The Defendant relies on the Fourth Amendment of the United States Constitution and Article I, Paragraph 7 of the New Jersey Constitution, both of which prohibit the issuance of warrants except upon a showing of probable cause, supported by oath or affirmation, and require that the place to be searched and the items to be seized be particularly described. The Defendant emphasizes that this "particularity"

---

[1] As discussed, *infra*, a separate search warrant for this Apple Watch was issued. Def. Exhibit J.

requirement serves to prohibit general seizures and to guard against broad, exploratory searches.

In support of his position, the Defendant cites State v. Missak, 476 N.J. Super. 302 (App. Div. 2023), arguing that New Jersey courts have recognized that a warrant authorizing the search of an entire cell phone without limitation constitutes an impermissible general warrant.

He submits that the search warrants issued for his iPhone, Apple Watch, iPad, and Apple MacBook are precisely the kind of overbroad instruments that the Missak court and others have deemed unconstitutional. Specifically, he contends that the warrants allowed law enforcement to seize "any and all" information from the devices without establishing probable cause to search and seize the entirety of the data contained within them.

The Defendant also alleges that the iPad and Apple MacBook were improperly included in search warrants that were issued for the Defendant's home, car, and business address. He argues that the language used in those warrants conferred unfettered discretion upon law enforcement to search the contents of those devices, thereby effectively rendering them invalid.

At oral argument, the Defendant asserted that "a bad warrant is a bad warrant," and that it is not the court's role to cure constitutional deficiencies in warrant applications. Nevertheless, he acknowledged that remedies short of total suppression are available to the court.

b. State's Opposition to Suppression

The State opposes the motion and urges the court to find that the search warrants at issue were supported by sufficient probable cause and described the items to be seized and the places to be searched with adequate particularity. The State argues that suppression is unwarranted and that the burden of proving the invalidity of a warrant rests with the Defendant. According to the State, the Defendant must demonstrate either that the issuing court lacked probable cause or that the resulting search was otherwise unreasonable.

The State acknowledges that the court in Missak invalidated a warrant authorizing an expansive search of all data on a seized phone due to insufficient probable cause. However, the State distinguishes the present case by asserting that the supporting affidavits in this matter articulated specific facts establishing probable cause.

The State maintains that the investigation involved arson and related offenses, and that officers had reason to believe evidence connecting the Defendant to those crimes would be found on his electronic devices over a broad timeframe.

The State argues that the Fourth Amendment does not demand perfect precision in describing the data to be searched or seized. It notes that digital files often overlap and are dispersed across a device, which complicates efforts to isolate particular categories of information. Accordingly, the State contends that the particularity requirement must be interpreted flexibly in the context of electronic data, similar to paper document searches where incidental exposure to unrelated information is both inevitable and permissible.

The State concludes that a search warrant is not deficient merely because it is broad, and that breadth alone does not transform an otherwise lawful warrant into a prohibited general warrant.

At oral argument, the State opposed any limitation of the search warrants. However, if the court were to impose temporal limits, the State requested that data retrieved from the iPhone X be limited to the period of November 6, 2018, to November 20, 2018, and that data from the Apple Watch be limited to July 4, 2018,[2] through November 20, 2018.

IV. LEGAL STANDARD

"The touchstone of the Fourth Amendment and Article I, Paragraph 7 of the New Jersey Constitution is reasonableness." State v. Hathaway, 222 N.J. 453, 476

---

[2] The Apple Watch was purchased on July 4, 2018.

(2015). The inquiry as to whether a search was reasonable applies equally to the issuing of a warrant, the execution of the warrant by police, and the subsequent search of items seized. State v. Chippero, 201 N.J. 14, 27 (2009); State v. Watts, 223 N.J. 503, 514 (2015); Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976). Generally, a search conducted without a warrant based on probable cause is considered *per se* unreasonable, unless there is a recognized exception to the warrant requirement. See State v. Hempele, 120 N.J. 182, 217 (1990); Riley v. California, 573 U.S. 373, 382 (2014). A search conducted under an improperly obtained or general warrant is similarly unreasonable. State v. De Simone, 60 N.J. 319, 322 (1972).

A general warrant is one that gives "no guidelines to the officer as to what kind of items [are] to be seized" but rather "delegate[s] to him the function of deciding" if any particular item fits the bill. State v. Muldowney, 60 N.J. 594, 600 (1972). "The evil inherent" in such a warrant is that it "leaves the protection of the constitutional rights afforded the person to be searched to the whim of that officer." Ibid.

To combat this evil, both the Fourth Amendment of the United States Constitution and Article I, Paragraph 7 require 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. A neutral judicial officer must evaluate the warrant application and be satisfied that

there is "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." State v. Sullivan, 169 N.J. 204, 210 (2001).

Probable cause is a "flexible, nontechnical concept." State v. Kasabucki, 52 N.J. 110, 116 (1968). While eluding precise definition, probable cause is "less than legal evidence necessary to convict though more than mere naked suspicion." State v. Mark, 46 N.J. 262, 271 (1966). It is a "suspicion of guilt that is well-founded; a reasonable basis for a belief that a crime has been or is being committed." Kasabucki, 52 N.J. at 116. The approach to evaluating a police officer's affidavit must be practical and realistic. Id. at 117. Few police officers have legal training, but the specialized experience and "work-a-day" knowledge that a police officer has is valuable. Id. In keeping with this sentiment, "New Jersey has adopted a totality-of-the-circumstances test to determine whether warrants are based on probable cause." State v. Gathers, 234 N.J. 208, 221 (2018).

Once probable cause is established, the warrant issued must describe the place to be searched and the things to be seized; directionless and discretionary searches are prohibited. State v. Feliciano, 224 N.J. 351, 366 (2016). "The particularity requirement, in general, 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." Ibid. (quoting State v. Marshall, 199 N.J. 602,

611 (2009)). Particularity requires "reasonable accuracy, [not] pin-point precision." State v. Wright, 61 N.J. 146, 149 (1972) (finding that the search warrant was not inaccurate in its failure to state the apartment number to be searched, as the warrant stated that the intended apartment was the one defendant resided in). The underlying reason for the particularity requirement is to require an "adequate description of the premises in a search warrant" to "prevent the police officer from entering property which he has no authority to invade." Id.

