

**IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT**

No. 6 MAP 2021

COMMONWEALTH OF PENNSYLVANIA,

Appellee,

v.

ERIC LAVADIUS GREEN

Appellant.

Brief Amici Curiae of the American Civil Liberties Union, American Civil Liberties Union of Pennsylvania, the Defender Association of Philadelphia, and the Pennsylvania Association of Criminal Defense Lawyers in Support of Appellant Eric Green

Appeal from the Order of the Superior Court at No. 242 MDA 2018 dated February 12, 2019 Affirming the Judgment of Sentence of the Lycoming County Court of Common Pleas, Criminal Division, at No. CP-41-CR-0000191-2015 dated July 14, 2017.

David Rudovsky, Pa. I.D. No. 15168
Kairys, Rudovsky, Messing,
Feinberg & Lin LLP
718 Arch Street #501
Philadelphia, PA 19106
(215) 925-2298

Peter E. Kratsa, Pa. I.D. No. 71009
President, Pennsylvania Association of
Criminal Defense Lawyers
Macelree Harvey, Ltd.
17 West Miner Street
West Chester, PA 19382

Aaron J. Marcus, Pa. I.D. No. 93929
Leonard Sosnov, Pa. I.D. No. 21090
Defender Association of Philadelphia
1441 Sansom Street
Philadelphia, PA 19001
(215) 568-3190

Andrew C. Christy, Pa. I.D. No 322053
ACLU of Pennsylvania
P.O. Box 60173
Philadelphia, PA 191902
(215) 592-1513 x138

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES	ii
STATEMENT OF INTEREST OF AMICI CURIAE	1
SUMMARY OF ARGUMENT	3
ARGUMENT.....	6
I. Search Warrants Permitting Broad and Unlimited Digital Searches Violate the Particularity Requirement of the Fourth Amendment and Article I, Section 8 of the Pennsylvania Constitution.....	6
II. The Proper Application of the Particularity Requirement for the Scope of a Search Is Critical to Ensuring that Searches and Seizures Pursuant to a Warrant Are Reasonable.	12
III. As This Case Shows, Courts Have a Number of Options in Preventing Overbroad Searches.....	18
1. Search Protocols Imposed by the Issuing Authority	19
2. Post-Search Court Review	23
3. Use Restrictions	24
4. The Plain View Exception	25
CONCLUSION	27

TABLE OF AUTHORITIES

Cases

<i>Andressen v. Maryland</i> , 427 U.S. 463 (1976)	7
<i>Arizona v. Gant</i> , 556 U.S. 332 (2009)	25
<i>Arizona v. Hicks</i> , 480 U.S. 321 (1987)	26
<i>Berger v. New York</i> , 388 U.S. 41 (1967)	6
<i>Birchfield v. North Dakota</i> , 136 S. Ct. 2160 (2016).....	9
<i>Blau v. United States</i> , 340 U.S. 332 (1951)	11
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018).....	1, 8, 11, 25
<i>Commonwealth v. Alexander</i> , 243 A.3d 177 (Pa. 2020).....	15
<i>Commonwealth v. Edmunds</i> , 586 A.2d 887 (Pa. 1991).....	8
<i>Commonwealth v. Fulton</i> , 179 A.3d 475 (Pa. 2018).....	3, 9, 10
<i>Commonwealth v. Gary</i> , 91 A.3d 102 (Pa. 2014).....	15
<i>Commonwealth v. Green</i> , 204 A.3d 469 (Pa. Super. Ct. 2019)	5
<i>Commonwealth v. Grossman</i> , 555 A.2d 896 (Pa. 1989).....	7
<i>Commonwealth v. Johnson</i> , 240 A.3d 575 (Pa. 2020).....	1, 3

