[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 WECHT **DECIDED: December 22, 2021**

The Fourth Amendment to the United States Constitution was designed to prohibit—*ex ante*—those searches and seizures that are unreasonable. At the time the Amendment was drafted and ratified, the founders were particularly concerned with unreasonable seizures that often occurred through the issuance of general writs of assistance, which permitted government officials to rummage through people's possessions for smuggled goods or contraband, all at the discretion of the officials and without limitation.[1] This practice was denounced as "the worst instrument of arbitrary power . . . since [it] placed the liberty of every man in the hands of every petty officer."[2] To curtail the use of general warrants—and to limit the arbitrary exercise of discretion by government agents—the Fourth Amendment requires that a warrant narrow the breadth of the search by stating the items to be seized and the places to be searched with

---

1 *Boyd v. United States*, 116 U.S. 616, 625 (1886).

2 *Id.* (internal quotation marks and citation omitted).

particularity.[3] Almost a century ago, the Supreme Court of the United States explained that the particularity requirement "makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left the discretion of the officer executing the warrant."[4]

While the times certainly have changed since *Marron* was decided in 1927, our bedrock constitutional principles have not. The Fourth Amendment still prohibits general searches; it still requires search warrant applications to be drafted with particularity. So, too, does the Pennsylvania Constitution. In fact, because Article I, Section 8 requires a warrant to describe the place to be searched and the items to be seized "as nearly as may be,"[5] this Court has held that our Constitution provides even more protection than its federal counterpart.[6] Thus, in Pennsylvania, a police officer requesting a search warrant must be as specific as reasonably possible about the place to be searched and the things to be seized, such that the subsequent search is confined to the limits authorized by a neutral and detached magistrate, which ensures that it is not a boundless hunt for evidence conducted at the investigator's whim.[7]

The present case tasks this Court with deciding how these hoary yet venerable principles apply in the modern age of sophisticated technology. In late 2014 and early

---

[3] U.S. CONST. amend. IV ("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.").

[4] *Marron v. United States*, 275 U.S. 192, 196 (1927).

[5] PA. CONST. art. I, § 8.

[6] *Commonwealth v. Watson*, 724 A.2d 289, 291 (Pa. 1998).

[7] *See Commonwealth v. Matthews*, 285 A.2d 510, 514 (Pa. 1971) (explaining that our Constitutions prohibit exploratory searches where "officers merely hope to discover evidence of [a]ny kind of [a]ny wrongdoing.").

2015, the Pennsylvania State Police ("the PSP") conducted an undercover investigation of an internet-based distribution network for child pornography. During that investigation, the PSP learned that an internet-capable computer linked to an IP address associated with Eric Green's residence was using a file sharing program called BitTorrent to obtain and distribute images of child pornography. The PSP applied for, and obtained, a search warrant for Green's residence.[8] On the warrant application, the PSP listed Green's residence as the place to be searched and identified the following as items to be seized:

> 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, tape, and optimal storage devices), peripheral input/output devices (such as keyboard, 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, memory cards.[9]

The affidavit of probable cause submitted in support of the warrant extensively described the investigating law enforcement agents' training and experience, the nature and difficulties attendant to investigations of internet-based crimes involving child pornography, the necessity of seizing various electronic devices and their associated

---

[8] Notably, on the face of the warrant application, the PSP listed only Green's residence as a place to be searched. The PSP did not indicate on the face of the warrant whether any electronic devices seized during the search of Green's home also would constitute places to be searched. *See* Application for Search Warrant, 1/14/2015, at 1.

[9] *Id.*

peripherals for subsequent searches, and the information giving rise to probable cause in this case.

