

COMMONWEALTH OF PENNSYLVANIA	:	IN THE SUPERIOR COURT OF
	:	PENNSYLVANIA
Appellant	:	
	:	
	:	
v.	:	
	:	
	:	
NNAEMEKA ANI	:	No. 1208 MDA 2021

Appeal from the Order Entered August 12, 2021
In the Court of Common Pleas of Centre County Criminal Division at
No(s): CP-14-CR-0001582-2019

BEFORE: BENDER, P.J.E., McLAUGHLIN, J., and STEVENS, P.J.E.*

OPINION BY BENDER, P.J.E.: **FILED: APRIL 17, 2023**

The Commonwealth appeals from the trial court's order granting Appellee Nnaemeka Ani's motion to suppress all evidence recovered from the execution of five search warrants. Each warrant pertained to Appellee's cell phone, its iCloud¹ backups, or its service provider records. The trial court determined that each warrant was lacking in probable cause and/or overbroad. The Commonwealth has abandoned its challenge to the first two warrants, arguing that the remaining three were valid. Our primary task is to decide the applicability of ***Commonwealth v. Green***, 265 A.3d 541 (Pa. 2021), issued after the trial court's order, which held that the standard

* Former Justice specially assigned to the Superior Court.

¹ The iCloud service backs up data contained on an iPhone, typically items like photos, videos, text messages, and device settings.

announced in ***Commonwealth v. Grossman***, 555 A.2d 896 (Pa. 1989) (holding that the Pennsylvania Constitution requires a description of items to be seized “as specifically as is reasonably possible”), applies to searches of digital spaces. Alternatively, the Commonwealth asserts that the three warrants established probable cause to at least some of the items requested in the warrants and that the trial court erred by failing to conduct a severability analysis. We conclude that the Commonwealth failed to establish probable cause to search Appellee’s cell phone for the vast majority of items requested. We agree that the doctrine of severability applies and hold that the Commonwealth may use locational data generated by the phone as well as data pertaining to Appellee’s use of the phone’s flashlight function with respect to the third warrant. We agree with Appellee that the fourth and fifth warrants must be suppressed as fruit of the poisonous tree. We therefore affirm in part, reverse in part, and remand for further proceedings.

I.

Factual and procedural history

The five search warrants involved Appellee’s alleged role in a series of home invasion crimes.² For ease of discussion, we first set forth a summary of the facts.

² We also note that this criminal case was consolidated with a rape case, for which Appellee has been convicted and sentenced. ***Commonwealth v. Ani***, (Footnote Continued Next Page)

The investigation commenced on November 2, 2019, when Natalia Beltran, a Pennsylvania State University student residing in the University Terrace apartment complex, called the State College Police Department shortly after 8:00 a.m., reporting that an unknown male had entered her bedroom. Beltran, who had been sleeping, stirred when the actor shone a light from his cell phone on her. She pretended to wake up to scare the individual, who fled the bedroom. Officers obtained surveillance video from the apartment complex, showing a male, later identified as Appellee, attempting to open several doors in the hallway. Appellee is seen entering Beltran's apartment at 08:05 a.m. and exiting three minutes later. Video surveillance showed Appellee entering two other apartments on November 2.

Building management confirmed that Appellee was a resident of University Terrace, and they suspected that he was responsible for two unresolved criminal trespass incidents reported by fellow University Terrace residents, occurring on October 13, 2019, and October 31, 2019. Officers spoke to eyewitnesses, who reported the following. Kate Deng discovered Appellee inside her University Terrace apartment on October 13, 2019. Appellee claimed that he was visiting a roommate of Deng's, and told Deng that he would text her roommate. The victim observed Appellee using his cell

283 A.3d 386 (Pa. Super. 2022) (unpublished memorandum). That matter is pertinent to the investigation as it is referenced within the fifth warrant application.

phone. Deng also reported that on October 16, 2019, she heard her front door close but no one else had been inside the apartment. Her roommate, Abigail Helmer, discovered that a vape cartridge had been moved from her bedroom to the living room. Deng identified Appellee from a photo lineup.

Regarding the October 31 incident, Hilda Sould told police that she heard someone inside her apartment. A neighbor confronted Appellee shortly thereafter and identified Appellee from a photo lineup.

Appellee was arrested on November 5, 2019, and the police seized a black iPhone 6 incident to the arrest. The authorities secured search warrants for the phone and ultimately found several incriminating images and videos occurring over the timespan of October 13, 2019, through November 5, 2019. These items included a photograph of Deng sleeping taken from inside her bedroom and evidence that Appellee took pictures of stolen credit cards.

The Commonwealth charged Appellee via criminal information with six counts, with a date range of October 13, 2019, through November 2, 2019. Counts one, two, and three were for violations of 18 Pa.C.S. § 3502(a)(1)(ii) (Burglary), and counts four, five, and six for violations of 18 Pa.C.S. § 3503(a)(1)(i) (Criminal Trespass). The first three counts do not specify a

victim. Counts four, five, and six name, respectively, Natalia Bertrand, Kate Deng, and Abigail Helmer.³

On April 1, 2021, Appellee filed a motion to suppress the five search warrants, arguing that each warrant was “not supported by probable cause, is overly broad, and is lacking in particularity[.]” Motion, 4/1/21, at 9 (first warrant). An identical claim was asserted against each of the other warrants. ***Id.*** at 11 (second warrant); 13 (third warrant); 15 (fourth warrant); 23 (fifth warrant). The Commonwealth filed a brief in response on July 26, 2021. The trial court entered an order and accompanying opinion on August 10, 2021, suppressing all evidence recovered from the warrants.

We now set forth the contents of each warrant application. This is necessary because the legal determination of whether a warrant was supported by probable cause is limited to the four corners of the affidavit. ***Commonwealth v. Coleman***, 830 A.2d 554, 560 (Pa. 2003). “[E]ven the slightest alteration in the underlying facts can have great effect on the probable cause analysis.” ***Commonwealth v. Johnson***, 240 A.3d 575, 589 n.7 (Pa. 2020) (Opinion Announcing the Judgment of the Court). In this regard, Appellee points to facts missing in some of the warrant applications. ***See, e.g.***, Appellee’s Brief at 22 (noting that the third warrant application,

³ It does not appear that the Commonwealth had charged Appellee with any additional crimes following the execution of these warrants and prior to the trial court’s suppressing the evidence.

unlike the first application, did not state that Appellee appeared to be sending a text message). The Commonwealth has abandoned its challenges to the first two warrants. Accordingly, before addressing the legal issues, we discuss the three warrants at issue, which are the third, fourth, and fifth warrants in chronological order.

Warrant #3 - April 21, 2020

This warrant listed the item to be searched as a “[c]ell phone belonging to [Appellee]. The cell phone is a black iPhone 6.” Application for Search Warrant, 4/21/20, at 1. Under the “identify items to be searched for and seized” field, the application states, “See attachment A.” That document was appended to the application. It states:

The memory/data storage of a black iPhone 6 cellular handset belonging to [Appellee] for data/information, and any “cloud” storage applications connected to the cellular handset, concerning any of the following on October 13, 2019, October 31, 2019, and November 2, 2019: use of the flashlight; Apple Health data; use of the camera application to take photographs or record video; use of any applications requiring the use of the phone’s keyboard, including text, photo, or video message applications, Internet browsers, and applications for voice or video calls; locational data, as compiled by the phone’s internal GPS device or other components or applications of the phone capable of identifying and memorializing the geographic location of the cellular handset. The search is to be conducted for evidence, direct and corroborative, of the criminal offenses identified in the Affidavit of Probable Cause to this warrant application, incorporated herein by reference in its entirety.

Id. (Attachment).

The affidavit begins by explaining the police response to Beltran’s apartment on November 2, 2019, and references her observation that the

male “entered her bedroom and flashed a light from his phone on her person.” **Id.** at 2. It discusses the video surveillance showing Appellee visiting two other apartments on November 2, 2019.

With respect to October 13, 2019, the affidavit establishes that Detective Hanes “interviewed the residents ... on 11/5/19.” **Id.** at 3. This interview included Kate Deng and her boyfriend, Peter Giammanco. **Id.** Deng informed Detective Hanes that she was in her bedroom and heard the back door to her apartment open. When she went to see if it was her roommate she saw “a black male standing in her kitchen who she did not know.” **Id.** The actor claimed that he was waiting for Deng’s roommate and “said he would text her roommate[.]” **Id.** He then exited the apartment. A few days later, Giammanco entered Deng’s apartment through the back entrance. He heard the front door close. He asked Deng if anyone else was home. Deng stated she had been sleeping and had not invited anyone inside. **Id.** Deng identified Appellee from a photo lineup. **Id.**

The affidavit also discusses the October 31, 2019 incident. Detective Hanes’ affidavit states that two police officers went to Hilda Sould’s apartment. She reported that on October 31, 2019, she heard a door close and went to investigate. As she did so, her neighbor Rafi Birro “was walking up to the apartment and stated he just saw a black male exit her apartment and jog away.” **Id.** Detective Hanes then interviewed Birro, who stated that he was returning to his apartment when he saw a black male exit Sould’s apartment.

The male “covered his face with a hood and jogged from the area.” **Id.** Birro identified Appellee from a photo lineup.