Warrants that preemptively authorize a search after satisfying a future condition not yet known at the time of the warrant's issuing may also be found invalid. In Marshall, a search warrant, which did not specify which apartment within a particular building was to be searched but rather permitted search of an apartment "if and only if" the suspect possessed documentation or keys to that specific unit or otherwise divulged the information, was held invalid because the role of the magistrate was "delegated to the police." Marshall, 199 N.J. at 613. The Court also found that a warrant containing instructions for further investigation or conditions to be met also cannot be supported by probable cause within the "four corners of the affidavit." Ibid. "[T]he probable cause determination must be made based on the information contained within the four corners of the supporting affidavit, as supplemented by sworn testimony before the issuing judge that is recorded contemporaneously." Marshall, 199 N.J. at 611 (quoting Schneider v. Simonini, 163 N.J. 336, 363 (2000)).

The particularity requirement applies not only to the places to be searched, but to what kinds of items may be seized. The warrant need not give "a minute and detailed description of the items to be seized. . . [b]ut the warrant must be sufficiently definite so that the officer executing it can identify the property sought with reasonable certainty." Muldowney, 60 N.J. at 600. When searching through digital evidence, such as cell phone data, the warrant should still specify the particular content sought in order to avoid a "fishing expedition." State v. Andrews, 243 N.J. 447, 481 (2020) (quoting United States v. Hubbell, 530 U.S. 27, 47 (2000)).

a. Validity

"A search based on a properly obtained warrant is presumed valid." Sullivan, 169 N.J. at 211. 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. at 317. A defendant has the burden to establish a warrant's invalidity, and must prove that there was no probable cause to support the issuance of the warrant. Keyes, 184 N.J. at 554; Missak, 476 N.J. Super. at 317. The court must limit its review of the validity of the warrant to the four corners of the document. Id. at 308 (noting that since the defendant is challenging the validity of the search warrant, the court must limit the summary of facts to the four corners of the certification.) Alongside the consideration of

the four corners, the court must also apply fundamental tenets of constitutional law to decide the validity of the warrant. Id. at 319.

When a trial court considers a motion to suppress evidence obtained based upon a search warrant, the court owes substantial deference to the issuing judge. See Kasabucki, 52 N.J. at 117. Another "trial judge of equal jurisdiction should regard as binding the decision of [a counterpart judge] that probable cause had been sufficiently shown to support a warrant, unless there was clearly no justification for that conclusion." Ibid.

New Jersey does not recognize the good-faith exception to the exclusionary rule. See, e.g., State v. Boone, 232 N.J. 417, 430 (2017). The court also cannot retroactively modify the language contained within a search warrant to bring it within the bounds of probable cause, but a court can sever unreasonable portions of a warrant to preserve those that are supported by probable cause. The redaction or severability principle "ensures that 'the suppression order will be commensurate with the deficiency of probable cause' and that the 'policy behind the exclusionary rule is served but not exalted.'" 2 Wayne R. LaFave, Search and Seizure § 3.7(d) (6th ed. 2024) (quoting People v. Hansen, 339 N.E.2d 873, 875 (N.Y. 1975)). This principle has been applied to cases where items were seized outside the scope of an otherwise valid warrant, State v. Dye, 60 N.J. 518 (1972), and to overbroad warrants where

items were seized in places the warrant identified with probable cause, State v. Burnett, 232 N.J. Super. 211 (App. Div. 1989).

Dye applied "the common sense judicial approach . . . that only to the extent that the interception includes irrelevant communications should it be deemed an unreasonable search and seizure." Id. at 540-41. The Court explained, "where articles of personal property are seized pursuant to a valid warrant, and the seizure of some of them is illegal as beyond the scope of the warrant, those illegally taken may be suppressed . . . but those within the warrant do not become so tainted . . . ." Id. at 537.

In Burnett, the trial court issued a warrant to search the business records of a dentist suspected of receiving kickbacks. The appellate court held the warrant, authorizing ten years of records, to be overbroad. Id. at 216. The evidence establishing probable cause to believe the dentist was receiving kickbacks was of recent vintage and the affidavit supporting the warrant included no evidence of when the dentist started performing services for union members. Ibid. Following the redaction principle, the court rejected the "defendant's contention that the entire warrant should be suppressed because of its overly broad authorization to seize records encompassing the ten-year period." Ibid. Instead, the court held that the "[d]efendant's constitutional rights were amply protected by reducing the excessive period of ten years to

a more reasonable period consistent with the facts set forth in the supporting affidavit," which was one year. Id. at 217.

Even if a warrant is deemed invalid, suppression also may not be warranted when evidence was also discovered "by means wholly independent" of the invalid warrant. Nix v. Williams, 467 U.S. 431 (1984). While the independent source doctrine "cannot sustain what otherwise was an impermissible search," the same evidence, found in another location and obtained through a subsequent valid warrant "is not automatically inadmissible." State v. Holland, 176 N.J. 344, 348, 355 (2003); compare State v. Hunt, 91 N.J. 338 (1982) (improperly obtained telephone records did not justify suppression of evidence found pursuant to later search warrant) with State v. Ravotto, 169 N.J. 227 (2001) (blood sample, forcibly drawn from defendant, not discoverable under independent source doctrine when there was nothing to indicate hospital staff would have drawn blood anyway).

b. Search Warrants for Electronic Devices

Searching a suspect's cell phone, even if seized incident to their arrest, requires a warrant. Riley, 573 U.S. at 403. Modern smartphones allow individuals to have far greater quantities of personal information on their persons than would be otherwise possible. Id. at 386. The information an individual stores on their phone also stretches back far further in time than they would generally keep on their person,

thus exposing years of private information to potential search. Id. at 394. These realities "implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." Ibid. Presently, most American adults always have a cell phone on their person, and that phone is steadily recording information about every aspect of their lives. Id. at 395. While this information is not "immune from search," the privacy implications inherent in accessing that much data are best protected by requiring a search warrant, even if the phone was properly seized without one. Id. at 401.