However, with regard to the actual demonstration of probable cause to support the sweeping search that the PSP sought in this instance, the PSP noted only that it had identified a single computer that had been using BitTorrent for purposes of sharing child pornography.[10] Despite asserting probable cause for a single device, the PSP nonetheless asked to search for "[a]ny and all" electronic devices inside the home. The vast authorization the PSP sought was not based upon any individualized suspicion of Green's potentially criminal activities, but instead upon, *inter alia*, the PSP's general belief that those who possess or distribute child pornography "sometimes" keep copies of the illicit contraband "in the privacy and security of their home."[11] The PSP did not assert that specific probable cause existed to believe that Green had done so, only that some people "sometimes" do. Based upon the apparent probable cause as to this one device, and the generalized assertions about how offenders of this type are believed to act, the PSP was issued a warrant allowing its troopers to seize virtually any device in Green's home capable of electronic storage and to search anywhere on those devices for evidence related to the receipt, distribution, or possession of child pornography. For all practical purposes, the PSP was permitted to enter Green's residence, seize any devices with a plug, remove them from the property, and then rummage through every digital file and any app on each device—without limitation—in the "hope [of] discover[ing] evidence of

---

[10] Affidavit of Probable Cause, 1/14/2015, ¶ 20 (stating, in the section entitled "Specific Probable Cause," that Corporal Goodyear "was able to locate ***a computer*** which was sharing child pornography") (capitalization normalized; emphasis added); *id*. ¶ 24 (providing the belief that "probable cause exists to believe that a user of ***the computer*** utilizing an internet account with a service address" that matched Green's address "was sharing child pornography").

[11] Id. ¶ 23c.

any kind of any wrongdoing."[12] The result was the discovery of approximately one hundred images of child pornography on Green's smart phone.

The Majority discerns no constitutional problems with the expansive seizure and searches that occurred in this case. In my view, the Majority's decision eviscerates the particularity requirement as it applies to searches and seizures of digital devices—a problematic result in this day and age when more and more private information is being stored on our laptops and smart phones. The result enables police to conduct unbridled scavenges of digital devices that would not be permitted when performing a search in any other context.

As I noted recently, in the twenty-first century, an "inextricable relationship . . . has developed . . . between a person and his or her internet-capable device."[13] I explained:

> Cell phones, smart devices, and computers have evolved in a way that integrates the internet into nearly every aspect of their operation and function. Advancements in the ability to use the internet have turned communication technologies that once were futuristic and fantastical gadgets possible only in the world of the Jetsons or Dick Tracey into everyday realities. Physical distance is no longer a barrier to face-to-face interaction. Applications such as Zoom, WebEx, and Skype allow face-to-face, personal, professional, and educational discussions that previously could be performed only in person or by conference call or telephone call. We now have at our fingertips the ability to manage our calendars or access an unlimited amount of information, regardless of where we are located. Instantaneously, a person can check news reports, weather forecasts, sports scores, and stock prices. Modern matchmaking and dating commonly now begin with internet connections. As time passes, the internet has come to be used and relied upon in nearly every aspect of our daily lives, from organizing family reunions, to scheduling medical

---

12 *Matthews,* 285 A.2d at 514 (capitalization adjusted).

13 *Commonwealth v. Dunkins*, ___ A.3d ___, 2021 WL 5346732, at *16 (Pa. 2021) (Wecht, J., concurring in part and dissenting in part).

> appointments, to conducting academic research, to operating every aspect of a business.[14]

This near omnipresence of smart phone usage in today's society has led to some seismic shifts in search and seizure law. The Supreme Court observed that smart phones have become a "feature of human anatomy"[15] and "such a pervasive and insistent part of daily life"[16] that "carrying one is indispensable to participation in modern society."[17] Because of this novel and important function, the Court held that police may not open or access such a device without a search warrant, even when the device is seized pursuant to a lawful arrest.[18] The Court then held that individuals have an expectation of privacy not just in the content on the devices, but also in the records that are generated by those devices. That expectation was so intertwined with contemporary existence that the Court held that it persists even in the face of some of the most fundamental and long-standing limitations on the Fourth Amendment, including the traditional principles that one does not possess an expectation of privacy while moving in public or when information is shared with third-parties.[19]

As courts throughout the country endeavor to ensure that technological innovation does not become an excuse for governmental overreach, today's Majority chooses a different approach—one that ignores the realities of how these devices work and how

---

14 *Id.*

15 *Riley v. California*, 573 U.S. 373, 385 (2014).

16 *Id.*

17 *Carpenter v. United States*, ___ U.S. ___, 138 S.Ct. 2206, 2220 (2018).