Warrant #4 - May 22, 2020

The fourth warrant was to be served on Apple, Inc., as the manufacturer of Appellee’s cell phone. The application requested a warrant to search the following:

All storage backups to the iCloud for the iOS device associated with the following email accounts: ralphemek@gmail.com & ranlmeks@gmail.com and associated with phone number, 14127588148, that ha[ve] occurred from 10/13/2019 through 11/5/2019. Items to be searched for are applications generating locational data and/or other information consistent with Ani’s presence and behavior at the scene of the offenses described in the affidavit. The backups should include information on, but not limited to, the subscriber information for the Apple accounts, mail logs, my Photo Stream; iCloud Photo Library; Internet Browsing History; Maps Search History; all messages including SMS; MMS, iMessages, and other messaging applications; Health Data; IP address logins; and other information on when iOS Device Backups had been completed by the device.

Application for Search Warrant, 5/22/20, at 1.

The affidavit of probable cause discusses the execution of Warrant #3. The affidavit states that Officer Dan Lewis of Ferguson Township assisted and was unable to complete a full extraction due to its passcode security. However, Officer Lewis “was able to perform a partial extraction of the cell phone.” **Id.** at 4. That partial extraction revealed that the phone was linked to two Apple iCloud accounts under the email addresses ralphemek@gmail.com and ranlmeks@gmail.com. Additionally, a backup to the cloud service was completed on November 5, 2019. The partial execution

also indicated that the phone connected to several WiFi access points in the University Terrace building around the time of the November 2, 2019 burglaries.

The detective stated, based on his training and experience, that iPhones use “Locational Based Services in several applications ... to assist the user with information and services.” **Id.** The affidavit listed dozens of applications which commonly use these location services, including Facebook, Instagram, web browsing apps, weather apps, messaging apps, dating apps, health apps, and ridesharing apps. Location data can also pinpoint where photographs and videos were taken by using GPS, Bluetooth, WiFi, and cell tower locations to determine the phone’s location. **Id.** Detective Hanes requested a search warrant for all storage backups to the iCloud service “that ha[ve] occurred from 10/13/19 through 11/5/19.” **Id.** The affiant intended to search for “applications generating locational data and/or other information consistent with [Appellee]’s presence and behavior at the scene of the offenses described in the affidavit.” **Id.**

Warrant #5 - September 8, 2020

The final warrant at issue was obtained after the execution of Warrant #4 produced several incriminating photographs. It requested permission to search for the following items:

Photographs, videos, and associated geolocation data comprising evidence of the crimes of rape/sexual assault, burglary, criminal trespass, loitering and prowling at nighttime, invasion of privacy, theft, identity theft, and access device fraud found on the iCloud

backups associated ralphemek@gmail.com [sic] & ranimeks@gmail.com and phone number, 14127588148, currently in the possession of affiant, Detective Martin-Hanes, at the State College Police Department.

Application for Search Warrant, 9/8/20, at 1.

The premises to be searched were listed as the iCloud back up data as provided by Apple, which was likewise “currently in the possession of the State College Police Department.” ***Id.***

A ten-page affidavit was attached. The affidavit begins by discussing a series of crimes reported to the Ferguson Township Police Department between July 2017 and December 2018. The affidavit supplies details of over a dozen incidents, which included a series of loitering complaints, suspected burglaries, and rape. All of these incidents occurred in the area of 110 West Aaron Drive, with a consistent suspect description. The affidavit relates that Appellee was arrested on December 17, 2018, and an iPhone was seized incident to the arrest.⁴ A search warrant for DNA was obtained, and on January 11, 2019, the lab reported that Appellee’s DNA was linked to a rape reported on October 18, 2017. Appellee was charged on January 15, 2019, for that rape, and, on May 18, 2019, Appellee posted bail and was released from Centre County Jail. As previously mentioned, Appellee was convicted of this rape.

⁴ It is not clear whether this was a different phone, as authorities seized an iPhone on November 5, 2019, when Appellee was arrested.

The next paragraph discusses the November 2, 2019 report from Beltran that precipitated this set of warrants, as well as the follow-up investigations and the execution of the April warrant. This affidavit describes what the authorities learned from Warrant #4. After Apple provided the material, Detective Hanes received assistance from “Glenn K. Bard of PATCtech,” who was able to decrypt the supplied data. ***Id.*** at 9. The data was then loaded into forensic software for review. This review “uncovered evidence of criminal activity committed by [Appellee] within the time frame specified in the warrant, 10/13/19 through 11/5/19.” ***Id.*** Additionally, “[a]s Bard was locating the relevant images ... he noticed numerous images of Driver’s licenses and credit cards in plain view.” ***Id.*** at 10. These images showed the name “Erica Culler” and Detective Hanes confirmed that Culler had made a report on July 16, 2018 “of an unknown black male who was seen holding her wallet[.]” ***Id.*** Based on the several unsolved incidents in the same geographic area with a suspect profile matching Appellee, this warrant sought to expand the search of Appellee’s phone.

Suppression and appeal

The trial court granted Appellee’s motion to suppress and filed an accompanying opinion with its order. The court concluded with respect to Warrant #3 that

not all items requested ... were supported by probable cause. Specifically, the [c]ourt finds the request to search the ‘use of any applications requiring the use of the phone’s keyboard, including text, photo, or video message applications, Internet browsers, and

applications for voice or video calls[]' that occurred on October 13, 2019, October 31, 2019, and November 2, 2019 to be overbroad and unsupported by probable cause.

Order, 8/10/21, at 10.

The court explained that the four corners of the affidavit mentioned Appellee's phone only twice, which established that Appellee was observed using his phone's flashlight function in Beltran's apartment and that he mentioned texting when confronted by Deng. The court concluded that these references "do[] not provide law enforcement with sufficient probable cause to have such broad access to [Appellee]'s cellular phone. The [a]ffidavit provided no information alleging [Appellee] took a photograph or filmed a video during the October 13th and October 31st incidents." ***Id.*** at 11. The court determined that the request to search for anything that used the phone's keyboard was "overbroad[,]" as it is difficult to imagine what application, if any, does not in some way require the use of the cellular phone's keyboard." ***Id.***

The Commonwealth filed a timely notice of appeal pursuant to Rule of Appellate Procedure 311(d)⁵ and complied with the trial court's order to file a Pa.R.A.P. 1925(b) statement. The Commonwealth raised, for the first time, a

⁵ "In a criminal case ... the Commonwealth may take an appeal as of right from an order that does not end the entire case where the Commonwealth certifies in the notice of appeal that the order will terminate or substantially handicap the prosecution." Pa.R.A.P.311(d). In its notice of appeal, the Commonwealth certified that the prosecution of Appellee is substantially handicapped by the trial court's order granting suppression.

claim that the trial court should have severed any portions of the warrant it deemed invalid. ***Id.*** The court filed a Rule 1925(a) opinion, adopting its previously-filed opinion as to the warrants. Responding to the severance claim, the trial court stated, “some items contained in the ... warrant applications were supported by sufficient probable cause. However, ... the vast majority of the items ... were unsupported[.]” Trial Court Opinion, 10/11/21, at 2. The Commonwealth raises the following two issues for our review:

[1.] Whether the suppression court erred in granting suppression on the following grounds:

- a. [T]hat Warrant #3 was overbroad because it “grant[ed] law enforcement ... unlimited access to [Appellee’s] cellular phone for the day in question, allowing them to use Warrant #3 as an investigatory tool”;
- b. [T]hat Warrant #4’s authorization to search for and seize “other information consistent with [Appellee]’s presence and behavior at the scene of the offenses” rendered the warrant “overly broad and lacking in particularity”; and
- c. [T]hat Warrant #5’s authorization to search for and seize “photographs, videos, and associated geolocational data comprising evidence” of crimes described in Affidavit #5 rendered the warrant invalid because the date range for those crimes was not specifically described.

[2.] Whether, assuming that portions of Warrants 3, 4, and 5 suffered from overbreadth, the suppression court erroneously failed to apply the doctrine of severance to the valid portions of the warrants.

Commonwealth’s Brief at 4.

II.

Parties' Arguments

Commonwealth

The Commonwealth's fundamental position is that there was probable cause to believe that Appellee's iPhone contained evidence of the home invasion crimes because Appellee was seen using his phone by various eyewitnesses. It emphasizes that a review of the four corners of an affidavit requires a commonsense view and courts cannot read the language in a hyper-technical fashion.

The Commonwealth submits that the Supreme Court of Pennsylvania's decision in **Green**, discussed in greater detail *infra*, establishes that the trial court erred in suppressing these warrants. Starting with Warrant #3, the Commonwealth argues that the trial court erroneously focused on the language permitting officers to search for the "use of any applications requiring the use of the phone's keyboard" as being overbroad. Application for Search Warrant, 4/21/20 (Attachment). The affidavit, which was expressly incorporated into the warrant, contained "limiting language constrain[ing] the search to evidence related to" criminal trespass and burglary offenses. Commonwealth's Brief at 26. Moreover, the warrant was limited to three dates: October 13, October 31, and November 2, 2019. "This temporal specificity goes above and beyond the **Green** requirements." **Id.** According to the Commonwealth, the temporal limitation and the limiting language ensured that "no indiscriminate or discretionary search of the phone could

have been conducted[.]” **Id.** The facts submitted in the application permitted the magistrate to conclude that “evidence of criminal activity was likely to be found on [Appellee]’s phone.” **Id.** at 27. The Commonwealth argues that the facts established “a pattern of trespassing into the residences of young women without their knowledge, when they were present, at times using his phone and, in any event, probably in possession of a phone that was compiling evidence of his location.” **Id.**

Turning to Warrant #4, the Commonwealth criticizes the trial court for focusing on the language allowing the affiant to search for evidence “consistent with [Appellee]’s presence and behavior at the scene of the offenses described in the affidavit.” Application for Search Warrant, 5/22/20, at 4. The trial court determined that this was too vague. The Commonwealth argues that the trial court read the language “in a vacuum, ignoring the detailed qualifications in the affidavit.” Commonwealth’s Brief at 28-29. “Had [the trial court] read the rest of the sentence, the court would have recognized that the crimes in the affidavit were limited to the dates the burglaries and trespasses occurred on October 13, 2019, October 31, 2019, and November 2019.” **Id.** at 29. Additionally, “the information sought was limited to only those items/information specifically identified in the affidavit.” **Id.** The warrant application “does not list general classes such as ‘all data’ or ‘all applications’; rather, the affiant specifies the exact types of data which should be included in the backups.” **Id.** The items requested “relate directly to the

'offenses described in the affidavit.'" **Id.** (quoting warrant application). The warrant was limited "to iCloud backups from October 13, 2019 through November 5, 2019 (which encompassed the criminal incidents described in the affidavit)." **Id.** at 30.

