[J-55-2021]
IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT

BAER, C.J., SAYLOR, TODD, DONOHUE, DOUGHERTY, WECHT, MUNDY, JJ.

COMMONWEALTH OF PENNSYLVANIA,	:	No. 6 MAP 2021
	:	
Appellee	:	Appeal from the Order of the
	:	Superior Court at No. 242 MDA
	:	2018 dated February 12, 2019
v.	:	Affirming the Judgment of Sentence
	:	of the Lycoming County Court of
	:	Common Pleas, Criminal Division,
ERIC LAVADIUS GREEN,	:	at No. CP-41-CR-0000191-2015
	:	dated July 14, 2017.
Appellant	:	
	:	ARGUED: September 22, 2021

OPINION

JUSTICE MUNDY **DECIDED: December 22, 2021**

This appeal originates from an investigation into internet sharing of child pornography. During the investigation, officers obtained a warrant to search for evidence of possession and distribution of child pornography on the electronic devices in the home of Appellant, Eric Green. We granted review in this matter to address whether that search warrant was overbroad.

I. Factual Background and Procedural History

On January 14, 2015, the Pennsylvania State Police applied for a search warrant for Appellant's residence. The application included an affidavit of probable cause written by Corporal Christopher Hill (Affiant), who stated that his affidavit was based on information he received from Corporal G. M. Goodyear. Affidavit of Probable Cause at ¶ 2. Affiant explained that Corporal Goodyear conducted undercover investigations into the

sharing of child pornography over the internet. *Id*. at ¶ 20. On December 28, 2014, Corporal Goodyear located a computer that was sharing child pornography on BitTorrent, a peer-to-peer file sharing network.[1] *Id*. Corporal Goodyear was able to download files

[1] These terms were defined earlier in the affidavit as follows:

> **File Sharing** - the practice of distributing or providing access to digitally stored information (computer files), such as computer programs, music files, movie files, picture files, documents, or any other type of computer file. It may be implemented in a variety of storage, transmission, and distribution models. Common methods are manual sharing using removable media, centralized computer file server installations on computer networks, World Wide Web-based hyperlinked documents, and the use of distributed peer-to-peer (P2P) networking.
>
> **Peer-to-Peer (P2P) Networking** - a network of computers composed of participants that make a portion of their resources (such as processing power, disk storage, and network bandwidth) available directly to their peers without intermediary network hosts or servers. Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model where only servers supply, and clients consume (i.e. computer users can both download other peers' computer files, as well as, make their own files available for upload, or "share").

Affidavit of Probable Cause at ¶ 6. The affidavit also provided the following illustration of how a peer-to-peer filing sharing program like BitTorrent operates in practice:

> For example[,] a person interested in obtaining child pornographic images would query a tracker with a search term that he believes will provide a list of child pornographic material. The tracker then responds with a list of possible matching .torrent files[, a filename extension similar to .doc or .pdf]. The results of the search are returned to the user's computer and displayed. The user selects from the results displayed indicating the file he/she wants to download. The files are downloaded directly from the computers sharing them and are then stored in the area previously designated by the user where it remains until moved or deleted.

directly from the user of that computer, which included a photograph of a prepubescent girl wearing a sheer dress with her legs spread as to clearly display her genital area. *Id*. Affiant explained that investigators can ascertain the IP address used by any computer sharing files. *Id*. at ¶ 19. As a result, Corporal Goodyear obtained the IP address for the computer that shared the image. He then utilized the American Registry of Internet Numbers to learn that the IP address was assigned to the internet service provider Comcast Cable Communications (Comcast).[2] *Id*. at ¶ 21. On January 12, 2015, in

---

Id. at ¶ 15.