18 *Riley*, 573 U.S. at 386.

19 *See Carpenter*, 138 S.Ct. at 2214-20.

they are used—thereby sanctioning the modern equivalent of the general warrant that the framers so despised.[20]

The typical smart phone (or laptop) user stores a significant amount of personal information on his or her devices. These devices likely contain medical records, personal schedules of the user or his or her family, intimate correspondence stretching back a decade or more, journal entries containing one's innermost thoughts, financial records, or confidential business documents. Rather than contemplate how police officers must craft a search warrant in order to maintain the constitutional boundary between the evidence that law enforcement possesses probable cause to believe is connected to the alleged crime and those private materials that unquestionably are not within that category, the Majority gives officers free rein to scour all digital files and any application on the phone or computer in hopes of locating incriminating information. Under the Majority's rule, a police officer need only seek permission to seize "any and all" electronic devices inside a home, and so long as the officer provides probable cause as to one of them, a subsequent search of every file, photo, history, application, and storage folder on those devices, without any sort of limitation, does not run afoul of the Constitution. In the absence of concrete guidance, the Majority effectively would give law enforcement unfettered access to years' worth of browsing history, bank records, and conversations—provided only that these are located on an electronic device. On little else than a mere showing of probable cause that *an* electronic device was connected to *some* crime, the whole of an individual's

---

[20] *See* Maj. Op. at 18-19 (declaring that a search of one's phone is not distinct in a meaningful way from a search of one's home and thus holding that "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"). The Majority inaptly equates the search of an entire home with a search of an entire cellphone. The search of all places in a home *and all effects located therein* is more akin to the search of an entire smartphone.

world will be unveiled and broadcast to the government's prying eyes. I cannot square this holding with any reasonable interpretation of the particularity requirement. Nor can I comprehend how such a broad holding protects the interests underlying that requirement.

Our Superior Court has addressed similar overbreadth challenges in *Commonwealth v. Orie*,[21] and in *Commonwealth v. Melvin*.[22] In *Orie*, former State Senator Jane Orie was convicted of a number of offenses in connection with her legislative staff's participation in campaign-related work. As part of the investigation into those activities, law enforcement obtained and executed approximately twenty search warrants. Orie argued that the warrants were overbroad and permitted the police to engage in unconstitutional fishing expeditions.

The Superior Court found no overbreadth issues with all but two of the warrants. However, one search warrant permitted the seizure of a flash drive that Orie had provided to a member of her staff. The warrant authorized a search of the flash drive for "any contents contained therein, including all documents, images, recordings, spreadsheets or any other data stored in digital format,"[23] without any restrictions to account for contents that law enforcement did not have probable cause to believe contained inculpatory information. Another warrant was for Orie's personal email account, authorizing the police to seize to "all stored communications and other files . . . between August 1, 2009 and the present, including all documents, images, recordings spreadsheets or any other data stored in digital format."[24]

The Superior Court first explained that the particularity clause

---

21 88 A.3d 983 (Pa. Super. 2014), *allocatur denied*, 99 A.3d 925 (Pa. 2014) (*per curiam*).

22 103 A.3d 1 (Pa. Super. 2014).

23 *Orie*, 88 A.3d at 1008.

24 *Id.*

> is a fundamental rule of law that a warrant must name or describe with particularity the property to be seized and the person or place to be searched . . . . The particularity requirement prohibits a warrant that is not particular enough and a warrant that is overbroad. These are two separate, though related, issues. A warrant unconstitutional for its lack of particularity authorizes a search in terms so ambiguous as to allow the executing officers to pick and choose among an individual's possessions to find which items to seize. This will result in the general "rummaging" banned by the [F]ourth [A]mendment. A warrant unconstitutional for its overbreadth authorizes in clear or specific terms the seizure of an entire set of items, or documents, many of which will prove unrelated to the crime under investigation . . . . An overbroad warrant is unconstitutional because it authorizes a general search and seizure. [25]

Drawing from these general principles, the Superior Court found the warrants for the flash drive and the email account to be constitutionally overbroad because the descriptions of the places to be searched and the things to be seized failed to include a "limitation to account for any non-criminal use."[26]

Similarly, in *Melvin*, the police obtained search warrants for two of former Justice Melvin's personal email accounts.[27] As in *Orie*, the Superior Court found that the warrants permitted the police to seize and search every email in the accounts, including those that bore no relation to criminal activity. In both cases, the relevant warrants permitted the seizure of every email in the account without any attempt to distinguish the potentially relevant emails from those unrelated to the investigation[.]"[28] Thus, the court reasoned

---

[25] *Id.* at 1002-03 (quoting *Commonwealth v. Rivera*, 816 A.2d 282, 290 (Pa. Super. 2003)).