Finally, regarding Warrant #5, the Commonwealth emphasizes that the trial court acknowledged that probable cause existed to conduct a limited search of Appellee's iCloud backups. The court, in its view, erred by citing the possibility that the Commonwealth was permitted to search all the way back to 2011, when the iCloud service was launched. Warrant #5 did not seek authorization to go back to 2011; rather, it "clearly defined the temporal scope of the warrant, identifying with specificity various criminal offenses committed from September of 2017 through 2019 concerning which there was a reasonable probability of [Appellee]'s involvement." **Id.** at 32. As with the prior offenses, the affidavit makes clear "that the items sought pertain to specifically-identified criminal acts," as set forth in the affidavit of probable cause. **Id.** at 33.

Alternatively, the Commonwealth argues that if this Court agrees that probable cause was lacking to some of the items, the trial court erred by failing to apply the doctrine of severance.

Appellee

Appellee submits that this Court should accept the trial court's analysis of each warrant. The court thoroughly reviewed each warrant and measured

the sufficiency of the warrant's description against the items supported by probable cause. Appellee explicitly notes that this claim is raised under both the Fourth Amendment to the United States Constitution and Article I, Section 8 of the Pennsylvania Constitution, and cites the **Grossman** standard, which is specific to Article I, Section 8.

Beginning with Warrant #3, Appellee points out that, unlike Warrant #1, this application did not mention Appellee's being seen texting on his phone. Appellee's Brief at 21-22. While the affidavit mentions Beltran seeing Appellee use his phone's flashlight, the only mention of texting is the conversation between Deng and Appellee, wherein Appellee told Deng that he was looking for her roommate and would text her. Appellee additionally submits that, in any event, there is nothing in the affidavit of probable cause to indicate that Appellee used his phone to take pictures or record video.

Turning to Warrant #4, Appellee agrees with the trial court that the request to search for information "consistent with" Appellee's presence and behavior gives officers unbridled discretion. "There is no indication of what type of 'other information' police were expecting to find on the phone." **Id.** at 29. The "vagueness and lack of any type of specificity and particularity provided for in this description" establishes "the lack of probable cause[.]" **Id.** Moreover, the warrant was not limited to three specific dates, unlike Warrant #3. Instead, the warrant was for an entire three-week period. In conjunction with the vague authority to look for any information "consistent with"

Appellee's presence, authorities were seeking to conduct a general exploratory search, which is forbidden by both the United States and Pennsylvania Constitutions. Appellee also submits that this warrant was tainted by the illegal searches performed under the three prior warrants, all of which were found invalid. ***Id.*** It is clear that the authorities relied on information from the prior warrants because Warrant #4 explicitly references the results of Warrant #3. ***Id.*** at 34. Appellee also argues that the Commonwealth would not have been able to determine the email accounts associated with his iCloud backups and his cell phone number absent the execution of the first two warrants, which the Commonwealth no longer challenges.

Finally, Appellee acknowledges that Warrant #5 establishes a stronger basis for probable cause because it references incriminating evidence found during the prior searches. However, Appellee maintains that the warrant is still defective because it gives police "*carte blanche* to search the entire phone for any and all photos and videos." ***Id.*** at 36. In any event, this warrant was tainted because the incriminating evidence on which this warrant rests were uncovered during the execution of Warrant #4. ***Id.*** at 38.

III.

Searching a cell phone presents difficult Fourth Amendment and Article I, Section 8 questions. While the validity of the warrant is a question of law, "we are not to conduct a *de novo* review of the issuing authority's probable cause determination, but are simply to determine whether or not there is

substantial evidence in the record supporting the decision to issue the warrant.” ***Commonwealth v. Torres***, 764 A.2d 532, 540 (Pa. 2001).

We begin with the general principles applicable to search warrants.

A

General principles

The United States Constitution⁶ and the Pennsylvania Constitution⁷ both protect citizens from unreasonable searches and seizures. The Fourth Amendment “was a reaction to the evils of the use of the general warrant in England and the writs of assistance in the Colonies, and was intended to protect against invasions of the sanctity of a man’s home and the privacies of life, from searches under indiscriminate, general authority.” ***Warden, Md. Penitentiary v. Hayden***, 387 U.S. 294, 301 (1967) (quotation marks and citation omitted). Pennsylvania’s analogous constitutional provision stems from the same concern. “The framers of the Pennsylvania Constitution thought the right to be free from unrestricted police intrusions so critical that

⁶ “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV.

⁷ “The people shall be secure in their persons, houses, papers and possessions from unreasonable searches and seizures, and no warrant to search any place or to seize any person or things shall issue without describing them as nearly as may be, nor without probable cause, supported by oath or affirmation subscribed to by the affiant.” Pa. Const. Art. I, § 8.

they secured the right for future generations by including it in the original Constitution of 1776.” **Grossman**, 555 A.2d at 899.

Obviously, this is not an absolute bar on searching protected areas, provided that the authorities possess sufficient probable cause to search as determined by a neutral magistrate. “The point of the Fourth Amendment ... is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate[.]” **Johnson v. United States**, 333 U.S. 10, 13–14 (1948). “[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.” **Illinois v. Gates**, 462 U.S. 213, 232 (1983). **See Commonwealth v. Gray**, 503 A.2d 921, 922 (Pa. 1985) (adopting **Gates** as the test for search warrants under Article I, Section 8). “To establish probable cause, the Commonwealth must demonstrate that a search meets the requirements of the ‘totality-of-the-circumstances’ test.” **Commonwealth v. Barr**, 266 A.3d 25, 40 (Pa. 2021) (citation omitted). A magistrate presented with an application for a warrant must “make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him ... there is a fair probability that contraband or evidence of a crime will be found in a particular place.” **Id.** (citation omitted).

If there is probable cause to search, the warrant must be properly limited in scope. “The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.” **Marron v. United States**, 275 U.S. 192, 196 (1927). Our charter has been interpreted to offer more protections than its federal counterpart in several areas, including the required degree of particularity.

The language of the Pennsylvania Constitution requires that a warrant describe the items to be seized “as nearly as may be....” The clear meaning of the language is that a warrant must describe the items as specifically as is reasonably possible. This requirement is more stringent than that of the Fourth Amendment, which merely requires particularity in the description.

Grossman, 555 A.2d at 899 (footnote omitted).

This Court has recognized that the particularity component subsumes two distinct, although often related, concepts. The first concept addresses the degree of particularity required. A warrant that is not “particular enough” permits “a search in terms so ambiguous as to allow the executing officers to pick and choose,” which amounts to the rummaging that so offended the drafters of the federal and state constitutions. **Commonwealth v. Santner**, 454 A.2d 24, 25 n.2 (Pa. Super. 1982). This first component thus ensures that the authorities are sufficiently limited in what they can seize. The second concept is overbreadth. A warrant can be clear in terms of what will be seized,

thus ensuring that the authorities' discretion does not permit a general rummaging. But if the warrant allows authorities to seize items for which probable cause does not exist, it may be overbroad. ***Id.***

Applying these concepts to the digital evidence sphere, our sister court, the Oregon Court of Appeals, offered a summary of these distinct concepts in a case involving the search of digital evidence, framing the former concept as "specificity."

Those two concepts—specificity and overbreadth—again, have independent significance. For example, a warrant can precisely and unambiguously identify items to be forensically examined, satisfying the specificity concern, but nevertheless be invalid as overbroad if there is no probable cause to examine some of those items. However, the two can, and frequently do, conflate. That is, failure to identify with sufficient specificity the place to be searched or the items to be seized and examined can sanction invasions of protected privacy unsupported by probable cause. ***See, e.g., State v. Castagnola***, 145 Ohio St.3d 1, 17, 46 N.E.3d 638, 656 (2015) (noting "overlap" of those concepts with respect to warranted searches of electronic devices).

State v. Mansor, 381 P.3d 930, 793–939 (Or. App. 2016), *aff'd*, 421 P.3d 323 (Or. 2018). Our Supreme Court has identified these defects as "symptoms of the same disease."

Moreover, for particularity purposes, we have clarified that although some courts have treated overbreadth and ambiguity as relating to distinct defects in a warrant, ***see Commonwealth v. Santner***, ... 454 A.2d 24, 25 n.2 ([Pa. Super.] 1982), "both doctrines diagnose symptoms of the same disease: a warrant whose description does not describe as nearly as may be those items for which there is probable cause." ***Grossman***, 555 A.2d at 899-900.