[2] The affidavit also included definitions for these terms:

> **IP (Internet Protocol) Address**, a numerical identification and logical address that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes. Although IP addresses are stored as binary numbers, they are usually displayed in human-readable notations, such as 208.77.188.166. Every machine that is on the Internet has a unique IP number - if a machine does not have an IP number, it is not really on the Internet.
>
> **American Registry of Internet Numbers (ARIN)** - The American Registry for Internet Numbers (ARIN) is a nonprofit organization, responsible for managing the Internet numbering resources for North America, a portion of the Caribbean, and sub-equatorial Africa. Other registry organizations are separately responsible for registering and maintaining domain names, which are commonly used unique identifiers that are translated into numeric addresses (IP numbers). IP numbers are globally unique, numeric identifiers that computers use to identify hosts and networks connected to the Internet. A free public database lookup is available from their website located at http://www.arin.net. This database can be searched to determine who an [IP] address is assigned. This is usually a large business or an Internet Service Provider (ISP).

Affidavit of Probable Cause at ¶ 6.

response to a court order, Comcast identified Appellant as the subscriber assigned to that IP address and provided his residential address. *Id*. at ¶ 22. Affiant explained that individuals involved in the sharing and downloading of child pornography usually maintain their collections in the privacy and security of their own home, often without the knowledge of others residing with them. *Id*. at ¶¶ 23a, 25. The user identified by Corporal Goodyear "had such a collection of child pornography available on a [file-sharing network.]" *Id*. at ¶¶ 24-25. Therefore, based on Corporal Goodyear's investigation, Affiant stated his belief that a user of a computer connected to the internet at Appellant's address was sharing child pornography on the BitTorrent Network. *Id*.

Affiant also provided extensive details relevant to the search warrant, such as background information about the investigators, their experience with computer-based crimes, and the technical processes involved in investigating those crimes. *Id*. at ¶¶ 1-19. Affiant began by describing his own and Corporal Goodyear's qualifications and certifications, including the fact that they both are certified forensic computer examiners. *Id*. at ¶¶ 3-7. Affiant received training on crimes involving handheld computing devices, basic cell phone investigations, internet investigations, intermediate data recovery and acquisition, and was also specifically trained in BitTorrent investigations. *Id*. Both Affiant and Corporal Goodyear participated in investigations where computers were used to facilitate crimes, including child pornography cases. *Id*. at ¶¶ 4-5. Through their experiences they became "familiar with the techniques and methods of operation utilized by individuals involved in criminal activity to conceal their activities from detection by law enforcement." *Id*.

Based on their qualifications, Affiant stated that he and Corporal Goodyear "know that searching and seizing information from computers often requires investigators to seize all electronic storage devices (along with related peripherals) to be searched later

by a qualified computer expert in a laboratory or other controlled environment." *Id*. at ¶ 7. Affiant explained that this type of seizure, along with a later search, is necessary because:

> a. Computer storage devices (like hard drives, diskettes, tapes, laser disks, and CD-ROMs) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he might store criminal evidence in [a] random order or with deceptive file names or deceptive file extensions. This requires searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.
>
> b. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive codes imbedded in the system, such as "booby traps"), a controlled environment is essential to its complete and accurate analysis.

Id. Affiant also explained that it is necessary to seize peripheral devices for "the analyst to be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence contained therein." *Id*. at ¶ 8.

On January 14, 2015, a magisterial district judge granted the warrant to search Appellant's home based on Corporal Hill's affidavit of probable cause. The warrant identified the items that could be searched for and seized as follows:

> Any and all computer hardware, including, but not limited to, any equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical or similar computer impulses or data. Any computer processing units, internal and peripheral storage devices, (such as fixed disks, eternal hard disks, floppy disk drives, and diskettes, tape drives, tapes, and optical storage devices), peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers), and related communication devices such as modems, cables, and connections, recording equipment, as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware. **These items will be seized and then later searched for evidence relating to the possession and/or distribution of child pornography.** This search is also to include any and all cellular phones, including, but not limited to, any cellular device that can collect, analyze, create, convert, store, conceal, transmit electronic data, and the items associated with any cellular device such as power cords, bases, sim cards, and memory cards.

Application for Search Warrant and Authorization at 1-2 (emphasis added).