[26] *Id.* at 1008. Despite finding the warrants to be overbroad, the Superior Court concluded that Orie nonetheless was not entitled to relief because the actual search of the drive and the email was performed pursuant to a second, constitutionally issued warrant. *Id.* at 1009.

[27] *Melvin*, 103 A.3d at 17.

[28] *Id*. at 17-18.

that the warrant for Melvin's email accounts permitted a general search and seizure that was unconstitutionally overbroad.[29]

Although not binding on this Court, *Orie* and *Melvin* nonetheless are, in my view, persuasive. Both decisions are consistent with, and meaningfully enforce, the protections provided by the particularity requirement. The Majority does not substantively attempt to discuss, distinguish, or even overrule these cases. But it is hard to discern how *Orie* and *Melvin* can remain on the books harmoniously with the Majority's decision in the present case. The Majority briefly explains that this case is unlike *Orie* and *Melvin* because this case is "not one where officers were given free rein to look at anything within the phone to generally look for evidence."[30] But that is exactly what happened here. PSP personnel developed probable cause for one device that they believed was located in Green's home. Based upon that suspicion, the PSP obtained a warrant for "any and all" electronic devices in the home, including keyboards, disc drives, and even scanners. Once seized, the PSP was allowed to take that equipment and then search every aspect of those devices for evidence.

As with *Orie* and *Melvin*, there was nothing set forth in the warrant before us to account for the presence of data or files that were not reasonably connected to the alleged crime. That the affiants stated that they were looking for evidence of distribution or possession of child pornography is no limitation at all. Such a statement informs the authorizing judicial officer as to *what* law enforcement agents are looking for, but it does not limit *where* they can look or *how* they must confine the technical parameters of their search to limit the exposure of unrelated, non-inculpatory personal information. It is

---

[29] *See id.* at 17-19. Ultimately, the Superior Court held that the error was harmless, and that Melvin was not entitled to relief. *Id.* at 19-22.

[30] Maj. Op. at 21.

difficult, if not impossible, to discern any cohesion between *Orie* and *Melvin* and this case. It seems to me axiomatic that if police officers cannot search a flash drive or an email address without guardrails or limitations to account for non-criminal material, then they likewise cannot search every file and folder stored on larger devices that contain much more information in the absence of similar restraints.

For further indicia of overbreadth, one need look no further than the first three words of the description of the items to be seized section of the warrant, "any and all." A number of courts have found that the use of this phrase in warrant applications led to constitutionally overbroad searches. For instance, in *United States v. Otero*, the Tenth Circuit Court of Appeals considered a warrant that described fourteen categories of items to be seized, some of which were computers or digital equipment, each of which began with the phrase "any and all."[31] The court first noted that the "modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important."[32] Because the particularity requirement must "affirmatively limit" the search to evidence related to the crimes suspected, the court found that the "any and all" warrant was overbroad in violation of the federal particularity requirement.[33]

Similarly, in *State v. Henderson*, the Supreme Court of Nebraska invalidated a search warrant for a smart phone that permitted the seizure of "any and all information"

---

31 563 F.3d 1127, 1130 (10th Cir. 2009).

32 *Id.* at 1132.