Johnson, 240 A.3d at 584.

B

Digital versus physical

Searching digital evidence poses unique issues, owing to the distinctions between searching physical versus digital spaces. Before the advent of personal electronic devices and their tremendous storage capacities, the usual Fourth Amendment case involved the search of a physical space. The United States Supreme Court has held that, when searching a physical space for an item, authorities may search anywhere where that item may be.

A lawful search of fixed premises generally extends to the entire area in which the object of the search may be found and is not limited by the possibility that separate acts of entry or opening may be required to complete the search. Thus, a warrant that authorizes an officer to search a home for illegal weapons also provides authority to open closets, chests, drawers, and containers in which the weapon might be found. A warrant to open a footlocker to search for marihuana would also authorize the opening of packages found inside. A warrant to search a vehicle would support a search of every part of the vehicle that might contain the object of the search. When a legitimate search is under way, and when its purpose and its limits have been precisely defined, nice distinctions between closets, drawers, and containers, in the case of a home, or between glove compartments, upholstered seats, trunks, and wrapped packages, in the case of a vehicle, must give way to the interest in the prompt and efficient completion of the task at hand.

United States v. Ross, 456 U.S. 798, 820–21 (1982) (footnotes omitted).

“The United States Supreme Court has advised that a valid search warrant authorizes the search of any container found on the premises that might contain the object of the search.” ***Commonwealth v. Petty***, 157 A.3d 953, 957 (Pa. Super. 2017) (citing ***Ross***). As a result, if police have probable cause to seize a particular piece of property, that

probable cause permits a search of anywhere where the item could be located. **See Commonwealth v. Turpin**, 216 A.3d 1055, 1060 (Pa. 2019) (holding that Article I, Section 8 “does not preclude a search of the entire residence regardless of whether a particular individual not named in the warrant has an expectation of privacy in certain areas of that residence”). This includes the ability to cursorily examine items to see what they are. **Andresen v. Maryland**, 427 U.S. 463, 482 n.11 (1976) (“[I]t is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.”).

That principle is much easier to apply in the physical world; an officer could not open a closet to search for a stolen vehicle. However, the container analogy breaks down when considering a device like a computer or phone. The United States Supreme Court’s decision in **Riley v. California**, 573 U.S. 373 (2014), held that the search incident to arrest exception does not permit a search of a phone. “Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter.” **Id.** at 397. Moreover, when executing a search of a physical space to seize items, the seizure and search occur more or less simultaneously. Officers who have probable cause to seize a particular item will first search for it then, when it is discovered, seize it. Searching through digital evidence differs in that it usually entails a search for the devices that are seized, followed by a later,

second search of the seized devices, with the later search almost always occurring off-site. **See Commonwealth v. Orie**, 88 A.3d 983, 1008 (Pa. Super. 2014) (“Given the distinctive nature of a USB flash drive, like other types of digital storage systems (*e.g.*, a computer hard drive), it must be *seized* in its entirety first and then *searched* at a later time (typically by someone with an expertise in this area).”) (emphasis in original).

The container analogy can become even more strained when the data “may not in fact be stored on the device itself. ... Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.” **Riley**, 573 U.S. at 397. And the very nature of digital evidence makes it far more difficult to identify in advance which “containers” in the device might hold the sought items. Consider child pornography, as discussed in our Supreme Court’s decision in **Green**. There, authorities discovered that a particular child pornography image was available on a file-sharing network. The affiants determined that the material was shared from Green’s residence, but they could not identify the particular device sharing the file. Thus, the affiants obtained a warrant to seize all electronic storage devices from his home, which would then be taken offsite and “searched for evidence relating to the possession and/or distribution of child pornography.” **Green**, 265 A.3d at 546 (quoting application for warrant). The **Green** Court first concluded that the warrant was not defective in terms of the items to be seized. The next question was whether the

authorized search of the devices seized was overbroad. Green argued that the authorities' probable cause "was limited to the evidence of child pornography shared from his IP address on December 28, 2014, and therefore the warrant was overbroad for failing to include 'specific dates, types of files, [or] specific programs.'" **Id.** at 554 (quoting Green's brief; bracketing in original). This asserted limitation was based on the fact that the affiant downloaded a specific child pornography image. The Court disagreed, stating:

Although Corporal Goodyear personally downloaded an image file depicting child pornography on December 28, 2014, that did not mean probable cause was limited to that particular date or that particular file. The affidavit of probable cause explained that, based on the corporals' experience investigating this type of crime, individuals who download and share child pornography usually maintain a collection of child pornography in a secure, private location for long periods of time. Importantly, the affidavit noted that the user investigated here "had such a collection of child pornography available on a [file-sharing] network." Affidavit of Probable Cause at ¶ 25. These facts established probable cause that someone was sharing a collection of child pornography in general, which is exactly what the warrant permitted the officers to search for and seize. Because probable cause was not limited to the single instance of conduct that [the a]ppellant points to, the warrant did not need to include a specific date, type of file, or program in order to satisfy the requirement to describe the items as nearly as may be.

Id.

Green also argued that the warrant's self-limiting language, which restricted the officers to search for "evidence relating to the possession and/or distribution of child pornography," was not a meaningful check on officers' discretion and was therefore overbroad. The Court responded that this case "is not one where officers were given free rein to look at anything within the

phone to generally look for evidence of a crime.” **Id.** at 554. The Court cited our decisions in **Orie, supra**, and **Commonwealth v. Melvin**, 103 A.3d 1 (Pa. Super. 2014), as cases that properly deemed a warrant overbroad because those warrants permitted rummaging.

The **Green** Court rejected the appellant’s request “to establish a unique overbreadth standard for the contents of electronic devices.” **Id.** at 555. Thus, the **Grossman** standard applies in the physical and digital spheres.

C

Two basic approaches to probable cause

This case requires us to determine how **Grossman’s** standard requiring that the warrant “must describe the items as specifically as is reasonably possible” applies to this set of facts. **Green** illustrates the difficult quandary. On the one hand, probable cause to search for evidence contained in a digital device like a phone will often require quite broad searches to find items for which the authorities have probable cause. But that search, in practice, ends up looking a lot like rummaging due to the differences in searching physical containers versus digital containers. **Green** recognized that the authorities needed to search everywhere on Green’s computer for evidence of child

pornography, as those files can exist anywhere. That search could lead investigators to discover evidence of other crimes.⁸

As an initial matter, we agree with the Commonwealth that some aspects of the trial court's opinion arguably conflict with **Green**. For example, in reviewing Warrant #3, the trial court concluded that "not all items requested ... were supported by probable cause." Trial Court Opinion, 8/10/21, at 10. Its opinion identified the request in Warrant #3 to search the "use of any applications requiring the use of the phone's keyboard, including text, photo, or video message applications, Internet browsers, and applications for voice or video calls" on October 13, October 31, and November 2 of 2019, as particularly problematic. The court concluded that this request was "overbroad and unsupported by probable cause" because it is difficult to imagine "what application, if any, does not in some way require the use of the cellular phone's keyboard." **Id.** at 11. The Commonwealth responds that the proper inquiry "is not whether probable cause existed for all applications using the keyboard on the phone; rather, it is whether probable cause existed for applications using the keyboard on the phone during the time frame sought based upon the information in the affidavit." Commonwealth's Brief at 26.

⁸ Courts have struggled with whether the plain view exception to the warrant requirement makes any sense in the digital search context. "A number of courts have considered the application of the plain view doctrine in computer search cases, and the cases are divided." **State v. Mansor**, 421 P.3d 323, 339 (Or. 2018) (collecting cases).

We note that some decisions from other jurisdictions have applied a “category” approach for smartphone searches. The United States Court of Appeals for the Fifth Circuit panel decision in ***United States v. Morton***, 984 F.3d 421 (5th Cir. 2021), ***overruled on reh’g en banc, United States v. Morton***, 46 F.4th 331 (5th Cir. 2022), is illustrative and has straightforward facts. Morton was stopped for speeding and gave officers consent to search his vehicle. That search revealed three cell phones, sixteen ecstasy pills, and marijuana, leading to his arrest for drug charges. Officers also recovered “children’s school supplies, a lollipop, 14 sex toys, and 100 pairs of women’s underwear in the vehicle,” and based on those items officers suspected that “Morton might be a pedophile.” ***Id.*** at 424. Officers applied for a search warrant for the three phones; however, the affidavit only sought to recover evidence relevant to the drug offenses based on the affiant’s training and experience with drug trafficking. The warrant sought to “search Morton’s contacts, call logs, text messages, and photographs for evidence of his drug possession crimes.” ***Id.*** The warrants were issued and, while searching the phones’ photographs, officers saw child sexual-abuse materials. A second warrant was secured, leading to 19,270 images. Morton was then convicted of possessing those materials.