On January 15, 2015, Corporal Hill and a team of other officials executed the search warrant on Appellant's home. N.T. Trial, 3/6/17, at 61. Those who executed the warrant included members of the mobile forensic lab, which allowed investigators to preview digital evidence on site. *Id*. During the search, authorities previewed a Samsung Galaxy phone and saw that it contained images of child pornography. *Id*. Appellant admitted that he was the only person who used that phone and that he used the BitTorrent program on the phone and his computer. *Id*. at 62-63. The phone was seized and data was later extracted for evidence of child pornography. *Id*. The forensic search of the phone discovered approximately 100 pornographic photographs of young girls. *Id*. at 7-9.[3] The Commonwealth subsequently charged Appellant with approximately 100 counts of both possession of child pornography and criminal use of a communication facility.

[3] These are the most specific details in the record relating to the execution of the search warrant and the forensic extraction of data from the phone. Notably, these details were

Prior to trial, Appellant filed a motion to suppress. Relevant to the issue before us, Appellant argued that:

> [T]he search warrant in this case [was] overbroad in violation of [Article I section 8 of the Pennsylvania Constitution and under the Fourth Amendment to the United States Constitution]. Here, the warrant allowed the police to seize and analyze and search any and all electronic equipment which would be used to store information without limitation to account for any non-criminal use of said equipment. That is to say, the warrant allows the police to search any and all files on the electronic devices regardless of whether said files were used for criminal purposes as opposed to non-criminal purposes.

Motion to Suppress at 2-3 (internal quotations omitted). Appellant also argued that the warrant was not supported by probable cause because the IP address could have been utilized by a device outside Appellant's residence. *Id*. at 3.

On June 30, 2016, the parties argued the motion to suppress during a hearing before the Honorable Nancy L. Butts. Corporal Hill testified regarding Appellant's challenge to probable cause based on the IP address. He explained that the IP address identified the physical location of the modem providing internet access to the device that was sharing child pornography. N.T. Suppression Hearing, 6/30/16, at 10. However, the IP address could not identify for the investigators the exact electronic device that shared the images. *Id*. at 10-11. Therefore, no information in this case could have led

---

elicited during trial and were not at issue during the suppression hearing. Appellant never claimed, within his motion to suppress or during the suppression hearing, that the officers' method of searching his home or device was improper in any way.

investigators to a particular device. The street address assigned to the IP address was the most specific identifiable location. *Id.* at 11-12.

The parties then argued the breadth issue without further testimony. Appellant claimed that the warrant was overbroad because it allowed officers "to seize all computers, regardless of who they belonged to or who used them or what they were used for, so that they can search all the files and all of the computers looking for child pornography." *Id*. at 15. The Commonwealth responded that the warrant was not overbroad because "there is a clear outline and clear delineation as to what needs to be seized and searched and [the warrant] also describes why those items need to be seized and searched." *Id*. at 17. It was further explained that although the warrant allowed all electronic devices to be searched, the language of the warrant would not allow officers to conduct an in-depth search of a device that did not have a peer-to-peer file sharing program downloaded:

> **THE COURT:** The Commonwealth's argument or this is what I'm hearing is that you may have grabbed all the electronics in a particular space, but if they don't have the BitTorrent Software to them you would immediately stop investigating that electronic device and go to the next one that would have that file-sharing application or program on it.
>
> **[THE PROSECUTOR]:** Correct, Your Honor.

Id. at 17-18. Appellant concluded by reiterating his argument that the warrant was overbroad because it allowed the potential for too many devices to be searched, but acknowledged that "most of the time [officers] can't trace [criminal activity] to a particular computer." *Id*. at 20.

On December 8, 2016, the suppression court issued an order and opinion denying Appellant's motion to suppress. Regarding Appellant's claim that the warrant was

overbroad, the court determined that "the scope of the warrant was sufficiently narrow as to exclude evidence of non[-]criminal behavior" because the warrant sought only "evidence relating to the possession and/or distribution of child pornography." Opinion and Order, Dec. 8, 2016, at 4. The court also held that the IP address provided sufficient probable cause to believe that the device that shared child pornography would be present at Appellant's home address. *Id*. at 6.