33 *Id.* (citing *United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005)). Although the warrant was invalid, the court did not order the seized evidence to be suppressed, finding that the warrant was executed in good faith. *Id.* at 1136.

from the device, and of "any other information that can be gained from the internal components and/or memory [c]ards."[34] The Court explained that such broad warrants contravene the particularly requirement because "they do not sufficiently limit the search of the contents of the cell phone."[35]

The warrant issued in this case is as overbroad as those in *Orie*, *Melvin*, *Otero*, and *Henderson*. None of the warrants in any of those cases limited the searches in a constitutionally meaningful way, leaving the searches to the discretion of the officers. The same is true here. The decisions as to where to look, what files or applications to open, and how deeply to dig all were left to the discretion of the officers. Nothing in the warrant to search and seize Green's electronic devices prevented law enforcement from examining any banking, social media, text messaging, or shopping apps on Green's device. But the warrant contains no indicia that any such apps would produce information connected to those effects within the phone. Similarly, the warrant contained no temporal limitations. Under its broad language, the warrant allowed police officers to search for information that was stored in the phone long before any crimes occurred, even though the investigators had reason to believe only that Green's crime occurred within a specific timeframe. Facially, these consequences fail our particularity requirement.

It is tempting to validate or accede to the broad allegations made by the PSP in the affidavit in support of its warrant application, finding particularity where it does not exist. For example, in the affidavit, the PSP asserts, *inter alia*, that those who collect and distribute child pornography "sometimes" maintain those images in a secure, private

---

[34] 854 N.W. 2d 616, 633 (Neb. 2014).

[35] *Id.* As with *Otero*, the *Henderson* Court ultimately held that, despite the unconstitutionality of the warrant, suppression was not required because the warrant was executed in good faith. *Id* at 634-35.

location for long periods of time.[36] Search warrants, however, must be particularized, that is, based upon individual facts and circumstances,[37] not based upon a police officer's belief as to how some individuals "sometimes" will act.[38] Broad-based assumptions of human behavior are sufficient neither to establish probable cause nor to satisfy the particularity requirement. The PSP did not offer specific probable cause that Green's conduct conformed to its assumptions.

The PSP also relied upon its belief that "a suspect may try to conceal criminal evidence, and he might store criminal evidence in random order or with deceptive file names or deceptive file extensions,"[39] in asserting that such a broad search and seizure was necessary. Again, however, the PSP did not assert any probable cause to show that Green was storing his files in such a way, or that he was engaging in such deceptive practices. Without any individualized beliefs, the PSP effectively is asking to perform certain actions because Green *might* act as others "sometimes" act. The problem with this type of reasoning is easily illustrated with a hypothetical. It is indisputable that a police officer can search only those areas for which there is "a fair probability that contraband or evidence of a crime will be found."[40] Thus, if a police officer obtains a search warrant to look for a rifle, the officer cannot look for that weapon in a woman's purse. A rifle cannot fit in a purse. Since it cannot be there, the police cannot look there.

---

36 Affidavit, 1/14/2015, ¶ 25.

37 *See City of Indianapolis v. Edmond*, 531 U.S. 32, 37 (2000) (citing *Chandler v. Miller*, 520 U.S. 305, 308 (1997)); *Commonwealth v. Mistler*, 912 A.2d 1265, 1271 (Pa. 2006).

38 *See, e.g.*, *Commonwealth v. Jacoby*, 170 A.3d 1065, 1085 (Pa. 2017) (rejecting a search warrant predicated upon the general belief that gun owners, even those who use the gun to commit murder, do not discard those firearms).

39 Affidavit, 1/14/2015, at 4.

40 *Illinois v. Gates*, 462 U.S. 213, 238 (1983)

By the PSP's logic in its affidavit, and via the Majority's approval, the police officer in the hypothetical still would be able to search in the purse, so long as the officer asserts in the affidavit that a person *could* dismantle the rifle into parts and then hide them throughout the house, including in a purse. The officer would not need to assert that the suspect actually did so, or even that he has probable cause to believe the suspect did so. The officer only would have to state that some other people "sometimes" *might* do so, and the entire house would be available to be searched. Clearly, this type of generalized conjecture does not comport with the constitutional requirement of a "fair probability" that the item will be located in a particular place. Yet, in this case, and in the context of searches for digital data generally, the Majority nonetheless allows searches predicated upon such bald extrapolations.