<i>Commonwealth v. Morin</i> , 85 N.E.3d 949 (Mass. 2017)	16
<i>Commonwealth v. Orie</i> , 88 A.3d 983 (Pa. 2014)	22
<i>Ferguson v. City of Charleston</i> , 532 U.S. 67 (2001)	11
<i>Horton v. California</i> , 496 U.S. 128 (1990)	6
<i>In re Application for Search Warrant</i> , 71 A.3d 1158 (Vt. 2012)	17, 20, 21, 22
<i>Jaffee v. Redmond</i> , 518 U.S. 1 (1996)	11
<i>Marron v. United States</i> , 275 U.S. 192 (1927)	6
<i>Mink v. Knox</i> , 613 F.3d 995 (10th Cir. 2010)	15
<i>NAACP v. Alabama ex rel. Patterson</i> , 357 U.S. 449 (1958)	11
<i>People v. Hughes</i> , No. 158652, 2020 WL 8022850 (Mich. Dec. 28, 2020)	16
<i>Riley v. California</i> , 573 U.S. 373 (2014)	passim
<i>Scott v. United States</i> , 436 U.S. 128 (1978)	22
<i>State v. Bock</i> , No. A169480, 2021 WL 1208543 (Or. Ct. App. Mar. 31, 2021)	26
<i>State v. Castagnola</i> , 46 N.E.3d 638 (Ohio 2015)	16
<i>State v. Dean</i> , 388 P.3d 24 (Ariz. Ct. App. 2017)	17
<i>State v. Henderson</i> , 854 N.W.2d 616 (Neb. 2014)	16

<i>State v. Keodara</i> , 364 P.3d 777 (Wash. Ct. App. 2015)	17
<i>State v. Mansor</i> , 421 P.3d 323 (Or. 2018)	17, 23, 24, 26
<i>United States v. Bishop</i> , 338 F.3d 623 (6th Cir. 2003)	26
<i>United States v. Christie</i> , 717 F.3d 1156 (10th Cir. 2013)	14, 15, 23
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 621 F.3d 1162 (9th Cir. 2010)	passim
<i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013)	15
<i>United States v. Hill</i> , 459 F.3d 966 (9th Cir. 2006)	13, 18
<i>United States v. Jones</i> , 565 U.S. 400 (2012)	9
<i>United States v. Otero</i> , 563 F.3d 1127 (10th Cir. 2009)	12, 15
<i>United States v. Ramirez</i> , 523 U.S. 65 (1998)	23
<i>United States v. Shipp</i> , 392 F. Supp. 3d 300 (E.D.N.Y. 2019).....	13
<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010)	11
<i>United States v. Williams</i> , 592 F.3d 511 (4th Cir. 2010)	13
<i>Upjohn Co. v. United States</i> , 449 U.S. 383 (1981)	11
<i>Wheeler v. State</i> , 135 A.3d 282 (Del. 2015)	16
<i>Wilkes v. Wood</i> , Lofft 1, 98 Eng. Rep. 489 (C.P. 1763)	7

Other Authorities

Apple, <i>Compare iPhone Models</i>	10
Apple, <i>iCloud</i> (2021)	11
<i>How Many Pages in a Gigabyte</i> , LexisNexis (2007).....	11
iClick, <i>How Big is a Gig?</i> (2013)	10
Orin S. Kerr, <i>Executing Warrants for Digit. Evid.: The Case for Use Restrictions on Nonresponsive Data</i> , 48 Tex. Tech. L. Rev. 1 (2015).....	17, 24
Wayne LaFave, <i>Search and Seizure: A Treatise on the Fourth Amend.</i> , Vol. 2 § 4.10(d) (5th ed. 2018)	17
Paul Ohm, <i>Massive Hard Drives, General Warrants, and the Power of Magistrate Judges</i> , 97 Va. L. Rev. Brief 1 (2011)	17
Samsung, <i>Galaxy S10+ 1TB</i> (Unlocked).....	10

Constitutional Provisions

Pa. Const. art. I, § 8.....	passim
U.S. Const. amend. IV	passim

STATEMENT OF INTEREST OF AMICI CURIAE

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization dedicated to defending the principles embodied in the Federal Constitution and our nation’s civil rights laws. The **ACLU of Pennsylvania** is the state affiliate of the ACLU that has a long-standing interest in protecting Pennsylvanians’ rights to privacy. The ACLU and the ACLU of Pennsylvania have frequently appeared before the United States Supreme Court and other state and federal courts, including this Court, in numerous cases implicating Americans’ right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and as amicus in *Riley v. California*, 573 U.S. 373 (2014), and *Commonwealth v. Johnson*, 240 A.3d 575 (Pa. 2020).

The Defender Association of Philadelphia is a private, nonprofit corporation which represents a substantial percentage of the criminal defendants in Philadelphia County at trial, at probation and parole revocation proceedings, and on appeal. The Association is active in all of the Pennsylvania trial and appellate courts, as well as before the Pennsylvania Board of Probation and Parole. The Association attempts to ensure a high standard of representation and to prevent the abridgment of the constitutional and other legal rights of the citizens of Philadelphia and Pennsylvania.