The files on a cell phone are not the only information within the protections of the Fourth Amendment; New Jersey residents also have a recognized privacy interest in the automatically generated and broadcasted information connected to those phones under both the State and Federal Constitutions. Carpenter v United States, 585 U.S. 296 (2018); State v. Earls, 214 N.J. 564, 568 (2013). Stored electronic communications, including phone logs, location data, and text message data can be obtained from a service provider only following the issuance of a valid warrant. N.J.S.A. 2A:156A-29. The holding in Carpenter was explicitly narrow and stood only for the proposition that a warrant is required before government agents access historical cell tower information; it does not apply to other features of cell phones or other types of surveillance or location data. Carpenter, 585 U.S. at 316. The New Jersey Constitution, however, affords greater protection and requires a warrant for

most types of cellular data, as cell phones are an "indispensable part of modern life." Earls, 214 N.J. 586

There is no hard and fast rule as to how far back a warrant for cell phone location data can reach. State v. Finesmith, 408 N.J. Super. 206, 213 (App. Div. 2009) (noting that the time frame requested should not be arbitrary). Warrants for locally stored data also do not generally require a date range, though Missak does draw a connection between the date ranges contemplated in a warrant and the probable cause requirement. 476 N.J. Super at 319-320.

Technology is constantly evolving, and with it the concepts of privacy interests for search warrants must evolve with it. Drawing in part on Riley and Carpenter's acknowledgement that cell phones have unique properties, Missak addressed the extent of probable cause required to authorize the search of the contents of a suspect's cell phone after it is secured subsequent to arrest. In Missak, the issue before the Appellate Division was the degree of probable cause required to search the entire contents of a cell phone. The case arose from a search warrant issued to examine the defendant's phone for evidence related to alleged crimes committed on December 8 and 9, 2021. Missak, 476 N.J. Super at 308. The warrant was supported by a certification asserting that the phone might contain evidence of the defendant's possession and use of the device during that two-day period. However, the court found that the certification failed to establish probable cause for an expansive search

of all data on the phone and could not justify a search for information predating the alleged crimes or for information unrelated to the offenses charged. Id. at 319. The court emphasized that their decision was based on a finding that "the search warrant's authorization for the State to search all the phone's contents, information, and data [was not] supported by probable cause." Ibid.

In Missak, police "expressly sought the search warrant for evidence of the crimes of luring and attempted sexual assault he allegedly committed on December 8 and 9, 2021, . . . establishing only probable cause to search the phone for evidence pertaining to those offenses." Missak, 476 N.J. Super. at 318. The court found that since the police knew the defendant had never had contact with the undercover special agent, acting as a 14 year old girl, outside specific dates, there was no reason to believe communication between the two would be found outside those dates. Id. at 320-22. The affidavit made vague assertions that defendant "may" have renamed files or hidden them in other areas on the phone, but gave no details to support probable cause that anything related to the crimes alleged in the affidavit would be found elsewhere on the phone. Id. at 320-21. The Appellate Division found that the State's affidavit did not meet the "constitutional mark" as probable cause requires more than just what "may" occur. Id. at 321.

Finding the warrant before them was sufficiently particular in describing its scope but lacked the necessary facts to justify that scope, the Appellate Division

reversed and quashed the warrant. Id. at 302. But, the Appellate Division noted that the State was "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." Id. at 323.

Taking the holdings and observations of Riley, Carpenter, and Missak together, it is clear that smartphones, laptops, and computers are not mere containers subject to inspection, like a file cabinet or a desk drawer. Pretending that these devices are mere containers for information is "like saying a ride on horseback is materially indistinguishable from a flight to the moon." Riley, 573 U.S. at 393. Their massive capacity to store personal information and their flexibility of use mean that there is not only a wider variety of information stored within them (pictures, videos, and text are all commonly found within a smartphone or computer), but also that data can be stored for so much *longer* than an analog medium. In fact, a laptop or smartphone can, and often does, contain files that are older than the device itself. It is also possible to filter this information in so many more ways: while files are not always properly labeled, metadata allows for many details about the content and creation of a file to be discovered.

The aforementioned cases make many astute observations about technology's place in the modern world and are all in agreement that electronically stored information (ESI) contained within a smartphone or computer will generally require a warrant. The overarching rule distilled from Riley, Carpenter, Missak, Earls, and their progeny is not that obtaining the warrant is a mere perfunctory step: those warrants need to connect the amount and type of ESI sought to the probable cause. ESI warrants that are too broad by location,[3] timeframe,[4] or type of data[5] will all fail to pass constitutional muster. There is no requirement to strictly limit timeframes or categories, and no justification for forcing the state to arbitrarily limit their requests: the rule is simply that the scope of the search must match the facts asserted. Compare Finesmith, 408 N.J. Super. at 213 (CDW should not be arbitrarily limited to two weeks when "the State seeks to show a pattern of use" spanning a year or more) with Facebook v. State, 254 N.J. 329, 367 (2023) (CDWs and search warrants alike

---

[3] United States v. Smith, 110 F.4th 817, 838 (5th Cir. 2024) (geofence warrants, which reveal the location data of every device detected in a certain area, are "highly suspect per se").

[4] Carpenter, 585 U.S. at 314-15 (the "exhaustive chronicle of location information" that cellphones create "implicates privacy concerns" beyond those of regular phone records); See also Burnett, 232 N.J. Super. at 217 (warrant could not support search of records for an "excessive period of ten years" without tying the facts in the affidavit to that timeframe) and Riley, 573 U.S. at 394 ("the data on a phone can date back [beyond] the purchase of the phone").

[5] Riley, 573 U.S. at 394 ("a cell phone collects in one place many distinct types of information"); State v. Dye, 60 N.J. at 537 (non-relevant telephone recordings are outside scope of an otherwise valid wiretap warrant); see also United States v. Winn, 79 F. Supp. 3d 904, 919 (S.D. Ill. 2015) ("Obviously, the police will not have probable cause to search through and seize [every piece of data that could conceivably be found] every time they search a cell phone.").

should not be applied too broadly or prospectively, but must follow the "traditional assertion that probable cause to search . . . exists at the moment the warrants are signed").