The initial panel determined that the warrant violated the Fourth Amendment, as probable cause must exist with respect to each “category” of information sought. “As the government properly conceded at oral argument,

separate probable cause is required to search each of the categories of information found on the cellphones.” **Id.** at 425 (footnote omitted). The panel found that its holding “dovetails with the Fourth Amendment’s imperative that the ‘place to be searched’ be ‘particularly describe[ed].’” **Id.** (alterations in original). Thus, the panel viewed the relevant “place” to be searched as a particular area of the phone’s digital contents, as opposed to the entirety of the phone itself. It concluded that probable cause existed to search the “categories” of contacts, call logs, and text messages on the cell phone, but not the “category” of photographs. The panel explained that the key flaw in the search request was that the officers only had probable cause to link Morton to minor possessory offenses, whereas the affiant relied on his experience with drug traffickers. The affidavit explained that “criminals often take photographs of co-conspirators as well as illicit drugs and currency derived from the sale of illicit drugs[.]” **Id.** at 429 (quoting affidavit).⁹ The panel acknowledged that this assertion might be relevant in a case where there was probable cause to establish the individual was a drug trafficker, but

⁹ The United States Court of Appeals for the Fifth Circuit heard the case *en banc* and subsequently decided in the government’s favor based on the good faith exception to the exclusionary rule, finding that the warrant was not “bare bones.” **Morton**, 46 F.4th at 339. As a result, the panel did not squarely address the validity of the warrant. Regarding the original panel’s approach, the **Morton en banc** panel noted that the “categories” concept was relevant to the scope of the warrant and whether it was “bare bones.” “Viewing the entire affidavit against the broad phone search it authorized, it is borderline rather than bare bones.” **Id.**

that was not the case under these facts. ***See also Burns v. United States***, 235 A.3d 758, 777–78 (D.C. 2020) (concluding that the affidavit in support of the warrant “established probable cause to look for and seize evidence likely to be found in at most three narrow categories of data on Mr. Burns’s phones”).

Other courts reject the notion that probable cause must be linked to any particular “category.” Those decisions explain that the very nature of digital evidence resists easy classification and, thus, requiring the authorities to establish probable cause for certain categories of information amounts to an *ex ante* restriction. This view holds that authorities must be given broad discretion to search, because authorities have no way to know what a file contains unless they open it.

Digital evidence also differs from physical evidence in that, for most files, there is no way to know what data a file contains without opening it, meaning that desired data may be located in any part of the digital media or organizational structure. Indeed, data stored on a computer hard drive may be physically located in multiples places on the drive, and it is unhelpful and often inaccurate to think of the data as being located at any particular “place” or “places.” In the physical world, a handgun cannot be disguised as—and will not be mistaken for—a kitchen table, nor will it be found in a pill bottle. But in the virtual world, that kind of deception—or error—is possible. A picture file may be intentionally disguised as a text file, for example, by changing the extension of the file name or by including the picture in a Microsoft Word document, which would be properly saved as a .doc (or similar) file. A picture file may contain text information if, for example, the picture is of a page of a book. Sophisticated users can hide digital data in much more complex ways, including changing date and time metadata and encrypting files so that they cannot be opened. ***See*** Orin S. Kerr, *Executing Warrants for Digital Evidence: The case for use restrictions on nonresponsive*

data, 48 Tex. Tech. L. Rev. 1, 16 (2015) (“Data can always be changed. Maybe the modification will be easy or maybe it will be hard. But it can always be done.”). Similarly, information can be hidden unintentionally. Most of us have had the experience of neglecting to name or properly “save” a document, only to have it disappear into an obscure temporary file, with its sole identifier a number assigned by the software. And even those with limited computer skills can easily delete their internet search “history” on a particular internet browser, although evidence of those searches will likely remain elsewhere on the hard drive. A forensic examiner who locates intentionally (or unintentionally) hidden information on a computer likely has responded to clues, followed instincts, and pursued many dead ends before being successful. **See** Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 545 (2005) (“[G]ood forensic analysis is an art more than a science.”).

State v. Mansor, 421 P.3d 323, 332 (Or. 2018).

This approach recognizes that if this type of search occurred in the physical world it would be materially indistinguishable from rummaging. The ***Mansor*** Court held that the proper balance between the legitimate law enforcement need to conduct comprehensive searches versus an individual’s right to privacy requires suppression of material that does not fall within the “particular evidence” as specified within the warrant.

To satisfy the particularity requirement of Article I, section 9, the warrant must identify, as specifically as reasonably possible in the circumstances, the information to be searched for, including, if available and relevant, the time period during which the information was created, accessed, or otherwise used. We acknowledge that, for practical reasons, searches of computers are often comprehensive and therefore are likely to uncover information that goes beyond the probable cause basis for the warrant. In light of that fact, to protect the right to privacy and to avoid permitting the digital equivalent of general warrants, we also hold that Article I, section 9, prevents the state from using evidence found in a computer search unless a valid warrant authorized the search for that particular evidence, or it is

admissible under an exception to the warrant requirement.

Id. at 326.

IV.

Review of Warrant #3

We now address the validity of the warrants, starting with Warrant #3.

A

No probable cause to search for the majority of items requested

As ***Green*** and ***Grossman*** hold, the natural starting point for this inquiry is addressing probable cause. “Consequently, in any assessment of the validity of the description contained in a warrant, a court must initially determine for what items probable cause existed. The sufficiency of the description must then be measured against those items for which there was probable cause.” ***Grossman***, 555 A.2d at 900. Initially, we reject the Commonwealth’s broad reading of ***Green***. The Commonwealth argues that

Green makes it clear that the Pennsylvania Constitution imposes no *per se* requirement that a search warrant for a digital device be expressly temporally limited, *i.e.*, that the warrant identify specific dates associated with the presence of evidence of criminal activity on the device. Similarly, there is no *per se* requirement that the warrant be categorically limited; the search warrant need not enumerate the exact categories of evidence or particular areas of the device -- files or programs -- that may be searched. Rather, a search warrant for a digital device with “limiting language provided in the warrant and supported by the affidavit of probable cause” will meet specificity requirements under the Pennsylvania Constitution.

Commonwealth’s Brief at 21.

The Commonwealth appears to interpret **Green** to say that its recognition of the need to conduct a comprehensive search of digital devices amounted to a holding that a warrant should be deemed valid provided there is probable cause to search the phone at all, where the affidavit contains “limiting language” cabining the authorities to searching for evidence of the crimes being investigated.

The **Grossman** standard asks for which “items” there exists probable cause, which is an analytically difficult concept in the digital arena. The requirement that the warrant identify the “item” could be read to mean “category,” such that text messages are treated differently than image files. The **Green** Court recognized that digital evidence can be easily disguised or hidden. **Green**, 265 A.3d at 554 n.6 (“[T]he affidavit also explained how easily these files can be hidden, modified, or destroyed, such that the device needs to be searched in its entirety by a qualified computer expert in a laboratory or controlled environment.”). Thus, an officer executing a warrant to search digital evidence cannot determine whether the “items” are present unless and until the device is thoroughly searched. **Green** thus suggests that this type of “category” approach is inappropriate, for the reasons discussed in **Mansor**. Moreover, the Commonwealth is correct that **Green** did not require

a temporal limitation, nor did it require the officers to limit their search to any particular category of evidence, such as image files.¹⁰

However, we “employ[] the principle that the holding of a judicial decision is to be read against its facts.” **Commonwealth v. Resto**, 179 A.3d 18, 22 (Pa. 2018). The probable cause inquiry asks whether “there is a fair probability that contraband or evidence of a crime will be found in a particular place.” **Barr**, 266 A.3d at 40 (citation omitted). The facts in **Green** involved a search of a computer for depictions of child pornography, which are themselves contraband. Thus, the materials targeted by the warrant were

¹⁰ Whether **Green** explicitly rejects the “category” approach in all respects is an issue that is ripe for further development. We are unprepared to say that the **Green** Court definitively rejected the categorical approach in all respects. It may be the case that child pornography cases are treated differently than other investigations for purposes of the “reasonably possible” standard. Additionally, as Appellee states in his brief, our Supreme Court has recognized that Article I, Section 8 protects a right to privacy that goes beyond the United States Constitution. **See generally Commonwealth v. Alexander**, 243 A.3d 177, 207 (Pa. 2020) (explaining that Article I, Section 8 “must be read in conjunction with more abstract considerations of how far the government may encroach on the rights of citizens”).

We also note that the approach outlined in **Mansor** is tempered in at least two critical ways. First, the tradeoff of permitting the authorities to perform expansive searches of digital data is that the discovery of any items that are not responsive to the warrant may not be used. Thus, searching for evidence of child pornography would require suppression of evidence of drug trafficking. Because this case involves an attack on how the warrants were drawn as opposed to how it was executed, that issue is not before us. Second, Oregon requires that the affidavit of probable cause be specific as to “the information” requested and “when it is possible to limit the material searched to a particular time period, that period should also be set out in the warrant.” **State v. Bock**, 485 P.3d 931, 935 (Or. App. 2021).

illegal to possess. In contrast to **Green**, the material targeted by the warrant in this case was not contraband. Instead, the Commonwealth searched the phone for evidence of the crimes.

Additionally, it is quite difficult to separate the probable cause resolution in **Green** from its analysis of the overbreadth question. In rejecting Green's argument that the probable cause was limited to the particular child pornography image downloaded, the **Green** Court pointed out that the target of the investigation was "sharing a collection of child pornography in general, which is exactly what the warrant permitted the officers to search for and seize." **Green**, 265 A.3d at 554. Thus, the "item" for which there was probable cause was a collection of child pornography, which could be anywhere on the device. In that context, a temporal limitation makes little sense as the Court's probable cause calculus did not consider a crime occurring over a particular period of time. Thus, nothing in **Green** suggests that a temporal requirement will never be required. If a temporal limitation is "reasonably possible," then **Grossman** demands its inclusion. In short, while **Green** rejected adding more protections to the **Grossman** standard, the baseline level of **Grossman** still requires more than the Fourth Amendment.

