[J-55-2021] [MO: Mundy, J.]
IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT

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

DISSENTING OPINION

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

The search warrant in this case authorized law enforcement to seize all digital devices connected to an IP address that it indicated would "later [be] searched for evidence relating to the possession and/or distribution of child pornography[.]" Search Warrant, 1/14/2015, at 1-2 ("items to be searched for and seized"). The question is whether this broad authorization to seize all devices and search through all data on the digital devices for evidence of possession and distribution of child pornography complied with Article I, Section 8's requirement that the warrant must describe the place to be searched and the things to be seized "as nearly as may be[.]"[1] I join the Dissenting

[1] Article I, Section 8 of the Pennsylvania Constitution provides that "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.

Opinion of Justice Wecht. I write separately to express my view that the search warrant was unconstitutional. Because law enforcement here had established probable cause to believe that Eric Lavadius Green ("Green") was sharing images of child pornography via BitTorrent, and in view of the vast personal information found on digital devices, the magistrate should have authorized only a search for images of child pornography on the digital devices. Absent that limitation, the warrant permitted the type of rummaging prohibited by the Constitution by authorizing the executing officers to search through other private information found on the devices.

This Court has stated that Article I, Section 8 has "twin aims," i.e., "the safeguarding of privacy and the fundamental requirement that warrants shall only be issued upon probable cause." *Commonwealth v. Waltson*, 724 A.2d 289, 292 (Pa. 1998).[2] Further, "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." *Commonwealth v. Matthews*, 285 A.2d 510, 514 (Pa. 1971). We are also guided by the well-established principle that the sufficiency of the description of the items to be searched for and seized must be "measured against those items for which there was probable cause." *Commonwealth v. Grossman*, 555 A.2d 896, 900 (Pa. 1989). Further, "[a]ny

[2] Similarly, the Fourth Amendment prohibits general searches to avoid placing "the liberty of every man in the hands of every petty officer." *Marron v. United States*, 275 U.S. 192, 195-96 (1927) (internal citations omitted). A particular warrant "assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search." *Groh v. Ramirez*, 540 U.S. 551, 561 (2004) (citing *United States v. Chadwick*, 433 U.S. 1, 9 (1977)). The Supreme Court's instruction with regard to seizures applies with equal force to searches – "As to what is to be taken," and as to what is to be searched, "nothing is left to the discretion of the officers executing the warrant." *Marron*, 275 U.S. at 196.

unreasonable discrepancy between the items for which there was probable cause and the description in the warrant requires suppression. An unreasonable discrepancy reveals that the description was not as specific as was reasonably possible." *Id*.

In addressing the concerns applicable to cell phone searches, which would apply to searches on almost all digital information, the United States Supreme Court has observed that a "cell phone search would typically expose to the government far **more** than the most exhaustive search of a house[.]" *Riley v. California*, 573 U.S. 373, 396 (2014). In applying *Riley*, this Court has observed that the "variety of information that can be stored, the details about a person's life that the information can convey, and the length of time the information can remain catalogued in a cell phone, which are carried by the great majority of people, led the Court to conclude that data stored on a cell phone is entirely distinguishable from any physical evidence counterpart." *Commonwealth v. Fulton*, 179 A.3d 475, 485 (Pa. 2018) (citing *Riley*, 573 U.S. at 393-94); *see also In re Search of 3817 W. West End, First Floor Chicago, Illinois 60621*, 321 F. Supp. 2d 953, 959 (N.D. Ill. 2004) ("The capacity of the computer to store … large quantities of information increases the risk that many of the intermingled documents will have nothing to do with the alleged criminal activity that creates the probable cause for a search and seizure.").

For that reason, I disagree with the Majority's position that the search of Green's digital devices should be treated identically to a search of a physical residence for physical things. Majority Op. at 18. The Majority is correct that these searches are held to the same constitutional standard, and that the items to be seized must be "as precisely identified as the nature of the activity permits." *Id*. at 20 n.6 (citing *Matthews*, 285 A.2d

at 514). However, as we explained in *Fulton*, data stored on digital devices is distinguishable from physical evidence, and our consideration thereof must account for the differences. Significantly, digital searches, by their nature, permit the use of modern forensic tools to narrow the content to be searched using specific software, dates, file types, hash values, etc., the combination of which avoids the rummaging that the Fourth Amendment and Article I, Section 8 seek to prevent. *See In re Search of 3817 W. West End,* 321 F. Supp. 2d at 953 (stating that "[a] number of courts addressing the issue have found that the search and seizure of a computer requires careful scrutiny of the particularity requirement"). As Green and Amici cogently argue, "[t]he same mobile device forensic tools ('MDFT') that are currently used to extract data and files from a digital device, can also be programmed to limit the search by targeting the files and data likely to contain the evidence being sought." Green's Reply Brief at 10-11 (citing Amicus Upturn, Inc.'s Brief at 16 (discussing the powerful filtering tools built into MDFTs which allow data responsive to the warrant to be quickly identified and saved, and non-responsive data to be permanently deleted)). The Majority ignores these tools, which were available to law enforcement to narrow and focus the search.[3]