Missak acknowledges this fact, and this court applies those principles to the issue at hand today. Since it is possible to narrow down and filter through the vast universe of ESI contained in modern devices, it is entirely reasonable to expect a search warrant to either articulate some boundaries for the ESI sought or articulate why probable cause supports the total removal of those boundaries and authorizes searching the equivalent of thousands of pages of documents. In order for the State to access the entirety of a device, they must offer facts that show a fair probability that the entirety of the device is relevant; or, facts that show the information they seek is concealed, spans a wide timeframe, or otherwise establish that it will be found elsewhere on the device.

In sum, the scope of a digital device search is Constitutionally reasonable only to the degree that the supporting affidavit's facts establish a fair probability that evidence relevant to the crime under investigation would be found in that particular data or within the particular time frame at issue. The Constitution prohibits authorizing exploratory or open-ended searches of electronic devices, absent this justification. See N.J. Const. art. I, ¶ 7; Riley, 573 U.S. 373; Carpenter, 585 U.S. 296 (2018); Earls, 214 N.J. 564; and Missak, 476 N.J. Super. 302.

V. ANALYSIS

The issue before this court is therefore whether these warrants authorize the search of the *entire contents* of Defendant's iPhone X, Apple Watch, iPad, and Apple MacBook laptop.[6] Since the iPhone and Apple Watch and the information sought from them were described with particularity and their searches were explicitly authorized by their respective warrants, the only question is whether the probable cause established supported the breadth of the search conducted. Since the iPad and MacBook laptop were not described with particularity, the question turns on whether the warrant in question authorized the search of *any* computer that may have been found in the places described therein.

The court does find the facts of this case to be distinguishable from Missak, as that case dealt with crimes occurring over a two-day period, where the Defendant and the alleged victim met online and had no contact or relationship prior to those two days. This case deals with crimes allegedly occurring over weeks and months, and the relationship between the Defendant and the victim was not only lifelong but was significantly entangled. Nevertheless, the Defendant has Constitutional protections against unreasonable searches, and the court must determine whether probable

---

[6] The court is mindful of the need to show deference to the findings and conclusions made by the prior judges in issuing these warrants. All the warrants in question, however, were issued prior to the decision in State v. Missak, or the unpublished cases cited to by Defendant which further discuss the principles in Missak. This Court has the benefit of guidance not available to Judges Oxley and McGann at the time and must take that guidance into consideration.

cause and particularity exist independently for the individual search warrants in order for the State to have access to the contents of these electronic devices and accounts.

This case is also procedurally dissimilar to Missak, as the Defendant in Missak filed a motion to quash before the warrant in question was ever executed. Given the timing of the application, the Appellate Division was able to fashion a remedy that protected Missak from a warrant that far exceeded its underlying probable cause, but did not prejudice the State from submitting a properly tailored warrant application. In this case, it is far too late; the State has already conducted their search of Defendant's iPhone X, Apple Watch, iPad, and laptop. The remedy of a new warrant is unavailable, but outright suppression does not serve the purposes of the exclusionary rule. Limiting the warrant's scope, however, properly and fully protects Defendant's constitutional rights, respects the presumption of validity and the deference to the issuing judges required of this court, and places the State in the same position they would be left in, were the remedy from Missak available.

In limiting the scope of the warrants to the extent they are supported by probable cause, this court is guided by the Supreme Court's holding in State v. Dye, and the Appellate Division's subsequent opinion in State v. Burnett.

In Dye, the defendant challenged a wiretap order as overly broad because it authorized the interception of telephone conversations that were unrelated to the underlying offense of bookmaking. In affirming the defendant's conviction, the Supreme Court noted:

> [W]here articles of personal property are seized pursuant to a valid warrant, and the seizure of some of them is illegal as beyond the scope of the warrant, those illegally taken may be suppressed, or excluded at the trial, but those within the warrant do not become so tainted as to bar their receipt in evidence.
>
> [60 N.J. at 537.]

Similarly, in Burnett, the defendant dentist argued that a warrant authorizing seizure of patient billings and other records from his office over a ten-year period was too broad. Rather than suppress all the evidence seized, the Appellate Division held that the appropriate remedy was to redact the warrant to a reasonable period consistent with the probable cause established by the supporting affidavit. 232 N.J. Super. at 216-17. According to the court:

> Defendant's constitutional rights are amply protected by reducing the excessive period of ten years to a more reasonable period consistent with the facts set forth in the supporting affidavit . . . The proper remedy is redaction, the striking of those portions of the warrant which are invalid for want of probable cause, and preserving those severable portions that satisfy the Fourth Amendment, and our state constitutional counterpart.
>
> [Ibid. (internal citations omitted).]

Balancing these principles with the binding authority of Missak, the path before this court is clear: the warrants must be individually examined and the items and locations searched narrowed to conform with the probable cause articulated within each individual affidavit.

For each search warrant, this court must find that the search warrant affidavits establish probable cause to search the "specific location or that evidence of a crime is at the place sought to be searched." Sullivan, 169 N.J. at 210. Acknowledging that police do not have special legal training, and that common-sense understanding of the world should inform any analysis of whether the facts alleged in an affidavit support a given conclusion, the court must determine if probable cause has been met by looking at the totality of the circumstances. See Gathers, 234 N.J. at 221.

a. **Apple iPhone X**

The Apple iPhone X was the subject of the CDWs issued by the Hon. Joseph Oxley, J.S.C., and a search warrant issued by the Hon. James McGann, J.S.C., all dated November 21, 2018. See Def. Exhibits A through E. This court considers the Tozzi affidavit in support of the CDW for Defendant's iPhone records for the time period of November 6, 2018, to November 20, 2018 only for the purposes of comparison to the Weisbrot affidavit.

The Tozzi affidavit goes to great lengths to establish probable cause. It not only describes the facts of the two separate fires at Defendant's house and the home

of the victims, she explains how investigators uncovered surveillance footage of a vehicle similar in make and model to the Defendant's vehicle traveling on roads between Ocean Township and Colts Neck in the early morning hours, first driving away from Defendant's home and then driving towards it a few hours later. It also gives particularized detail as to the injuries sustained by the Caneiro family, the locations where their bodies were found in and around the home, and notes that a 911 call was placed at approximately 3:30 A.M. and that the caller had reported the sound of gunshots near Keith Caneiro's home.