On March 6, 2017, during Appellant's bench trial, the Commonwealth introduced 99 pornographic images of young girls that were recovered from Appellant's cellphone. At the conclusion of trial, the Honorable Richard A. Gray found Appellant guilty of 99 counts of possession of child pornography and one count of criminal use of a communication facility. On July 14, 2017, the trial court sentenced Appellant to an aggregate term of four to eight years of imprisonment.

Appellant filed a notice of appeal to the Superior Court, claiming, *inter alia*, that the lower court erred in denying his motion to suppress. A unanimous panel of the Superior Court affirmed Appellant's conviction in a published decision. *Commonwealth v. Green*, 204 A.3d 469 (Pa. Super. 2019). In assessing Appellant's contention the warrant was overbroad, the Superior Court differentiated the instant case from two of its prior cases: *Commonwealth v. Orie*, 88 A.3d 983 (Pa. Super. 2004) (holding a warrant was overbroad for authorizing the search of a flash drive for "any contents contained therein" with no limitation to account for non-criminal use), and *Commonwealth v. Melvin*, 103 A.3d 1 (Pa. Super. 2014) (same, for a warrant requesting "all stored communications" to and from two email addresses). Here, the panel agreed with the suppression court that the warrant was not overbroad, holding that:

> The denial of the motion to suppress was not error. [Appellant] was under investigation for computer-based criminal acts, *i.e.*, possession of child pornography on electronic equipment. The warrant contained a general description of the items to be seized, but permitted the seized devices to be searched only for evidence relating to the possession and/or distribution of child pornography.

Id. at 483 (quotations omitted). The Superior Court also rejected Appellant's argument that the warrant was unsupported by probable cause because someone outside Appellant's residence could have used the IP address associated with his residence. The Superior Court reasoned that "police were not required to prove their suspicion beyond a reasonable doubt, or disprove arguments that [Appellant] might conceivably raise. . . . Rather, to obtain a warrant, police need only show the probability that evidence of criminality is in the place they seek permission to search. The affidavit here made that showing." *Id*.

Appellant filed a petition for allowance of appeal with this Court, which we granted to address the following issue: "Was the search warrant issued for [Appellant's] home and electronic devices overbroad, and did the affidavit fail to establish probable cause?" *Commonwealth v. Green*, 243 A.3d 1293, (Table) (Pa. 2021) (per curiam order).

II. Analysis

Appellant advances two main arguments as to why the search warrant was overbroad. He first avers that the search warrant "was overbroad due to the disparity between the immense number of items requested to be seized and later searched, and the underlying probable cause offered to support the warrant." Appellant's Brief at 12. He also maintains that the search warrant "was overbroad in that the language used to

particularize the search did nothing to curtail law enforcement from searching each and every file on the seized devices." *Id*. We address each of these components in turn.

The first issue is familiar, as it simply deals with the search and seizure of physical items (computers, cell phones, and other electronic devices) within a physical space (Appellant's home). The second issue is novel, as our Court has not before assessed when a search warrant is overbroad regarding a digital search of electronic files contained within a personal electronic device. Although this Court recently granted review of such an issue in *Commonwealth v. Johnson*, 240 A.3d 575 (Pa. 2020), we never reached the issue of whether the language contained in the warrant in that case was in fact overbroad. That was because an overbreadth analysis begins with an assessment of probable cause, and we held as a threshold matter that there was no probable cause to believe any evidence of criminality would be found within Johnson's phone. *Id*. at 590. Nevertheless, this Court in *Johnson* thoroughly outlined the relevant legal standards for an overbreadth challenge as follows:

> Article I, Section 8 of the Pennsylvania Constitution[4] ensures that citizens of this Commonwealth are protected from unreasonable searches and seizures by requiring that warrants: (1) describe the place to be searched and the items to be seized with specificity and (2) be supported by probable cause to believe that the items sought will provide evidence of a crime. *See, e.g.*, *Commonwealth v. Waltson*, 555 Pa. 223, 724 A.2d 289, 292 (1998). Regarding the former requirement, we have interpreted the phrase "as nearly as may be" in Article I, Section 8 "as requiring more specificity in the description of items to be seized than the federal particularity requirement." *Id*. at 291, *citing Commonwealth v. Grossman*, 521 Pa. 290, 555 A.2d 896, 899 (1989) ("The clear meaning of the language is that a warrant must describe the items as specifically as is reasonably possible."). This more stringent requirement makes general searches impossible and "'prevents the seizure of one thing under a warrant describing

another.'" *Grossman*, 555 A.2d at 899, *quoting Marron v. United States*, 275 U.S. 192, 196, 48 S.Ct. 74, 72 L.Ed. 231 (1927); *see also Commonwealth v. Matthews*, 446 Pa. 65, 285 A.2d 510, 514 (1971) ("It cannot be disputed that general or exploratory searches through which officers merely hope to discover evidence of [a]ny kind of [a]ny wrongdoing are not constitutionally permissible.").

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*, 308 Pa. Super. 67, 454 A.2d 24, 25 n.2 (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. For that reason, when assessing the validity of the description contained in a warrant, the natural starting point for a court is to determine for what items probable cause existed. *Id*. at 900. "The sufficiency of the description [in the warrant] must then be measured against those items for which there was probable cause. Any unreasonable discrepancy between the items for which there was probable cause [to search] and the description in the warrant requires suppression." *Id*. This is because "[a]n unreasonable discrepancy reveals that the description was not as specific as reasonably possible[,]" *id*., meaning the warrant is overbroad, ambiguous, or perhaps both.

At the same time, we have also recognized the fact-dependent nature of such claims, and cautioned that "search warrants should 'be read in a common sense fashion and should not be invalidated by hypertechnical interpretations. This may mean, for instance, that when an exact description of a particular item is not possible, a generic description will suffice.'" *Commonwealth v. Rega*, 593 Pa. 659, 933 A.2d 997, 1012 (2007), *quoting* Pa.R.Crim.P. 205, Cmt. In that vein, we have held that "where the items to be seized are as precisely identified as the nature of the activity permits and an exact description is virtually impossible, the searching officer is only required to describe the general class of the item he is seeking." *Matthews*, 285 A.2d at 514; *see also Commonwealth v. Johnson*, 615 Pa. 354, 42 A.3d 1017, 1032 (2012) (search warrant not overbroad where "police were not certain as to the details of the assault and could not know exactly what to specify in the warrant application" and

"[t]hus, they needed only to describe the class of items to be seized"); *Commonwealth v. Sherwood*, 603 Pa. 92, 982 A.2d 483, 504-05 (2009) (descriptions not overbroad, as the warrants "described the items police were seeking as nearly as possible under the circumstances" and the particular evidence sought "could be found in numerous places"); *In re Search Warrant B-21778*, 513 Pa. 429, 521 A.2d 422, 426 (1987) (search warrant not overbroad where "investigators had no legitimate means of discovering information to narrow down the location of the records").

---

[4] Article I, Section 8 provides, "[t]he 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.

Id. at 584-585.

Additionally, our standard of review for the denial of a suppression motion is *de novo* and "is limited to determining whether the suppression court's factual findings are supported by the record and whether the legal conclusions drawn from those facts are correct." *Commonwealth v. Shaffer*, 209 A.3d 957, 968-69 (Pa. 2019). "Our scope of review is to consider only the evidence of the Commonwealth and so much of the evidence for the defense as remains uncontradicted when read in the context of the suppression record as a whole." *Id*. When the sole issue on appeal relates to a suppression ruling, our review includes only the suppression hearing record and excludes from consideration evidence elicited at trial. *Commonwealth v. Yandamuri*, 159 A.3d 503, 516 (Pa. 2017).

With this legal framework in mind, we will address: (1) whether the warrant was overbroad in the items it permitted to be seized, and (2) whether the warrant was overbroad with respect to the digital search of the electronic devices.