The Pennsylvania Association of Criminal Defense Lawyers (“PACDL”)

is a professional association of attorneys admitted to practice in Pennsylvania who are actively engaged in providing criminal defense representation. As amicus curiae, PACDL presents the perspective of experienced criminal defense attorneys who seek to protect and ensure by rule of law those individual rights guaranteed in Pennsylvania, and who work to achieve justice and dignity for defendants. PACDL includes approximately 900 private criminal defense practitioners and public defenders throughout the Commonwealth.¹

¹ Amici certify, pursuant to Pa. R.A.P. 531(b)(2), that no person or entity, other than amici, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief, nor authored this brief in whole or in part.

SUMMARY OF ARGUMENT

This case presents a fundamental and highly consequential issue in Fourth Amendment and Article I, Section 8 jurisprudence on which this Court previously granted review, but ultimately did not decide, *see Commonwealth v. Johnson*, 240 A.3d 575 (Pa. 2020): What procedures are necessary to ensure that digital searches of the personal and private information in cell phones, computers, and other electronic devices adhere to constitutional protections against general and overbroad searches? This appeal presents the Court with the opportunity to establish the principles and standards for digital searches under the United States and Pennsylvania Constitutions.

New and increasingly sophisticated technology and means of communication in a digital world result in the accumulation and storage, in our electronic devices, of vast amounts of private information and documents. This Court and the United States Supreme Court have recognized the threats that governmental access to this information unregulated by the judiciary poses to personal privacy, and both courts have ruled that the Fourth Amendment and Article I, Section 8 of the Pennsylvania Constitution require probable cause and search warrants to search or seize this information. *See, e.g., Riley v. California*, 573 U.S. 373 (2014); *Commonwealth v. Fulton*, 179 A.3d 475 (Pa. 2018).

In the U.S. Supreme Court’s landmark decision in *Riley*, the Court issued a directive to police to “get a warrant” when seeking to search a cell phone seized incident to arrest. 573 U.S. at 403. But while *Riley* mandated *that* a warrant was required based on the privacy interests people have in their digital devices, it did not resolve *how* warrants would, in practice, do so. Even so, addressing the questions *Riley* left unanswered about the proper *execution* of warrants involves consideration of the same significant risks to privacy as those that prompted *Riley*’s specific mandate. There is a vast amount of stored information on these devices that is outside the scope of the warrant’s probable cause and particularity showings and is unrelated to the evidence properly sought by investigators. Fortunately, law enforcement has access to software programs that facilitate narrow, targeted searches of electronic devices. This brief explains the role of such technology in permitting legitimate searches while protecting against general warrants and overbroad searches consistent with the Fourth Amendment and Article I, Section 8.

In this case, in the course of investigating Mr. Green for possession of child pornography, police investigators secured a warrant for all of his electronic devices—not only computers, cell phones and other storage media, but also modems, monitors, and scanners, which do not store information. Having authorized the seizure of all imaginable equipment, the warrant also authorized a

search for “evidence relating to the possession and/or distribution of child pornography.” *Commonwealth v. Green*, 204 A.3d 469, 482 (Pa. Super. Ct. 2019). But the court placed no limits whatsoever on *how* that search could be conducted, either by reference to the nature of the information, type of file (for example, photographs), or time frame (for example, the date that investigators believed Green had downloaded the file), or by tethering the search to a specific criminal statute describing the conduct under investigation. Nor did the warrant contain any limits on the police’s use or retention of non-responsive personal information. Pursuant to the broad authority in the warrant, investigators seized Green’s cell phone, extracted all the information on it, *see* Trial Tr. 64, and “processed” or analyzed “whatever [was] on the phone,” *see* Trial Tr. 64. Images obtained from the cell phone were admitted at trial.² The lower courts approved the seizure of essentially all computer hardware in Green’s house and held that the warrant’s authorization to search the seized items for any and all information, limited only by the warrant’s reference to “possession and/or distribution of child pornography,” was sufficiently particular. *Green*, 204 A.3d at 482.