[3] The Commonwealth argues that a search of everything in the devices was authorized because in a home search for drugs, officers are entitled to open dresser drawers and leaf through its contents, potentially exposing items like sex toys or intimate photographs. Commonwealth's Brief at 16-17. Thus, the same is true here: the officers were permitted to look at each and every file to see if it contained evidence of child pornography. The counter arguments, which are largely developed by the Amici, essentially posit that the vast amount of private information on phones and computers distinguishes their searches from those of homes. Phones, unlike homes, store data regarding a person's movements and store deleted information long after it would be physically discarded. *See Riley*, 573 U.S. at 393. Further, they assert that technology has obviated the need for humans to perform that type of intrusive search in the digital sphere.

That there exist technological and other rudimentary tools to minimize a digital search to avoid exposure to non-criminal data has been recognized by the Superior Court. Indeed, the Superior Court has addressed search warrants that utilized procedures to narrow the content to be searched and to avoid the type of rummaging prohibited by the particularity requirement. In *Commonwealth v. Melvin* and *Commonwealth v. Orie*, the Superior Court approved of search warrant procedures authorizing a search process which required first, review by a special master for privilege, and second, limited the search to certain file types and documents containing keywords. *Commonwealth v. Melvin*, 103 A.3d 1, 32 (Pa. Super. 2014); *Commonwealth v. Orie*, 88 A.3d 983, 1003 (Pa.

There is little doubt that technological tools can perform an initial screening function; even the basic search function of common operating systems like Microsoft Windows allows users to filter files by type, such as photographs, videos, or music. This does not end the matter as technology likewise allows the sophisticated user to evade or otherwise frustrate these types of basic filtering. However, the affidavit of probable cause suggests Green was not a sophisticated user of technology. *See* Affidavit of Probable Cause, ¶¶ 17.d, 20 (describing how during the installation of a BitTorrent client, various settings are established, including a default setting to share files; Green's computer was configured to share files).

These arguments address how a search is performed, and I agree with Justice Wecht that technology can provide some level of "guardrails or limitations to account for non-criminal material[.]" Dissenting Op. at 10-11 (Wecht, J.). Simultaneously, just how sophisticated these tools are is not developed in any meaningful fashion by Green, and thus I am unprepared to say at this juncture whether the Fourth Amendment and/or Article I, Section 8 demand that a search warrant for digital devices must state exactly how the search will be conducted, and that topic in my view remains ripe for development in future cases. Presently, I limit my analysis to the fact that the warrant authorized the officers to search for material well beyond images. To borrow the Commonwealth's analogy, a police officer searching Green's home for printed copies of child pornography could open a dresser drawer to see if the photographs were there. The officer could not, however, read through the pages of a diary that happened to be in that drawer. This warrant, however, authorized the officer to do just that if Green happened to store his thoughts in a digital format. *See* infra at 9.

Super. 2014).[4] By contrast, the court found that a warrant authorizing seizure of all stored communications from identified email accounts for a specific period of time to be overbroad because it "did not justify the search of all communications for that period." *Id*. at 1008-09. *Orie* and *Melvin* shed light on the reality that investigators must narrow and tailor searches of digital information to avoid overbroad searches. They also demonstrate that those capabilities exist. *See also In re Search of 3817 W. West End,* 321 F. Supp. 2d at 959 ("[C]omputer technology affords a variety of methods by which the government may tailor a search to target on the documents which evidence the alleged criminal activity… includ[ing] limiting the search by date range; doing key word searches; limiting the search to text files or graphic files; and focusing on certain software programs."). In my view, at a minimum, the underlying warrant was required to specify that it authorized a search for images of child pornography, because that was the scope of the probable cause established.

Here, the affidavit of probable cause described how the Pennsylvania State Police determined that there were likely to be images of child pornography on a digital device at Green's residence. First, it described the background of the investigation. The affiant explained that BitTorrent is a peer to peer ("P2P") file sharing protocol, that "allows the

[4] One of the approved search warrants allowed seizure of computer hardware and search of electronically stored data referencing "Joan Orie Melvin or her 2009 political campaign, and checks, campaign contribution, thank you letters, and mastheads for Joan Orie Melvin's 2009 political campaign, and Orie's 2001-2009 elections or political campaigns, and checks, campaign contributions, thank you letters, and masthead for Orie's 2001 through present political campaigns." *Orie*, 88 A.3d at 1005. Significantly, law enforcement did not view the data within those items, but instead, obtained a second search warrant for the data contained within the computer hard drives, which authorized search of certain file types (Microsoft outlook calendar data, Microsoft excel spreadsheets) and documents containing certain keywords. *Id*. at 1006-07.

user to set up file(s) on a computer to be shared with others running compatible P2P software." Affidavit of Probable Cause, ¶11. It further explained:

> A person interested in obtaining child pornographic images would query a tracker [computer that coordinates file sharing] 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. 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.