In this case, we find that there was no probable cause to believe that the phone would contain actual evidence of the crimes. As the **Mansor** approach is more favorable to the Commonwealth, we will accept *arguendo* that it applies here; thus, if the authorities had probable cause to believe the

phone contained “items” then the authorities could search the whole phone for those items. The Commonwealth essentially identified four “items” it expected to find on Appellee’s phone: what we will refer to as “trophies” (*e.g.*, photos or videos of items Appellee stole and/or the apartments that he entered), potential communications about the crimes (as reflected in the request to search text messages), location data, and evidence concerning the phone’s flashlight usage.

We begin with the first two of these “items” and conclude that the Commonwealth failed to establish probable cause that those items would be present on the phone. We find support for this holding in the Supreme Court of Pennsylvania’s decision in ***Johnson, supra***, which held that the affidavit failed to establish probable cause to justify any search of Johnson’s phones. Our Supreme Court had granted review “to consider an issue that is not so simple: the permissible scope of ... a warrant, under Article I, Section 8 of the Pennsylvania Constitution, to search an individual’s cell phone for evidence relating to illegal narcotics activity and firearms possession.” ***Id.*** at 578. The plurality did not resolve that issue because it concluded that the affidavit of probable cause failed to support any search of Johnson’s cell phone. In that case, police officers were dispatched to a specific apartment due to a 911 call of shots fired. Officers entered and detained five individuals, including Johnson. Officers observed, in plain view, two bricks of heroin. They also recovered three stolen firearms from the top of the apartment’s hot water

tank. Johnson was arrested and officers seized two cell phones during a search incident to arrest. Officers sought a search warrant for Johnson's cell phones, stating in the affidavit the following:

As a result of the foregoing, your Affiant[s] respectfully request a search warrant issued for the black and gray Apple iPhone cellular phone and the black Samsung flip cellular telephone listed above, as well as any and all electronic and/or digital data contained within the cellular telephone or its storage medias/memory cards, such as incoming/outgoing calls, call logs, emails, personal calendars, cellular internet usage, wireless internet usage, GPS data, contact information, text messages, voice mails, notes, photographic images, IP addresses, contact information, and voice recordings whether or not the electronic and/or digital data has been erased, hidden, password protected or encrypted.

Id. at 580 (quoting affidavit of probable cause).

The lead Justices expressed skepticism that the phones had any connection to the drugs and firearms. "Naturally, one might pause at this juncture to wonder, 'What do appellant's cell phones have to do with the drugs and firearms in the apartment?'" ***Id.*** at 581. The Commonwealth's probable cause argument reduced to the proposition that, where "a drug-dealing operation was being run out of the apartment in which police encountered [the appellant] in the middle of the night, with ... multiple cell phones on his person, there was at the very least a fair probability that evidence of his involvement in that operation would be found in the text messages on those phones." ***Id.*** at 586-87 (quoting Commonwealth's brief; bracketing in original). The plurality rejected the conclusion that probable cause to arrest Johnson for constructive possession necessarily supplied probable cause to search his

phones. **Id.** at 587. The affidavit of probable cause must establish a nexus, and the plurality found one lacking. The affidavit did not allege that Johnson personally possessed, or was even aware of, drugs, guns, or anything else related to the criminal activity. There was “no information about the frequency with which [the] appellant visited the apartment or the duration of time he was present on the night in question.” **Id.** at 588. “Simply put, the affidavit of probable cause in this case provide[d] little more than the bare fact that [the] appellant was present in a place where illegal contraband happened to be found.” **Id.** The Court noted the possibility that an affiant’s specialized knowledge set forth in the affidavit could be relevant, but that it did not apply “under the particular facts of this case” because nothing in the affidavit of probable cause “remotely establish[ed]” that Johnson was a drug trafficker as opposed to a guest where drugs were located. **Id.** That four other people were present in the apartment, while the owner was not, was additional support for that conclusion.

As to the warrant’s alleged overbreadth, the plurality determined that “the probable cause and overbreadth inquiries are not easily separated; on the contrary, as **Grossman** makes clear, it is impossible to consider an overbreadth challenge to a search warrant without taking probable cause into account.” **Id.** at 586. When probable cause is wholly absent, “the warrant is, quite literally in some sense, entirely ‘overbroad.’” **Id.**

Johnson provides some guidance on the probable cause inquiry here. Just as the lead opinion rhetorically asked what Johnson's phones had to do with the drugs and firearms, one wonders what Appellee's cell phones had to do with the alleged home invasion crimes. We recognize that, unlike in **Johnson**, there is a stronger basis to conclude Appellee was linked to criminal behavior. Whereas the appellant in **Johnson** was arguably merely present at a location where drugs and firearms were kept, the affidavit of probable cause in support of Warrant #3 established that Appellee was identified in photo lineups by several eyewitnesses, and he was seen on video surveillance exiting the apartment.

But the affidavit in support of Warrant #3 does not, in our view, establish sufficient probable cause to conclude that a search of Appellee's cell phone would yield any type of "trophy" evidence relevant to the burglaries or criminal trespasses. The probable cause formulation established by **Gates** permits a court to consider "probabilities in particular factual contexts," and courts examining probable cause tend to credit, at least in some circumstances, inferences of human behavior related to the crimes at issue. **See, e.g., Commonwealth v. Lyons**, 79 A.3d 1053, 1065 (Pa. 2013) (finding probable cause to support search of murder suspect's home for evidence where: victim's co-worker indicated Lyons and victim had extramarital affair; victim and Lyons were in frequent contact; Lyons went "on the run" after murder; and affiant stated that in his experience perpetrators

of “gruesome crimes” often leave trace evidence in home); **Commonwealth v. Torres**, 177 A.3d 263, 275 n.5 (Pa. Super. 2017) (noting that “[s]ome federal courts have held that it is reasonable to infer that drug traffickers will often keep drug-related evidence in their residences and businesses”); **id.** at 278 (Moulton, J., concurring) (opining that “evidence of drug dealing unconnected to a home does not, without more, give probable cause to believe that additional contraband will be found in the home”).

A thorough treatment of this concept is set forth in **Commonwealth v. Jacoby**, 170 A.3d 1065 (Pa. 2017). The affiant applied for a warrant to search Jacoby’s home fifteen months after a murder. The **Jacoby** Court determined that the affidavit of probable cause sufficiently established that Jacoby committed the homicide, but it failed to establish a basis to search his home for the potential murder weapon. The detective’s affidavit in support related “that a .32 caliber shell casing was found at the scene of the murder. She further indicated that the casing most likely came from a .32 caliber firearm, possibly one manufactured by Kel-Tec.” **Id.** at 1082. Jacoby was the registered owner of a Kel-Tec .32 caliber firearm. **Id.** The affidavit further related that the weapon sought “is a unique item,” and that Jacoby was a convicted felon ineligible to possess a firearm. **Id.** at 1083. The affidavit concluded it was reasonable to believe Jacoby kept the weapon in his home, even after that long period of time, as he “was likely to retain the weapon due to the difficulty in procuring another one in light of his felon status.” **Id.** The

Court explained that these facts were not sufficient to establish a nexus to Jacoby's home.

Probable cause to search Jacoby's home did not exist simply because probable cause existed to believe that he had committed the murder, with a weapon of the same caliber as one that he owned, and then drove in the general direction of his home fifteen months before the search warrant was issued. Together and by themselves, these factors do not justify entry without some nexus to the home. The trial court overlooked the significant gap of time between the murder and the search, and then attempted to buttress its conclusion with an unsourced assessment of general human behavior. Without support, the trial court reasoned that people—felons especially—generally do not discard firearms, even those used in murders.

This broad perspective on probable cause finds no support in Pennsylvania law and is troubling on several levels. First, the trial court deviated from the search jurisprudence summarized above without acknowledging or attempting to distinguish it. The trial court would hold that, if police officers develop probable cause that a person committed an offense anywhere in the Commonwealth with a weapon of the same caliber as the one that he or she owns, probable cause exists automatically to search that person's home, no matter where it is located. It is easy to discern the infirmity of this approach. If the trial court's reasoning were to prevail, when a person commits an offense with such a weapon in Erie County, police automatically would have probable cause to search that person's home, even if it is located in Delaware County. This is inconsistent with Fourth Amendment jurisprudence.

Additionally, the trial court's method for evaluating probable cause does not require consideration, in any way, of the time lapse between the commission of the offense and the search. Rather than addressing the time gap, the trial court would rest upon its belief that people generally hold on to guns (even those used in murders) and that, as such, probable cause to search for guns exists in apparent perpetuity. By this logic, in the case of the Erie murder, the trial court would find probable cause to search the Delaware County residence not only immediately after the murder, but also fifteen months later, and presumably even ten years after the crime.

Finally, aside from the deviation from the core principles of the Fourth Amendment and Article I, Section 8 that necessarily results from evaluating probable cause in such general, categorical terms, there is another obvious peril in considering probable cause in this manner. People of different genders, races, religions, and backgrounds might respond to certain circumstances differently. Similarly, older people might not conduct themselves as a younger generation would. Mainers might not behave like Texans. There is nothing even to suggest that similar people within the same general category would respond to a set of circumstances in the same way. Probable cause to search Jacoby's home must be evaluated based upon the circumstances of his case, his behavior, and any nexus to the location to be searched, but not upon categorical assumptions. Our Constitutions prohibit such categorical conclusions, as well as those searches that are based upon such conclusions.