Such indiscriminate searches of cell phones and other electronic storage media are inconsistent with the fundamental protections of the Fourth Amendment

² The record does not establish how many other storage devices from Green’s house were seized and searched, nor what innocent information—either about Green or regarding the friends and family with whom he communicated—that police may have seen there.

and Article I, Section 8 of the Pennsylvania Constitution. Like all searches, searches of digital devices must be particularized—that is, limited to files and folders for which there is probable cause to search—to survive constitutional scrutiny.

ARGUMENT

I. Search Warrants Permitting Broad and Unlimited Digital Searches Violate the Particularity Requirement of the Fourth Amendment and Article I, Section 8 of the Pennsylvania Constitution.

The Fourth Amendment protects individuals from unreasonable government searches and seizures, including the infamous “general warrants” that gave English customs officers blanket authority to search private houses, papers, and effects. The United States Supreme Court has addressed the problem of general warrants through the Fourth Amendment’s “particularity” provision to ensure that “nothing is left to the discretion of the officer executing the warrant.” *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also Horton v. California*, 496 U.S. 128, 140 (1990) (“[s]crupulous adherence” to particularity requirement “limit[s] the area and duration of [] search”); *Berger v. New York*, 388 U.S. 41, 58–59 (1967) (observing that wiretaps that fail to “particularly describe” the “property” to be intercepted give law enforcement a “roving commission to ‘seize’ any and all conversations”).

The Supreme Court has also recognized that searches of papers and documents present even “grave[r] dangers inherent in executing a warrant” than

searches of “physical objects whose relevance is more easily ascertainable.”

Andressen v. Maryland, 427 U.S. 463, 482 n.11 (1976); *cf. Wilkes v. Wood*, Lofft

1, 4, 98 Eng. Rep. 489, 491 (C.P. 1763) (commenting that general warrants are akin to “fetch[ing] a sack, and fill[ing] it” with all of a person’s private papers).

That is because these kinds of searches present heightened risks that police executing search searches will make “unwarranted intrusions upon privacy.”

Andressen, 427 U.S. at 482 n.11.

Article I, Section 8 of the Pennsylvania Constitution provides even greater privacy protections against general warrants. In *Commonwealth v. Grossman*, 555 A.2d 896 (Pa. 1989), this Court explained that article I, section 8 was “more rigorous” with respect to the particularity requirement, stating:

Although some courts have treated overbreadth and ambiguity as distinct defects in warrants, 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. Consequently, any assessment of the validity of the description contained in a warrant, a court must initially determine for what items probable cause existed. The sufficiency of the description must then be measured against those items for which there was probable cause. Any unreasonable discrepancy between the items for which there was probable cause and the description in the warrant requires suppression.

Id. at 899–900 (citation omitted). Applying this test, this Court ruled that, where an affidavit provided probable cause for only three files, a search warrant authorizing a search of over 2,000 files was unconstitutionally overbroad. *Id.* at 900.³

Decisions by the United States Supreme Court and this Court on digital searches of cell phones and other electronic devices explain such searches’ unique invasiveness, and underline the need for courts to limit the scope of these searches and seizures by adhering to the particularity requirement and ensuring that warranted searches are not overbroad.

In *Riley v. California*, 573 U.S. 373, the Court declined to extend the search-incident-to-arrest exception to the digital information contained on an arrestee’s cell phone, reasoning that the significant privacy interests implicated by searches of cell phones outweigh the governmental interests in officer safety and preservation of evidence that underlie the exception. *Id.* at 386. The Court understood that the highly invasive search of an electronic device implicates privacy interests far beyond traditional searches of physical objects, and that equating the two “is like saying that a ride on horseback is materially indistinguishable from a flight to the moon.” *Id.* at 393. Rejecting wooden

³ Given this Court’s more protective application of article I, section 8’s particularity requirement in cases presenting the issue of overbroad searches, and its prior examination in those cases of factors under *Commonwealth v. Edmunds*, 586 A.2d 887 (Pa. 1991), a full *Edmunds* analysis is not essential.

application of older Fourth Amendment doctrines, the Court explained that “any extension of th[e] reasoning” from cases involving physical objects “to digital data has to rest on its own bottom.” *Id.*; *see also Carpenter v. United States*, 138 S. Ct. 2206 (2018) (rejecting argument that the “third party doctrine” vitiates any privacy claim regarding seizures of historic cell site information); *Birchfield v. North Dakota*, 136 S. Ct. 2160, 2176 (2016) (determining whether the search-incident-to-arrest exception should apply to unwarranted blood tests “by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy, and on the other, the degree to which it is needed for the promotion of legitimate governmental interests”); *United States v. Jones*, 565 U.S. 400 (2012) (finding reasonable expectation of privacy against government installation and monitoring of GPS device to track suspect’s movements on public streets, long considered areas in which one had no expectation of privacy).