In addition to the probable cause suggested by a vehicle similar to Defendant's being seen departing and returning around the time when gunshots were heard in Colts Neck, the Tozzi affidavit offered further links between Defendant and his brother by mentioning that "v) During the course of this investigation it was learned that Paul Caneiro and his brother, Keith Caneiro, owned two businesses together: Square One Consulting and Ecostar Pest Company." Def. Exhibit A at 8.

The Tozzi affidavit requested information from the time period of November 6, 2018, up to and including November 20, 2018. Def. Exhibit A at 1. The court finds the above summarized facts specifically establish probable cause for the iPhone records for the time period requested, not only because the affidavit described the victims' injuries in a manner consistent with homicide and offered a reasonable suggestion that Defendant may have driven to his brother's house around the time

when gunshots were reported in that area, but because the affidavit suggested a close working relationship between Defendant and his brother, two weeks was a reasonable period of time to search for evidence of a possible motive. [7]

As mentioned, the Tozzi affidavit describes both fires, states that Keith and Paul owned businesses together, and that there were four homicides which occurred at the Colts Neck fire. Def. Exhibit A at 6-7. In paragraph w, Det. Tozzi writes that she believes the T-Mobile records will contain evidence of "murder, aggravated arson, possession of a firearm, possession of a firearm for an unlawful purpose, unlawful possession of a weapon and possession of a weapon for an unlawful purpose." Def. Exhibit A at 8.

In comparison, the Weisbrot affidavit was submitted approximately three hours earlier on November 21, 2018. The Weisbrot affidavit was submitted in support of a search of the residence at 27 Tilton Drive, a Porsche Macan, a Porsche 911 Carrera, a 2016 Jeep Wrangler, a 2016 Porsche Cayenne, and an Apple iPhone X. Def. Exhibit D at 1-7.

The Weisbrot affidavit addressed probable cause for the search of the iPhone in paragraphs m and r, stating the phone was: "m) Seized from the person of Paul Caneiro . . . [and the] affiant has probable cause to believe that evidence of the crime

---

[7] The court has also evaluated the remaining paragraphs of Det. Tozzi's affidavit as part of the totality of the information provided to the court.

of Aggravated Arson and other related crimes exists within the phone." More specifically, it stated the affiant

> r) . . . has probable cause to believe that evidence of the crime of Aggravated Arson and other related crimes will be found within the residence and curtilage at 27 Tilton Drive, Ocean Township, NJ as well as within the vehicles, which were all located at the residence at the time of the fire. In addition, your affiant has probable cause to believe that evidence relating to these crimes is located within Paul Caneiro's Apple iPhone X. Your affiant knows that these devices contain a variety of information including but not limited to call history, text detail records, applications as well as significant information relating to location of the device at the time that it's being accessed.
>
> [Def. Exhibit D at 10-11.]

Compared to the Tozzi affidavit's specificity, this affidavit is lacking in significant facts, including that the four victims suffered from gunshot or knife wounds and the business relationship between the Defendant and his brother. The description of the Colts Neck crime scene suggests foul play but does not articulate the scene as that of a homicide. It does not even mention that Keith was found outside the home, only that there was a fire and four deaths.

The Weisbrot affidavit states that the iPhone X will have "evidence of the crime of Aggravated Arson and other related crimes." Def. Exhibit D at 11. It does state that the affiant believes the iPhone, Defendant's residence, and all the vehicles may contain "evidence immediately apparent as being relevant to the investigation into the Aggravated Arson . . . and/or relevant to the investigation into the deaths at

15 Willow Brook Road, Colts Neck."[8] Def. Exhibit D at 2-6. However, it draws few connections between the fire at Defendant's home and the fire at the Colts Neck property and does not specifically state the other crimes being investigated.

Applying every common-sense inference to the facts alleged in the Weisbrot affidavit, this court does not find that it is obvious that the phrase "other related crimes" necessarily means the four Colts Neck homicides, as the State argued. The court must look at the four corners of the affidavit, and nowhere in the Weisbrot affidavit is there an indication that the deaths were homicides. The Weisbrot affidavit does state that the deaths of the four Caneiro family members were "currently pending autopsies, but significant trauma was noted." Def. Exhibit D at 10. But there is no description of the types of injuries the victims suffered; they were simply pending autopsies after being found at the scene of a fire. Det. Weisbrot and Det. Tozzi both submitted their affidavits on November 21, 2018. Def. Exhibit A; Def. Exhibit D. The State knew on November 21, 2018, that the Defendant was suspected of more than arson. Det. Weisbrot could have chosen to include more information for his probable cause for the search warrant but did not do so.

---

[8] The court notes that context makes it clear the "crime of Aggravated Arson" mentioned in the Weisbrot affidavit refers to the fire at Defendant's home.

The court also finds that there was no temporal limitation for the information sought from the iPhone, nor justification for omitting such a limit. While temporal limits are not strictly necessary if the information or evidence sought is not time-limited in nature, some probable cause is strictly time-based. In Missak, all the evidence sought had been created in a two-day period; there was no possibility of finding evidence of the crime under investigation from a time before the defendant learned of his victim's existence. The only justification given for searching beyond those two days was a conclusory assertion that "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." Missak, 476 N.J. Super. at 320–21. The court found that too speculative.

Here, this court finds that the Weisbrot affidavit similarly does not establish probable cause for unlimited data from Defendant's phone, as it does not develop a connection between the entirety of the phone and the probable cause demonstrated. The court cannot find probable cause to search weeks, months, or years in the past when the affidavit only suggests that Defendant may have left his home the night of the fire, and when the warrant affidavit only describes the crime of arson by name. The CDW, by contrast, was issued approximately three hours later and is based on a supporting affidavit that is significantly more detailed. Even though the CDW

makes connections between the Defendant and the Colts Neck homicides, those connections cannot be carried over to support probable cause for a separate warrant. See Marshall, 199 N.J. 602.

But Det. Weisbrot's request for a warrant for the Defendant's phone is founded on more than an impermissible hunch; the affidavit includes facts establishing probable cause to search the phone itself, at least in part. The Weisbrot affidavit establishes Defendant's suspicious behavior starting in the early morning hours of November 20, 2018. Def. Exhibit D at 10. The affidavit further explains that a white Porsche consistent with Defendant's Porsche left the area of Tilton Drive at 2:07 a.m. only to return home later. Def. Exhibit D at 10. Two white Porsches were observed at 27 Tilton Drive during the initial response to the fire there. Def. Exhibit D at 10. And, approximately eight and a half hours later, the Defendant's brother and the brother's family were found deceased due to significant trauma. Def. Exhibit D at 10.