A. Items the Search Warrant Permitted to be Seized

The first issue we must address is whether the search warrant "was overbroad in that it authorized seizure of a sweeping list of devices." Appellant's Brief at 11. As we explained in *Johnson*, the natural starting place in assessing the validity of the description contained in a purportedly overbroad warrant is to determine for what items probable cause existed. *Johnson*, 240 A.3d at 587. Probable cause is determined by the totality of the circumstances. *Id*. In determining whether probable cause exists to support a search warrant, the issuing authority is "simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Commonwealth v. Torres*, 764 A.2d 532, 537-38 (Pa. 2001) (citing *Commonwealth v. Gray*, 503 A.2d 921 (Pa. 1986)). A court reviewing the underlying probable cause determination "must view the information offered to establish probable cause in a common-sense, non-technical manner." *Id*. "[P]robable cause is based on a probability, not a *prima facie* case of criminal activity." *Commonwealth v. Housman*, 986 A.2d 822, 843 (Pa. 2009).

Appellant acknowledges that "probable cause existed for law enforcement to seize his phone and computer to look for evidence of the BitTorrent 'seeding' of suspected child pornography observed on December 28, 2014." Appellant's Brief at 15.[4] However, according to Appellant, that is *solely* where probable cause existed, and therefore the warrant was overbroad in requesting to seize "every digital device found at the Appellant's

[4] The affidavit of probable cause describes "seeders" as "clients/peers that are sharing the files." Affidavit of Probable Cause at ¶ 14.

address capable of accessing the internet, as well as all peripheral devices, software, etc., with no restriction on ownership whatsoever." *Id*. at 20. We disagree with this contention, as the affidavit of probable cause supporting the warrant was not as narrow as Appellant would suggest.[5]

We find that there was probable cause to search and seize all digital devices in Appellant's home, and so the warrant was not overbroad by failing to specify only Appellant's personal phone and computer. Corporal Goodyear's investigation in this case led him to an IP address being used by an unknown device to share child pornography. The owner of that IP address, Comcast, subsequently responded to a court order, identified Appellant as the subscriber of that IP address, and provided Appellant's residential address associated with that subscription. With that information, the warrant explained: "Based on the facts set forth in this affidavit, I believe that probable cause exists to believe that a user of the computer utilizing an internet account with a service address of [Appellant's residential address], was sharing child pornography on the BitTorrent network." Affidavit of Probable Cause at ¶ 24. The warrant did not request to

[5] It is worth emphasizing at this point, that in *Johnson*, a point of contention was the fact that no party affirmatively argued or briefed probable cause. Notwithstanding this Court's explicit pronouncement that probable cause "is one of [the] main tenets" of an overbreadth analysis and that the two concepts could not be "meaningfully untangle[d]," *Johnson*, 240 A.3d 585, 586, Appellant forgoes a complete probable cause analysis in his brief. Although probable cause was specifically included in our grant for review, Appellant's brief goes so far as to omit probable cause from the question presented. Appellant's Brief at 6. Instead, he partially concedes that probable cause existed for certain items (his phone and computer) but provides no probable cause analysis for items he claims made this warrant overbroad (every other digital device). *Id*. at 14-15. This is particularly troubling given the fact that both lower courts found that there *was* probable cause to search all electronic devices in his home. In light of our observations in *Johnson*, going forward, litigants should include analysis of any alleged insufficient showing of probable cause as it relates to their overbreadth challenge.

search a particular device or even name a particular user because there was no way for investigators to obtain that information prior to a search. Corporal Hill explained the following in this regard during the suppression hearing:

> Q: Okay. And you can't simply tell by the IP address the exact electronic device that was utilized to connect with a website?
>
> [Corporal Hill]: At times, yes. In this case, no.
>
> . . .
>
> Q: Alright. But just to clarify, there was no information in this case which could – which would have led you to a particular device as opposed to just the IP address?
>
> [Corporal Hill]: Correct.

N.T. Suppression Hearing, 6/30/16, at 10-12. Based on the information available to the corporals at the time they requested the warrant, the pornography could have been shared by any user on any device using the internet in the home. There was no way to narrow this inquiry without conducting a search.