The architects of our Constitutions rejected general searches, and instead charged police officers with demonstrating specific and articulable facts to establish probable cause that a particular person committed a particular crime and that evidence of that crime would be found in a particular place. The trial court's approach shortcuts this bedrock inquiry with general assumptions about human behavior, untethered to the actual facts at hand, and was erroneous. For these reasons, we find an absence of probable cause in the warrant to believe that the murder weapon would be found in Jacoby's residence fifteen months after the murder. As such, we need not address Jacoby's staleness argument.

Id. at 1084–85.

Jacoby does not appear to completely foreclose some consideration of the probability that a particular offender will behave in certain ways with respect to assessing whether a sufficient nexus has been established, a point underscored by the ***Green*** Court's crediting the affiant's training and experience of how child pornographers generally act. ***Jacoby*** does, however, hold that categorical assumptions cannot be the sole justification for probable

cause. In that respect, the affidavit here is even weaker than the flawed affidavit in **Jacoby**, because these affidavits did not even attempt to claim that home invaders are likely to have used their phones to aid the commission of their crimes. To reiterate, it is questionable the extent to which a crime like drug trafficking would ever permit a *per se* inference that a phone would contain evidence of drug trafficking. But at least it could be said that the “typical” drug trafficker would use their phones in a manner that justifies a conclusion that the phone is likely to contain some relevant evidence of drug trafficking. There is no obvious link to how a phone would aid the present offenses in the same way that drug trafficking does. As reflected in the very first warrant application—the suppression of which the Commonwealth does not challenge—the affiants merely speculated that the phone may contain evidence of the crime. Application for Search Warrant, 11/11/19, at 3 (“Your Affiants would like to access [Appellee]’s phone to determine if there are any videos that may have recorded the crime, or if [Appellee]’s phone connected [to] WiFi at or around the victim’s apartment to determine his location.”).

We add that in **Johnson**, the Court reserved the question of whether an affiant’s training and experience with drug trafficking could be used to support probable cause to search a phone. On this point, the **Johnson** decision cited, *inter alia*, **Commonwealth v. Morin**, 85 N.E.3d 949, 960 (Ma. 2017), wherein the Massachusetts Supreme Judicial Court offered “some guidance ... on the search of cellular telephones.” **Id.** at 960. “To begin, police may not

rely on the general ubiquitous presence of cellular telephones in daily life, or an inference that friends or associates most often communicate by cellular telephone, as a substitute for particularized information that a specific device contains evidence of a crime.” **Id.**

We are mindful that **Johnson** is a plurality decision and not binding. However, we deem its logic compelling, as supplemented by the preceding discussion. Relying on an assumption that a phone may contain evidence of a crime is the type of generic conclusions in place of individual circumstances that **Jacoby** forbids. The fact that Appellee was seen using his cell phone establishes little more than his using his phone. The **Riley** decision declined to extend the search incident to arrest exception to the warrant requirement to smartphones largely **because** smartphones are so integral to daily life, a phenomenon that has only accelerated in the eight years since **Riley**. Thus, it is quite easy to conjure up reasons why a phone might contain evidence of a crime. “It would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone.” **Riley**, 573 U.S. at 399. **Riley** would amount to a mere paperwork requirement if the Commonwealth could obtain a warrant to search a phone based on little more than the fact that a citizen carried a phone while committing a crime. Thus, the fact that Appellee was seen using his phone in the hallways of the victims’

apartments and commented to Deng that he was sending a text message is of minimal value.

The Commonwealth hypothesizes that Appellee may have taken photographs or videos during the commission of these crimes. Perhaps, but that could be said of any crime, and seeks to enshrine a level of generality in place of individual circumstances, which **Jacoby** forbids. The phone in **Johnson** could have included text messages establishing that Johnson was involved in what looked from the outside to be a drug operation. As in **Johnson**, the notion that Appellee took evidence of his “trophies” or videotaped his crimes rested on pure conjecture. We cannot imagine that, in the era before cell phones became a daily part of life, a court would authorize a search warrant for a home on the basis that such “trophy” photographs would likely be present in a burglary suspect’s home. “[W]hen it comes to the Fourth Amendment, the home is first among equals.” **Florida v. Jardines**, 569 U.S. 1, 6 (2013). **Riley** recognized that records stored on the phone are more comprehensive than what would ever be stored in a home. “Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house[.]” **Riley**, 573 U.S. at 396 (emphasis in original); **Green**, 265 A.3d at 564 (Wecht, J, dissenting) (“The search of all places in a home *and all effects located therein* is more akin to the search of an entire smartphone.”) (emphasis in original).

Finally, there is no indication that Appellee was using his phone to communicate about the crimes. Some decisions have permitted the search of a phone for evidence where specific facts warrant an inference that the phone may have some evidence pertinent to the crimes. ***See Commonwealth v. Dorelas***, 43 N.E.3d 306, 312 (Ma. 2016) (holding that there was probable cause to search phone for evidence of communications where “the defendant had been receiving threatening communications on his iPhone with respect to money he owed to ‘people’ and indeed had been using his iPhone while arguing with an individual immediately prior to the shooting”). Here, the only evidence to hint that Appellee used his phone to communicate are the references to Appellee’s using his cell phone in the hallway and telling Deng he would send a text message. Given the pervasiveness of cell phone usage in daily life, including the use of text messages as a means of communication, we cannot conclude that the affidavit’s references to Appellee using his cell phone established probable cause to believe the phone contained evidence of the home invasion crimes or that Appellee was in contact with potential accomplices. Thus, the warrant was not supported by probable cause to support a search of the phone for what we have described as the first two “items.” We therefore conclude that, even when viewing the warrant with the deference owed to the initial magistrate, there was no substantial basis to conclude the phone would contain those items.

We thus agree with the trial court that the warrant was defective, albeit for slightly different reasons. “[A]s an appellate court, we may affirm on any legal basis supported by the certified record.” **Commonwealth v. Williams**, 125 A.3d 425, 433 n.8 (Pa. Super. 2015) (citation omitted); **Commonwealth v. Parker**, 249 A.3d 590, 593 (Pa. Super. 2021) (addressing potential alternative basis for affirmance where Commonwealth appealed).

B

Probable cause existed for locational data and flashlight use

This case is unlike **Johnson**, however, in that we find that probable cause was not wholly absent. While the affidavit failed to establish a nexus between the crimes and Appellee’s phone to justify a search for the first two types of “items” we previously described, we agree that the affidavit did establish probable cause that Appellee possessed the cell phone while committing the crimes and that he used the cell phone’s flashlight functionality while doing so. Thus, there was probable cause to obtain records concerning the phone’s movement and its flashlight usage, and we agree that a properly drafted warrant seeking those “items” would have been lawful. **Cf. People v. Reyes**, 174 N.E.3d 127, 141 (Ill. App. 2020) (stating that “probable cause to look for GPS data would not necessarily support a search of all of a cell phone’s data”). Indeed, Appellee indicates that there is a much stronger basis to conclude that probable cause existed for these items. **See** Appellee’s Brief at 28 (noting that “probable cause might be found” for locational data generated

by the phone). This raises the question of whether we may sever the invalid portions from the remainder of the warrant. **See Commonwealth v. Casuccio**, 454 A.2d 621, 629 (Pa. Super. 1982) (“It would be totally unrealistic to invalidate [a] warrant *in toto* merely because the affiant and issuing authority erred in seeking and permitting a search for other items as well and we decline to do so.”); **see also Commonwealth v. Bagley**, 596 A.2d 811, 824 (Pa. Super. 1991) (explaining that “[t]he doctrine of severance mandates that invalid portions of a search warrant may be stricken and the remaining portions held valid, as long as the remaining portions of the warrant describe with particularity the evidence to be seized”).

Initially, we address Appellee’s argument that severability is inconsistent with the Pennsylvania Constitution and its broader privacy protections. **See generally Commonwealth v. Edmunds**, 586 A.2d 887 (Pa. 1991) (holding that Pennsylvania Constitution does not recognize good faith exception to exclusionary rule); **see also Commonwealth v. Alexander**, 243 A.3d 177, 183 (Pa. 2020) (“While **Edmunds** involved an application of the exclusionary rule, our holding was tethered to the fundamental concern for privacy within our own constitution.”). Appellee also points out that the Commonwealth “argues in favor of severance, but never addresses the doctrine’s validity or application under the Pennsylvania Constitution.” Appellee’s Brief at 43. That charge is correct, and we add that our Supreme Court has yet to address this issue. **Johnson**, 240 A.3d at 591

(Saylor, C.J., dissenting) (noting the distinction between whether probable cause to search a cell phone exists and the “separate requirement that warrants not be overbroad[,]” and “the associated question of severability”). Nonetheless, our precedents have accepted the severability doctrine, and we decline to announce a departure from federal law in the absence of focused briefing on the issue from both parties. ***Cf. Commonwealth v. Bishop***, 217 A.3d 833, 840 (Pa. 2019) (holding that defendants seeking a new holding departing from federal constitutional law must raise the issue in the trial court and provide reasons supporting that view). We acknowledge that the doctrine has become relevant only on appeal, and Appellee had little incentive to ask for a departure when seeking suppression. By the same token, the Commonwealth had no incentive to argue a “compromise” position. We therefore rely on our existing caselaw and apply the doctrine.