To further emphasize the breadth of the warrant at issue in this case, consider one more hypothetical, one in which the present facts are slightly modified. Assume that this same warrant was issued for a residence in which three people lived: a husband, a wife, and their fourteen-year-old daughter. The warrant, predicated upon probable cause that the husband used a desktop computer to share child pornography, authorizes the police to seize the husband's iPad, the wife's laptop, the daughter's smart phone, the family's scanner, and a long-since obsolete fax machine held over from years before. The police can retain those devices for as long as it would take for them to be searched. It could be days, weeks, or even months. Once those devices were submitted to trained experts, every file, program, or folder contained on those devices would be available for probing and inspection. If the police were searching for photographs of child pornography, nothing would prohibit the officers from scouring the wife's personal calendar. If they are looking for audio files, they can read every page of the daughter's personal diary. If they are seeking only documents, they nonetheless can pore over countless personal,

confidential messages passed between the girl and her friends or love interests. The warrant places no bounds on the police at all.

The particularly requirement is necessary to ensure that "nothing is left to the discretion of the officer executing the warrant."[41] Here, however, everything was left to the discretion of the PSP. Fairly read, this warrant permitted the PSP—based upon probable cause for a single device—to seize "any and all" electronic devices from the home, to keep them for however long was deemed necessary, to turn them over to some expert at some future date, and to have them searched without constraint by those technicians. Simply put, the warrant authorized the PSP to take *any* device and to search *anywhere* on that device. This is precisely the general exploratory expedition that the particularity requirement was designed to thwart.

Our Constitution requires that warrants describe the places to be searched or the things to be seized "as nearly as may be."[42] It is a heavy burden, but not an insurmountable one. That requirement does not preclude police from obtaining warrants. It merely requires them to write warrants in a way that circumscribes the parameters of the requested searches. It is not unreasonable to require that the warrant "tell the officers how to separate the items subject to seizure from irrelevant items."[43] In this case, for example, the PSP had probable cause to believe that Green was using BitTorrent to share and collect images of child pornography. The PSP could have sought a warrant for

---

41 *Marron*, 275 U.S. at 196.

42 PA. CONST. art. I, § 8.

43 *Davis v. Gracey*, 111 F.3d 1472, 1478–79 (10th Cir. 1997) ("We ask two questions: did the warrant tell the officers how to separate the items subject to seizure from irrelevant items, and were the objects seized within the category described in the warrant?"); *see also United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982) (Stating that a request to search must be accompanied by "sufficiently specific guidelines for identifying the documents sought . . . [to be] followed by the officers conducting the search.").

devices capable of running that program, and for a search of only those programs on the devices that interact with that program. There was no probable cause to believe that Green (not child pornographers generally) was using electronic devices for any other purpose. Such a search would preclude the PSP from searching, for example, digital calendars, notetaking applications, or medical records on the device that cannot be used with the BitTorrent program. And it would place the discretion of where to search in the hands of the issuing judicial officer and not the investigator. The warrant in this case was not limited in any way, but, instead, allowed police officers to rummage anywhere they wanted on any device they seized, regardless of whether the PSP had any indication that the particular device was the one running the BitTorrent program.

Because the Majority endorses this unconstitutional rummaging, I dissent.[44]

Justice Todd and Justice Donohue join this dissenting opinion.

---

[44] Because these situations largely are fact and circumstance dependent, setting forth a specific protocol on how to search for digital data may be premature at this point. I note that there is a national debate on whether courts should create such protocols, and, if so, what they might look like. *See Henderson*, 854 N.W.2d at 633 (collecting sources). Some courts already have developed such requirements. For instance, in *In re Application for Search Warrant*, 71 A.3d 1158 (Vt. 2012), the Supreme Court of Vermont held that digital searches: (1) should be conducted by trained computer experts working behind a firewall to ensure that no one views non-criminal material that officers are not permitted to view, such that investigators only get the information related to the underlying offense after the expert uncovers that information; (2) should be conducted using specific and limiting software; and (3) should limit the copying of files so that only relevant material gets turned over to the police while all else is returned to the owner immediately. *Id*. at 1184-85. While these protocols appear sound as a general matter, any proposal for their adoption in Pennsylvania should await contextualized consideration in an appropriate future case.