Importantly, the warrant also included self-limiting language that permitted the officers only to search for "evidence relating to the possession and/or distribution of child pornography." This line was critical in focusing the search and seizure to items connected with the criminal activity for which there was probable cause. This limiting language prevented an indiscriminate or discretionary search of the home because any actions taken by the searching officers were restricted to only what could yield evidence of child pornography. The record reflects that this was not an exploratory search, but one "directed in good faith towards the objects specified in the warrant." *Matthews*, 285 A.2d at 514.

Ultimately, given the realistic limitations of this investigation and the nature of this crime, the warrant could not have described the device sharing the contraband with any more detail than the IP address and associated physical address. There was, nevertheless, probable cause to believe that evidence of criminality would be found on a device within the home. Stated simply, the warrant described as particularly as reasonably possible the items for which there was probable cause. Therefore, the warrant was not overbroad in this respect. *See Matthews*, *supra* ("where the items to be seized are as precisely identified as the nature of the activity permits . . . the searching officer is only required to describe the general class of item he is seeking.").

Having concluded that the warrant was not overbroad with respect to the physical items it permitted to be searched and seized, we now address whether the warrant was overbroad with respect to the digital forensic search of the seized devices.

B. The Digital Forensic Search of the Device

To answer whether the warrant was overbroad with respect to the digital search of the device, we must first address whether a different legal standard should apply to an overbreadth challenge to the search of a digital device than the standard already outlined by our Court in *Grossman* and *Johnson*. Appellant suggests that "it is [the] very uniqueness in the often highly private information contained and accessible on [personal] devices, as well as their sheer storage capacity, that supports a more critical view of the language used in the warrant applications to avoid overbreadth." Appellant's Brief at 23. At the outset, this argument is at odds with *Johnson* where we stated, "we see no logical reason why the legal framework articulated in *Grossman* should not apply here [to an overbreadth challenge to the search of a cell phone.]" *Johnson*, 240 A.3d at 565.

Nevertheless, Appellant views the "application of a stricter view of the particularity requirement in searches of digital devices such as his as a logical extension of the reasoning of the Supreme Court in *Riley v. California*, 573 U.S. 373 (2014), and this Court in *Commonwealth v. Fulton*, 179 A.3d 475 (Pa. 2018)." Appellant's Brief at 21.

In *Riley*, the High Court recognized that cell phones often contain a vast amount of highly personal information such that its contents may not be searched without a warrant. In *Fulton*, our Court held that the rule created in *Riley* "is exceedingly simple: if a member of law enforcement wishes to obtain information from a cell phone, get a warrant." *Fulton*, 179 A.3d at 319. A warrant is required to search a cell phone "because, like one's home, an individual's expectation of privacy is in the cell phone itself, not in each and every piece of information stored therein." *Id*. at 316-17. In fact, "a cell phone search would typically expose to the government far **more** than the most exhaustive search of a house." *Id*. (citing *Riley*, 573 U.S. at 396-97) (emphasis in original).

Because a cell phone often contains even more personal information than a home, it logically follows that a warrant should be required to search the contents of a cell phone, just as a warrant is required to search the contents of a home. This rationale, however, does not support the conclusion that, once obtained, a warrant to search a digital device should be held to a higher overbreadth standard than a warrant to search a home simply because of the former's storage capacity. Of course, as discussed *supra*, our Constitution requires that *all* warrants, including warrants to search a digital space, (1) describe the place to be searched and the items to be seized with specificity and (2) be supported by probable cause to believe that the items sought will provide evidence of a crime. In applying this standard, courts must be cognizant of the privacy interests associated with

personal electronic devices. However, just as with a search of a home and other spaces where an individual maintains a privacy interest, if there is probable cause that evidence of a crime will be found within an electronic device, that evidence should not be shielded simply because a defendant comingles it with personal information in a digital space with vast storage capacity. This is particularly so when, like here, the nature of the crime is electronic or internet based.