Severability presents a question of law, and we must apply the doctrine as if we were the trial court. Here, the Commonwealth asks this Court to follow the trial court’s lead with respect to all three warrants. Beginning with Warrant #3, the Commonwealth explains that the trial court’s analysis “state[d] that ‘not all items’ were supported by probable cause, clearly implying that a search for and seizure of some, if not the remainder, of the identified items was supported by probable cause.” Commonwealth’s Brief at 38-39. It argues that the trial court merely determined that “applications using the phone’s keyboard was the sole class of items not supported by

probable cause,” and the trial court therefore erred when it “chose to suppress the entire warrant” in lieu of conducting a severability analysis. ***Id.*** at 39. The Commonwealth, however, does not suggest which items should be suppressed, perhaps because it does not wish to concede that probable cause was lacking in any respect. “The suppression court in this case invalidated the entire warrant based upon the conclusion that the search for and seizure of one out of five classes of items was unsupported by probable cause, clearly in violation of the caselaw regarding severance.” ***Id.*** at 40.

Consistent with our foregoing analysis, which departed from the trial court’s analysis in some respects, we find that Warrant #3 was valid only as to the recovery of locational data and evidence concerning the phone’s flashlight use.

At this juncture, we address Appellee’s assertion that severability is not warranted, as a restriction of the doctrine is that it does not apply to general warrants. ***See Casuccio***, 454 A.2d at 630 (applying severance doctrine because “the warrant was not essentially general in character”). Appellee suggests that this warrant was general in character because “the warrants’ descriptions in this case seeks ‘all’ of broad categories of items without limitation.” Appellee’s Brief at 49.

We disagree. This warrant did not authorize a search of “any and all data” on the phone. Warrant #3 specifically delineated several items, and we agree with the Commonwealth that the warrant was quite limited in temporal

scope, as it was confined to the three known incident dates. We agree that those temporal restrictions are relevant and as drawn the warrant did contain a check on the officers' authority. We therefore do not interpret Warrant #3 as authorizing a general rummaging of Appellee's phone, except to the extent that a comprehensive search is often required due to the distinctions between physical and digital searches. We therefore agree with the Commonwealth that severability is warranted, and the Commonwealth may lawfully use the results of Warrant #3 with respect to locational data and any evidence concerning flashlight usage.

V.

Warrant #4 and Warrant #5 must be suppressed

Turning to Warrant #4, the Commonwealth similarly asserts that "this warrant contained legitimate support for numerous classes of items which were tied to the facts and probable cause listed in the affidavit, on which the reviewing magistrate (another Court of Common Pleas Judge) found reason to sign the warrant." Commonwealth's Brief at 41. Finally, for Warrant #5, the Commonwealth suggests that the court "could have deemed fit to suppress any information pre-July 2017 if it existed which would have allowed the supported time period of July of 2017 onwards to remain intact as properly supported. Such a decision would have been a much more proper remedy than *in toto* suppression of the entire warrant." ***Id.*** at 43.

Warrant #4 was effectively the same as Warrant #3 in substantive terms and differed in the place to be searched, with Warrant #3 targeting the phone itself and Warrant #4 authorizing a search of the phone's iCloud backups. Appellee argues that these warrants would not have been executed absent the unlawful execution of Warrant #3, and the warrants must therefore be suppressed as fruit of the poisonous tree. "[G]enerally speaking, the exclusionary rule applies to evidence that was obtained from a search or seizure in violation of the Fourth Amendment. The fruit of the poisonous tree doctrine extends the exclusionary rule to render evidence inadmissible which was derived from the initially illegally obtained evidence." ***Commonwealth v. Santiago***, 209 A.3d 912, 916 n.4 (Pa. 2019).

We agree with Appellee that both warrants must be suppressed in their entirety. First, we agree with Appellee that Warrant #4 would not have been executed without linking Appellee's phone to the iCloud accounts `ralphemek@gmail.com` and `ranlmeks@gmail.com`. The Commonwealth discovered those email addresses during the execution of Warrant #3. Application for Search Warrant, 5/22/20, at 4 (explaining that a partial extraction and examination of Appellee's cell phone revealed it was linked to those two Apple iCloud accounts). Similarly, the execution of Warrant #4 yielded incriminating photographs, which in turn supported Warrant #5.

There is a common problem to both discoveries: it is not clear how the Commonwealth came across this information. Returning to this Court's

adoption of the severability doctrine, the **Casuccio** Court cited Professor LaFave's influential search and seizure treatise as supporting the adoption of the doctrine. We find persuasive an additional observation from this treatise that is pertinent to our analysis:

It has been correctly noted that the "question of whether this kind of surgery might be performed might also depend to some extent upon the facts of each case, e.g., how was the warrant executed?" This is because the items described in the warrant determine the permissible intensity and duration of the search. ... But when other objects are seized under authority of the plain view doctrine (perhaps those objects insufficiently described in the warrant or those objects for which probable cause was not shown in the affidavit), a more careful inquiry into the circumstances is required. If the items were discovered before those to which the warrant was properly addressed were found and while the police were looking in places where the latter objects could be located, then it may be said that the discovery occurred while executing the lawful portion of the warrant. Were the circumstances otherwise, then it must be concluded that these other items were found during execution of the invalid part of the warrant.

2 Search and Seizure § 4.6(f) (6th ed.) (footnotes omitted).

Here, the Commonwealth discovered Appellee's email addresses during the partial execution of Warrant #3, and then discovered photographs when executing Warrant #4. We agree that a search of Appellee's cell phone per Warrant #3 was justified only for locational data and flashlight usage. Thus, the email addresses were not proper subjects of the search. Accordingly, we must conduct a "more careful inquiry into the circumstances" to determine if the Commonwealth was permitted to recover the email addresses, which in turn led to the fourth and fifth warrants.

We conclude that the answer is no for two related reasons. First, as noted *supra* at note 8, the applicability of the plain view exception to digital searches has generated divergent results. The treatise quoted above discusses a search of a physical space, and it is not clear on what basis we could decide whether the discovery of the email addresses and the incriminating photographs “occurred while executing the lawful portion of the warrant.” ***Id.*** There was no evidence presented at the evidentiary hearing concerning the execution of the warrant. Thus, even if we were inclined to apply the “plain view” exception in the digital arena, there is simply no factual record on which to test whether the officers exceeded the scope of their authority. ***See Green***, 265 A.3d at 555 n.7 (“It should be noted that [Green] and amici repeatedly suggest that officers will look through a suspect’s private information once a warrant provides a limited scope of access to a personal digital device. This, however, is a separate issue than the overbreadth claim before us.”). Second, and relatedly, just as we decline to decide Appellee’s argument that the Supreme Court of Pennsylvania would reject the severability doctrine, we are not prepared to address the difficult question of plain view without any advocacy by the parties. The Commonwealth does not claim that the plain view exception applies. Instead, the Commonwealth chose to defend the warrants, both before the trial court and on appeal, on the basis that they are supported by probable cause, and the Commonwealth does not raise any exceptions to the warrant requirement. As our Supreme

Court explained in ***Commonwealth v. Price***, 284 A.3d 165, 173 (Pa. 2022), the “inevitable discovery doctrine is not a subsidiary issue to a claim of adequate probable cause to support the issuance of a search warrant,” as inevitable discovery is an exception to the warrant requirement. Plain view is likewise an exception to the warrant requirement. ***Commonwealth v. McCree***, 924 A.2d 621, 628 (Pa. 2007) (“[U]nder both the Fourth Amendment and Article I, § 8, the plain view exception to the warrant requirement requires a determination of whether the police have a lawful right of access to the object seen in plain view.”). If the record established a clear application of the plain view exception, we could perhaps excuse the failure to raise that issue on the basis that a severability analysis requires a determination of what items were severable on a *de novo* basis. But there is no caselaw establishing that the plain view exception could apply under these circumstances. We therefore decline to consider its application.

As a result, we apply the severance doctrine to permit only the recovery of locational data and usage of the cell phone’s flashlight functions from the execution of Warrant #3. The remaining two warrants are suppressed in their entirety as fruit of the poisonous tree.¹¹

¹¹ The Commonwealth obtained locational data during the execution of Warrant #3. Application for Search Warrant, 5/22/20, at 4 (“On 4/21/20, your Affiant obtained a search warrant. ... Off. Lewis’ search of the cell phone also found [Appellee]’s cell phone had connected to access points for Wi-Fi throughout the ‘W’ building of University Terrace.”).

VI.

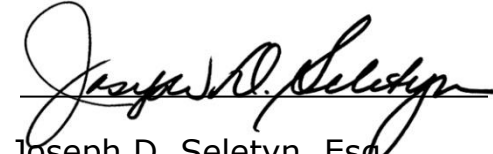
Conclusion

We conclude that Warrant #3 failed to establish probable cause to search Appellee's cell phone for anything other than locational data and usage of the cell phone's flashlight functions. The recovery of those items during the execution of Warrant #3 is severable from the defective portions of that warrant.

We affirm the trial court's ruling suppressing Warrant #4 and Warrant #5 on the alternative basis that those warrants are fruit of the poisonous tree. The record does not establish any basis for the Commonwealth to search Appellee's iCloud data other than the discovery of his email addresses during the execution of Warrant #3. The record further establishes that Warrant #5 would not have been obtained but for the recovery of incriminating photographs during the execution of Warrant #4. There was no probable cause to recover Appellee's email addresses during the execution of Warrant #3, and we decline to apply the plain view exception under these circumstances. We express no opinion on whether that exception applies during digital searches. We therefore remand for further proceedings.

Order affirmed in part, reversed in part, and remanded for further proceedings consistent with this opinion. Jurisdiction relinquished.

Judgment Entered.

A handwritten signature in black ink, reading "Joseph D. Seletyn", is written over a horizontal line.

Joseph D. Seletyn, Esq.
Prothonotary

Date: 04/17/2023