In evaluating the facts constituting probable cause for the issuance of a search warrant, "[t]he facts should not be reviewed from the vantage point of twenty-twenty hindsight by interpreting the supporting affidavit in a hypertechnical, rather than a commonsense manner." State v. Sheehan, 217 N.J. Super. 20, 27 (App. Div. 1987). Instead, probable cause for the issuance of a search warrant requires a fair probability that contraband or evidence of a crime will be found in a particular place. Chippero,

201 N.J. at 28. The reasonable probabilities that flow from the Weisbrot affidavit supports the issuing judge's finding of probable cause that Defendant's suspicious behavior started before November 20, 2018.

The Weisbrot affidavit provides facts that lead to a commonsense inference that the fire at Defendant's home was planned, that a vehicle left Defendant's home in the early morning and did not return for approximately two hours, and that another suspicious fire was discovered at his brother's home later that same day. These facts create a well-grounded suspicion that a search of Defendant's phone will reveal his whereabouts during and before his early-morning departure from his home, because (1) the affidavit establishes that it is Defendant's cellphone; (2) cellphones are frequently kept in the possession of the owner at all times; and (3) Defendant's cellphone contained information regarding Defendant's location before, during, and/or after these incidents in the form of GPS related data. See State v. Evers, 175 N.J. 355, 381 (2003). Therefore, because Det. Weisbrot's affidavit established probable cause to believe that Defendant's iPhone contained at least some evidence, most likely in the form of GPS information, a narrower search and forensic examination of the device is still reasonable.

As to how the search must be narrowed, it is more reasonable to limit by time than by location or category of data. The Weisbrot affidavit establishes a timeline

that supports extending the search window to include November 19, 2018. The affidavit describes Defendant's vehicle departing his residence at approximately 2:07 A.M. on November 20, conduct that, to this Court based on the totality of the circumstances, implies planning or decision-making taking place beforehand. Common sense dictates that preparing for conduct as serious as arson would require advance preparation, which would reasonably occur in the late hours of November 19. Considering these facts in their totality, there is a fair probability that evidence of planning or intent concerning Defendant's arson of his own home would be found in data created or accessed on Defendant's iPhone during November 19 and November 20, 2018, justifying a limited search covering that timeframe.

The affidavit explains that cell phones contain a variety of information, and it is common knowledge that computers are dynamic, with relevant information created by a variety of applications and often stored in non-linear environments. See, e.g., United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009) ("it is folly for a search warrant to attempt to structure the mechanics of [a computer] search and a warrant imposing such limits would unduly restrict legitimate search objectives"). Any application or website may create relevant data: web searches can show planning, applications can access the microphone, camera, or GPS transponder of a phone and files and permissions can be shared across applications and devices.

The most sensible approach, and the one that both protects Defendant's Constitutional rights and supplies the State with the full portion of the search that was supported by probable cause. Accordingly, for all the stated reasons, it is this Court's order that the admissible, extracted data is limited to that created between November 19-20, 2018, a roughly 30-hour period leading up to the fire at Defendant's home, and further finds that all data created in that time period is admissible, regardless of where it is stored on the device.

b. **Apple Watch**

Det. Petruzziello submitted an affidavit in support of an application for a CDW for the T-Mobile records pertaining to cell phone number [redacted], registered to Defendant's Apple Watch, and for a search of the watch itself. The Defendant is challenging the validity of the affidavit and search warrant for the Apple Watch, under the same rationale that it contains no restrictions and is therefore another general warrant. Defendant argues there is no probable cause that allows for "any and all" of the data to be retrieved on the Apple Watch.

Det. Petruzziello's affidavit lists the "grounds for this application and the probable cause" as being supported by much the same facts as the prior warrants, albeit with more details that were gathered through the ongoing investigation. It specifically mentions the investigation into the Apple Watch in paragraph qq:

qq) Additionally, upon review of the aforementioned cell phone extraction of Paul Caneiro's cell phone, four incoming text messages from Keith Caneiro's cell phone to Paul Caneiro's cell phone were revealed. All were sent between the hours of 3:14 a.m. and 3:18 a.m. on November 20, 2018, approximately four minutes after the report of shots fired in Colts Neck. A review of the previously obtained records for Keith Caneiro's cell phone identified several entries that were listed as both incoming and outgoing with Paul Caneiro's telephone number ([redacted] Keith Caneiro's telephone number [redacted], and a third number identified as [redacted] for the time period listed above. On December 17, 2018, your affiant issued a grand jury subpoena to T-Mobile to obtain subscriber information for [redacted]. The results indicated that the aforementioned number is associated with Paul Caneiro, and was effective July 4, 2018. Additionally, the subscriber information identified the rate plan as being associate with an Apple watch. Your affiant reviewed the previously obtained records associated with Paul Caneiro's Apple ICloud account, which identified an Apple watch that was purchased on July 4, 2018 in the name of Paul Caneiro. The watch was more specifically identified as a series three, which has a built in cellular feature.

[Def. Exhibit I at 11-12.]