Id. ¶15. Additionally, "[d]uring the installation of a BitTorrent client, various settings are established which configure the host computer to share files. Depending upon the client software used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed." *Id*. ¶17.d. Thus, the installation of a BitTorrent client typically creates a setting whereby the host computer will share files.

Then, the affidavit of probable cause set out the specific probable cause relating to Green as follows:

SPECIFIC PROBABLE CAUSE

> 20. On December 28, 2014 at 0815 HRS EST, Corporal GOODYEAR was conducting undercover investigations into the internet sharing of child pornography. He was able to locate a computer which was sharing child pornography on the BitTorrent file sharing network using client software which was reported as uTorrent3.3. He determined that the user of this computer system configured his BitTorrent client software to "seed" files.
>
> Cpl. GOODYEAR was subsequently able to download contraband digital files from this user. The downloaded file(s) were viewed and one of them is described as follows:
>
> **Name of file**: ism-024-074.jpg
> **Type of file**: Image

> **Description**: This image file depicts a prepubescent girl approximately 12 years old sitting on a rocky outcropping in front of an unidentified body of water. The girl has brown hair which is braided and is wearing a multicolored sheer piece of fabric and various bracelets on both wrists. She appears otherwise nude and has her legs spread so as to display her genital area which is clearly visible. In the upper left corner of the image is printed a company logo "LS Island"
>
> * * *

Affidavit of Probable Cause, ¶ 20. The affiant described how law enforcement identified the IP address of the device from which that image was downloaded, and determined it related to a Comcast Cable Communications Inc. IP address for which the subscriber was listed as Green. *Id*. ¶22. The affiant then averred that "I believe that probable cause exists to believe that a user of the computer utilizing an internet account with a service address of 105 N 5th St. Apt 7 Hughesville, PA 17737, was sharing child pornography on the BitTorrent network." *Id*. ¶24.

In consideration of the facts and circumstances conveyed by the affiant, the affidavit of probable cause established probable cause to believe that images of child pornography would be found on devices using the IP address associated with Green's Comcast account. *Commonwealth v. Jones*, 988 A.2d 649, 655 (Pa. 2010) (internal citations omitted) ("Probable cause exists where the facts and circumstances within the affiant's knowledge and of which he has reasonably trustworthy information are sufficient in themselves to warrant a man of reasonable caution in the belief that a search should be conducted."). I agree with the Majority on that point. Majority Op. at 20. However, the averments in the affidavit of probable cause do not establish probable cause for anything other than digital depictions of child pornography that Green downloaded and shared with other users via the BitTorrent protocol.

The warrant, nonetheless, authorized officers to examine material on the devices that went far beyond that. Although the probable cause was limited to images of child pornography, the warrant's only limitation was that officers were only to search for evidence relating to the possession and/or distribution of child pornography. Search Warrant, 1/14/2015, at 1-2. That sentence does not adequately cabin officer discretion or the scope of the search. One officer could read the warrant as authorizing a broad search of every single file on the computer and phone – every spreadsheet, every executable, every deleted text message, every Apple pay record, all of the exercise data on the app tracking Green's steps. To that officer, those pieces of information could be evidence that Green purchased contraband images, could show communications with other persons involved in illegality, could show his movement to demonstrate where and when he looked at contraband images, and could reveal his most personal thoughts regarding his attraction to children. By contrast, another officer could decide to restrict his search to image files and those downloaded or shared via the BitTorrent protocol. His focused search would certainly uncover the collection of child pornography on which probable cause was based, but it would not give the officer access to all the data that together creates a mosaic of Green's life and conduct. *Riley*, 573 U.S. at 394-397 (describing how "[t]he sum of an individual's private life can be reconstructed" through digital data, and in particular, cell phones). The search warrant's authorization for an unlimited search of all data therefore violates the notion that "nothing is left to the discretion of the officers executing the warrant." *Marron*, 275 U.S. at 196.

Thus, the warrant's authorization to search all files on the computer for evidence of possession and/or distribution of child pornography exceeded the scope of probable cause, which only extended to images of child pornography. *Grossman*, 555 A.2d at 900 (providing that the sufficiency of the description must be measured against the items for

which there was probable cause). For that reason, I would hold that this warrant does not adequately describe, as nearly as may be, the things to be searched.

Here, the search warrant should have specified that law enforcement could only search for images in order to target Green's collection of child pornography. Because this search warrant violated the particularity requirement, all evidence seized pursuant to it should have been suppressed. I would reverse the order of the Superior Court and remand to the trial court.

Justice Wecht joins this dissenting opinion.