And in *Commonwealth v. Fulton*, 179 A.3d 475 (Pa. 2018), this Court extended *Riley*, finding that the simple act of powering on a cell phone was a search governed by the warrant requirements of the Fourth Amendment and Article I, Section 8. The Court reasoned that monitoring of calls and texts reveals a vast amount of private information:

Contrary to the finding of the trial court and the argument advanced by the Commonwealth before this Court, there is little difference between monitoring the internal and external viewing screens on a cell phone and searching the phone’s call logs. Both result in accessing “more than

just phone numbers,” but also “any identifying information that an individual might add” to his or her contacts, including the caller’s photograph, the name assigned to the caller or sender of the text message. *See Riley*[], [573 U.S. at 400]. Further, and unlike a call log, monitoring a phone’s incoming text messages allows the viewer to see the content of a text message, which indisputably constitutes private data.

Id. at 489.

With each passing year, the privacy interests at stake in searches of computer hard drives, laptops, smart phones, and other electronic storage medium become even stronger, far outstripping those implicated in physical-world searches. A decade ago, a typical commercially available eighty-gigabyte hard drive could carry data “roughly equivalent to forty million pages of text—about the amount of information contained in the books on one floor of a typical academic library.” *United States v. Comprehensive Drug Testing, Inc.* (“CDT”), 621 F.3d 1162, 1175 (9th Cir. 2010) (en banc) (“[E]ven inexpensive electronic storage media today can store the equivalent of millions of pages of information.”). In 2014, when the Supreme Court decided *Riley*, the top-selling smartphone could store sixteen gigabytes of data. *Riley*, 573 U.S. at 394.⁴ Today, the minimum storage on Apple’s current line of iPhones is sixty-four gigabytes.⁵ Some Android

⁴ Sixteen gigabytes of storage is the equivalent of about 3,680 songs, 8,672 digital copies of *War and Peace*, 9,520 digital photos, or eight feature-length movies. iClick, *How Big is a Gig?* (2013), https://www.iclick.com/pdf/02_howbigisagig_infographic.pdf.

⁵ Apple, *Compare iPhone Models*, <https://perma.cc/A7G9-AJQX> (last visited Apr. 6, 2021).

models offer one terabyte of storage, roughly sixty-four times more than a *Riley*-era phone.⁶ Laptops sold in 2019 can store up to four terabytes,⁷ the equivalent of more than 2.5 billion pages of text.⁸ The quantity of information accessible via a laptop or a smart phone increases exponentially with cloud-based storage.⁹ *CDT*, 621 F.3d at 1176 (explaining that the proliferation of digital networking “has made it possible to store information at remote third-party locations, where it is intermingled with that of other users”).

This massive amount of highly sensitive information includes Internet browsing history,¹⁰ medical records,¹¹ email,¹² privileged communications,¹³ and

⁶ Samsung, *Galaxy S10+ 1TB* (Unlocked), <https://perma.cc/8BJ4-EP9W> (last visited Apr. 6, 2021).

⁷ See *Compare Mac models*, Apple, <https://perma.cc/Y8J2-YYZL> (last visited Apr. 6, 2019).

⁸ See *How Many Pages in a Gigabyte*, LexisNexis (2007), <https://perma.cc/ZG8X-2EGW>.

⁹ Apple, *iCloud* (2021), <https://perma.cc/5UMQ-NV3K> (last visited Apr. 6, 2021) (providing up to 2TB of remote storage).

¹⁰ See *Riley*, 573 U.S. at 395–96 (“An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual’s private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.”).

¹¹ See *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (holding that one has an expectation of privacy in diagnostic test results).

¹² See *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (“[E]mail requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve.”).

¹³ See *Jaffee v. Redmond*, 518 U.S. 1, 15 (1996) (psychotherapist-patient privilege); *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981) (attorney-client privilege); *Blau v. United States*, 340 U.S. 332, 333 (1951) (marital communications privilege).

associational information.¹⁴ From this diverse array of information, an observer can piece together the arc of one's entire life, including the most intimate, closely held secrets.