Petruzziello's affidavit mentions surveillance cameras showing a vehicle, consistent with the vehicle driven by Defendant, leaving Defendant's home in the early morning hours of November 20, 2018, and it mentions the four homicides that occurred at 15 Willow Brook Road. Def. Exhibit I at 6-7. The Petruzziello affidavit submits that during the time the Defendant's vehicle was gone from his home, there was a report of shots fired near Keith's home and Keith and his family suffered multiple gunshot and knife wounds. The affidavit further states that Defendant and Keith had shared business ventures, that Keith had noticed missing money, and this led to

a confrontation between Keith and the Defendant on November 19, 2018. This confrontation included Keith threatening to withhold the Defendant's wife's salary.[9] The affidavit clearly shows that Defendant and Keith's relationship had deteriorated, and that Defendant was experiencing financial pressures. Def. Exhibit I at 10-11. The affidavit details the business relationship the brothers had, the blood found at the Defendant's home, and how "Corey Caneiro further revealed that Keith told him that he was frustrated with Paul and the amount of money spent from their business accounts." By way of further support, Det. Petruzziello's affidavit further indicated that

> ii) During the course of this investigation, it was learned . . . Keith Caneiro confronted Paul Caneiro in and around April 2018 regarding missing money.
>
> [REDACTED] revealed on April 30, 2018, an ACH deposit description of [REDACTED] in the amount of $14,008.74 and on May 15, 2018, an ACH deposit titled [REDACTED] in the amount of $43,672.50. Based upon your affiant's training and experience, the deposit descriptions relate to a QuickBooks, Online account or general ledger.
>
> [. . .]
>
> Immediately after the receipt of deposits, funds in the amount of $14,000 on April 30, 2018 and $43,000 on May 15, 2018 were transferred to TD Bank, Individual Checking account, in the name of Paul Caneiro, 705 Cookman Avenue, Suite 2, Asbury Park, New Jersey.
>
> [. . .]

---

[9] The record in this case shows that the Defendant and Keith had an arrangement wherein Defendant's wife drew a salary from their joint businesses.

> kk) On November 23, 2018, investigators continued to search the home of Paul Caneiro, (via search warrant obtained from the Honorable Joseph W. Oxley, J.S.C.), at 27 Tilton Drive, Ocean, NJ, utilizing a NJSP Cadaver Detection K9. NJSP Trooper Matthew Cocking and his K9 Creed conducted a K9 search of the 27 Tilton Drive, Ocean Twp., property for the presence of blood. K9 Creed indicated the presence of blood in the basement of the residence near where the fire was located. In this area was a plastic container containing clothing with red stains consistent with blood. K9 Creed also detected the presence of blood in the trunk of the Porsche Macan bearing NJ registration [redacted]. A piece of paper with red colored staining was located in the truck.
>
> [Def. Exhibit I at 7-10.]

These statements establish a well-grounded suspicion of potential motive evidence as far back as April 2018. A showing of probable cause does not require information sufficient to support a conviction, but the information must establish more than just a suspicion that a crime has occurred and that evidence of such will be found. Mark, 46 N.J. at 271. Here, the affidavit shows an outline of events that unfolded between the two brothers, how two fires occurred at the residences of the brothers, and the manner in which Keith Caneiro and his family had been killed. It also shows that Defendant was confronted by his brother for financial misappropriation prior to Defendant's purchase of the Apple Watch. Det. Petruzziello also not only offered facts which suggest Defendant never repaid the trust and had reason to conceal any future misappropriations, but explained that, in his experience, files can not only be concealed on such devices but "in order to fully retrieve data from a computer or other digital communications system, the analyst will need access to all

storage media and devices that were or may have been used by the suspect." Def. Exhibit I at 12.

There is probable cause to search the Apple Watch as far back as April 2018 or shortly before then. The CDW records connected to Keith's cell phone revealed that the Defendant bought his Apple Watch on July 4, 2018, and used the watch regularly, including to communicate with his brother. These communications had a potential relevance to motive, as the business partnership was shown to be deteriorating.

There was sufficient probable cause to support the conclusion that other data, such as bank transaction confirmations, were saved locally in the watch's storage. Petruzziello's affidavit therefore creates not just a specific link between the crimes alleged and the Apple Watch, but between the crimes alleged and the entirety of the Apple Watch.

Unlike the search warrant affidavit for the iPhone, which only rationally related to calls and location data immediately before and after the fire at Defendant's home, this court finds probable cause that data on the Apple Watch, including copies of emails or app notifications and communications with the victim regarding their shared business could all provide evidence of misappropriation or otherwise speak to motive.

Therefore, it was reasonable to limit the search to the original purchase date and search the Apple Watch in its entirety, from July 4, 2018, to November 20, 2018. There is no need to extend the search parameters earlier than the day the watch was placed into service; as mentioned supra, files on a device may predate that device, so extending the search parameters beyond the day Defendant purchased the watch increases the risk of unreasonable intrusion into prior-created ESI and would not provide any evidence related to the watch itself.

c. **iPad and Apple MacBook laptop**

An iPad and Apple MacBook laptop were retrieved during the search of the Porsche Cayenne, which was authorized by the search warrant issued on November 21, 2018, by the Hon. James J. McGann, J.S.C. Def. Exhibit M at 2. The search of the vehicle itself is not in dispute and this court defers to the prior determination that probable cause existed.

Defendant's iPad and laptop were recovered from the Porche Cayenne and subsequently searched, pursuant to a search warrant. Unlike the iPhone, the iPad and laptop were not specifically named in the search warrant. They fell into the broad category of "[a]ny and all cellular telephones, computers, laptops, [and] tablets" that the warrant authorized searching, after the State seized same during their search of

Defendant's home and vehicles. And, unlike the Apple Watch, separate search warrants for the iPad and laptop's contents were never issued. Defendant urges the court to suppress these devices in their entirety based on the lack of individual warrants.

The State defends the search of these devices based on the warrant's authorization to seize "[a]ny and all cellular telephones, computers, laptops, tablets and permission to search same pursuant to this warrant." Def. Exhibit M at 1. The State argues that this statement allows for the search of any cellular telephones, computers, laptops, and tablets found during the search of the 2016 Porsche Cayenne. As there was no search warrant issued for these electronic devices, the Defendant is requesting a heightened remedy and requests total exclusion. The State is seeking for the court to not exclude the contents retrieved from these devices, but if the court is inclined to limit the data, it asks the court to maintain the same temporal limitation as the court has set for the other devices.

A phone or electronic device, even if properly seized, requires a warrant to search its contents. Riley, 573 U.S. at 403. While Riley framed the issue as whether a cell phone could be searched after arrest, the rationale for requiring a warrant hinged on the fact that cell phones can now store personal data on a far larger and grander scale, and "are in fact minicomputers" with "immense storage capacity." Id. at 393. If cell phones have the capability to carry immense personal data, a laptop or tablet is worthy of the same protection. Thus, to search the Defendant's iPad and

laptop, they must fall within the probable cause articulated in the warrant application.