Thus, consistent with *Johnson*, we hold that the *Grossman* standard for an overbreadth challenge applies equally to the search of a digital space as it does for a physical search. *Johnson*, 240 A.3d at 585. Applying that standard to the digital search in this case, we again look to see whether the warrant described "as nearly as may be those items for which there is probable cause." *Grossman*, 555 A.2d at 899 ("The clear meaning of this language is that a warrant must describe the items as specifically as reasonably possible."); PA. CONST. art. I, § 8.

As discussed earlier, Appellant argues that 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." Appellant's Brief at 15. According to Appellant, the warrant was overbroad because it "allowed for the prohibited 'rummaging' through *all* files on *all* seized devices, nearly all of which contained private, non-criminal material." *Id*. at 16. Appellant's argument again minimizes the depth of probable cause and exaggerates what that warrant authorized in this case.

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 Appellant 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.[6]

Appellant also argues that the warrant's self-limiting language allowing a search only for "evidence relating to the possession and/or distribution of child pornography" did not cure its alleged overbreadth because officers still had access to the entire device and all the personal, non-criminal information therein. As discussed *supra*, it is undisputed that "a warrant cannot be used as a general investigatory tool to uncover evidence of a crime. Nor may a warrant be so ambiguous as to allow . . . the general 'rummaging' banned by the Fourth Amendment." *Commonwealth v. Rega*, 933 A.2d 997, 1011 (Pa.

[6] Even if the investigators had been able to discover some type of identifying metadata or file type prior to the search, the 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. Therefore, the affidavit explained why the warrant could not include the specific details that Appellant argues should be necessary. Again, "where the items to be seized are as precisely identified as the nature of the activity permits and an exact description is virtually impossible, the searching officer is only required to describe the general class of the item he is seeking." *Matthews*, 285 A.2d at 514.

2007) (citation omitted). This case, however, is not one where officers were given free rein to look at anything within the phone to generally look for evidence of a crime. *See e.g.*, *Orie*, *supra*; *Melvin*, *supra*. Instead, the warrant was issued because an unknown user within Appellant's home was under investigation for an internet-based crime. The warrant only allowed the officers to search for evidence of that particular crime. They could not indiscriminately rummage through any and all files as Appellant suggests, but rather could only conduct a digital forensic search "by a qualified computer expert in a laboratory or other controlled environment" and only for evidence of child pornography. Affidavit of Probable Cause at ¶ 7. We are, as the lower courts were, satisfied that the limiting language provided in the warrant and supported by the affidavit of probable cause was specific enough that rummaging would not be permitted, nor would this warrant be used as a general investigatory tool. Because we find that the warrant sufficiently described the items for which there was probable cause, it was not overbroad.[7]

III. Conclusion

[7] It should be noted that Appellant 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. In assessing overbreadth, a reviewing court must determine if the warrant describes the items for which there is probable cause with sufficient particularity. When a warrant is not overbroad on its face, a separate and subsequent issue may be whether the searching officers went beyond the scope of authority granted by that warrant. *See e.g.*, Wayne R. LaFave, 4 *Search and Seizure: A Treatise On The Fourth Amendment*, § 4.10 *Scope and intensity of the search* (6th ed. 2020) ("Assuming that a warrant meets the constitutional requirements of particularity, the descriptions provided are highly relevant in determining the permissible scope and intensity of the search which may be undertaken pursuant to the warrant."). This latter issue is not subsumed within the question granted for review and there was no evidence that such overreach occurred here. As discussed *supra*, the officers conducted an expert forensic search only of devices that contained a file-sharing program and only for evidence of child pornography, which is exclusively what was discovered during the search.

We find no reason to establish a unique overbreadth standard for the contents of electronic devices. Applying the traditional overbreadth standard to the facts before us, we find no error with the lower courts' determinations that the warrant was not overbroad because it described the physical devices and digital data for which there was probable cause as nearly as may be under the circumstances.

Accordingly, the judgement of the Superior Court is affirmed.

Chief Justice Baer and Justices Saylor and Dougherty join the opinion.

Justice Donohue files a dissenting opinion in which Justice Wecht joins.

Justice Wecht files a dissenting opinion in which Justices Todd and Donohue join.