As mentioned, "[t]he touchstone of the Fourth Amendment and Article I, Paragraph 7 of the New Jersey Constitution is reasonableness." State v. Hathaway, 222 N.J. 453, 476 (2015). The inquiry as to whether a search was reasonable applies equally to the issuing of a warrant, the execution of the warrant by police, and the subsequent search of items seized. State v. Chippero, 201 N.J. at 27, State v. Watts, 223 N.J. 503, 514 (2015), Andresen v. Maryland, 427 U.S. 463 n.11 (1976).

The entire contents of the iPad and MacBook laptop were searched based on a broad authorization to search any devices seized, but Missak still requires probable cause. Here, this court finds that there was no probable cause established for "any and all cellular telephones, computers, laptops, tablets and permission to search same pursuant to this warrant." Def. Exhibit D at 6. Det. Weisbrot's affidavit established a "fair probability that contraband or evidence of a crime will be found." Chippero, 201 N.J. at 18 (quoting United States v. Jones, 994 F.2d 1051, 1056 (3d Cir. 1993)), but did not explain why it was likely to be found on any and every computer encountered. The affidavit did not set out reasons to believe that any computers were even likely to be found within the Cayenne. Even if we assumed the Defendant owned these devices, and assumed they would be found inside the car, the court would then

need to draw the inference that the devices would contain evidence of arson and "related crimes."

Furthermore, it authorized the search of these devices without any regard to ownership. In United States v. Griffith, the District of Columbia Circuit found that a search warrant that allowed for all electronic devices in a home to be seized, with no regard to who owned said devices, was overly broad. United States v. Griffith, 867 F.3d 1265, 1276 (D.C. Cir. 2017). "[I]t allowed unfettered access to any electronic device in the apartment even if police knew the device belonged to someone" other than the defendant. Id.

Courts have allowed more latitude in connection with searches for contraband like weapons or narcotics, but when the police seize commonplace personal effects, those circumstances call for special care to minimize intrusion upon privacy. See Stanford v. State of Tex., 379 U.S. 476, 486 (1965); Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976). A generalized search for a device such as a computer or phone may also warrant greater latitude when a reasonable investigation cannot produce a more particular description. In Griffith, it was noted that police might have probable cause to seize a suspect's phone, yet lack knowledge about the phone's make, model, or serial number, if they based their probable cause on information from an informant that such a phone existed. In such an instance, any devices seized would need to

be at least examined to determine their ownership and their relevance. Griffith, 867 F.3d at 1277.

The touchstone of any search, warranted or warrantless, is reasonableness. See Hathaway, 222 N.J. at 476. There are certainly situations where it may be reasonable to search any and all computers located within a particular location. If the things being searched for can reasonably be found on a computer and there is sufficient justification that they will be found on a computer located in a certain place, then there is some rational support for the proposition that computers should not be treated "differently from storage mediums such as filing cabinets and briefcases." United States v. Giberson, 527 F.3d 882, 887 (9th Cir. 2008). If probable cause allows, then "there is no reason why officers should be permitted to search a room full of filing cabinets or even a person's library for documents listed in a warrant but should not be able to search a computer." Id. at 888.

But here, there was nothing in this warrant that would justify a limitless and unfocused search every computer found. Certainly, there was justification to seize the computers and secure them, but once secured there was ample time to obtain a warrant. See State v. Miranda, 253 N.J. 461, 483 (2023). Although the warrant is presumed reasonable, there is not enough to support a preemptive authorization of the devices without some showing they would be found there, and a mere possibility

is not enough to justify anticipatory authorization. See State v. Ulrich, 265 N.J. Super. 569, 576 (App. Div. 1993) (rejecting anticipatory warrants except in strictly proscribed circumstances); See also Marshall, 199 N.J. at 613 (warrant that "delineated the conditions that needed to be satisfied" was relying on information outside the four corners of the affidavit to establish probable cause and was invalid). Therefore, since the affidavit does not outline what computers were expected to be found or how ownership would be determined, the court finds that the information retrieved from the iPad and MacBook laptop must be suppressed. While the seizure of the iPad and MacBook during the vehicle search was lawful under the valid warrant authorizing the search of the Porsche Cayenne, any examination of their contents required independent probable cause, which was not established in the Weisbrot affidavit.

VI. CONCLUSION

Consistent with the foregoing findings and the constitutional standards articulated in Missak, Riley, Marshall, and their progeny, the Defendant's motion to suppress is **granted in part** and **denied in part** as follows:

Regarding the Apple iPhone X, the search warrant established probable cause to examine Defendant's iPhone for data relevant to the planning and execution of the alleged crime of arson beginning November 19, 2018, and extending through November 20, 2018. Accordingly, only data created or accessed during that period

is admissible. Data created outside this timeframe shall be suppressed and excluded from use at trial unless the Defendant affirmatively offers or relies upon such data, in which case evidence that is reasonably necessary to explain, contextualize, or rebut that item shall be admissible.

With respect to the Apple Watch, the affidavit supporting the search warrant established probable cause for a broader period encompassing the deterioration of the Defendant's financial relationship with the victim. The search of data from the Apple Watch covering the entire timeframe from July 4, 2018, when the device was purchased and activated, through November 20, 2018, is supported by probable cause, and such data is admissible.

As to the iPad and Apple MacBook laptop, the search warrant's blanket authorization to search "[a]ny and all cellular telephones, computers, laptops, tablets and permission to search same" failed to identify with particularity the specific devices expected to be found or articulate probable cause to believe those devices contained evidence of the alleged crimes. As a result, all data recovered from the iPad and MacBook laptop is suppressed in full.

To ensure effective enforcement of this ruling, the State shall, within 20 days of this order, review all data extracted from Defendant's devices, sequester and exclude any data beyond the authorized timeframes for the iPhone and all data from the iPad and MacBook, and provide written certification to the court and defense

counsel confirming that all such data has been excluded from use. Evidence derived solely from suppressed data shall likewise be inadmissible unless the State demonstrates by clear and convincing evidence that it was obtained through an independent, lawful source.[10]

For these reasons, the Defendant's motion to suppress evidence seized pursuant to the search warrants executed on his electronic devices is **GRANTED IN PART** and **DENIED IN PART**.

---

[10] State v. Smith, 212 N.J. 365, 395 (2012).