Because the personal information contained in our electronic devices is both qualitatively and quantitatively more sensitive than the information in physical items, *Riley*, 573 U.S. at 393–97, privacy protections against government searches must be proportionally stronger. As relevant here, “[t]he 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.” *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009).

II. The Proper Application of the Particularity Requirement for the Scope of a Search Is Critical to Ensuring that Searches and Seizures Pursuant to a Warrant Are Reasonable.

Forensic analysis of electronic devices presents challenges to compliance with traditional Fourth Amendment doctrine. Given the amount of information these devices store, it is almost always the case that only a fraction of that

¹⁴ See *Carpenter*, 138 S. Ct. at 2217 (“As with GPS information, the time-stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations’.”); *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958) (“[C]ompelled disclosure of affiliation with groups engaged in advocacy may constitute . . . a restraint on freedom of association.”).

information is responsive to probable cause. *See, e.g., CDT*, 621 F.3d at 1168 (in the digital context, responsive information will almost always be intermingled with nonresponsive information). Nonetheless, courts routinely permit investigators to seize all relevant storage media (though not monitors and keyboards as was done here) on the grounds that searching stored information onsite is too time consuming and, without proper forensic tools and procedures, can interfere with the integrity of any evidence that investigators might find. *See, e.g., United States v. Hill*, 459 F.3d 966, 974–75 (9th Cir. 2006) (“[T]he process of searching the files at the scene can take a long time. . . . Police would have to be present on the suspect’s premises while the search was in progress.”).

This seizure of storage devices often results in gigabytes of private information being held by the government. It is all the more important, then, for courts to insist that investigators conduct narrow, refined, and logged searches of these devices. Moreover, there need to be limitations on how the government may use seized private information, particularly that for which there was no probable cause to seize. While some courts have permitted investigators to effectively review every file on the assumption that evidence can be intermingled with innocent files, *see e.g., United States v. Williams*, 592 F.3d 511 (4th Cir. 2010), others have properly imposed significant protections to ensure that searches of

digital information hew to the scope of a proper warrant while protecting the gigabytes of irrelevant—but highly sensitive—personal information.¹⁵

For example, in *CDT*, the en banc Ninth Circuit recognized that the “pressing need of law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.” 621 F.3d at 1176; *see also id.* at 1167–69. Law enforcement officers had obtained a warrant to search the electronically stored drug-testing records of ten Major League Baseball players. In executing the warrant, officials examined the drug-testing records of hundreds of other players who were not subject to the warrant, but whose files were intermingled with those of the ten suspected players. Expressing deep concern with the scope of the search, the court set forth search protocols that could be considered on a case-by-case basis for limiting overbroad searches. Five judges would have gone further: when seeking a warrant to search a computer hard drive or electronic storage medium, those judges would, among other things, require the government to either forswear reliance upon the plain-view doctrine, or consent to rigid *ex ante* search protocols “designed to uncover

¹⁵ Online service providers often have tools to limit initial over-seizures of data demanded from user accounts. Courts have suggested that the practical concerns that may justify over-seizure of data stored on personal devices may not hold true for data stored in social media accounts. *See United States v. Shipp*, 392 F. Supp. 3d 300, 309 (E.D.N.Y. 2019) (“[T]he information associated with [social media accounts] is categorized and sorted by the company—not the user.”).

only the information for which it has probable cause.” *Id.* at 1178–80 (Kozinski, C.J., concurring).

Similarly, in *United States v. Christie*, 717 F.3d 1156 (10th Cir. 2013), then-Judge Gorsuch recognized the need for limits on digital computer searches:

On the one hand, we have held invalid warrants purporting to authorize computer searches where we could discern no limiting principle: where, for example, the warrant permitted a search of “‘any and all’ information, data, devices, programs, and other materials,” *United States v. Otero*, 563 F.3d 1127, 1132–33 (10th Cir. 2009) (alteration omitted), or “all computer and non-computer equipment and written materials in [a defendant’s] house,” *Mink v. Knox*, 613 F.3d 995, 1011 (10th Cir. 2010). On the other hand, we have said warrants may pass the particularity test if they limit their scope either “to evidence of specific federal crimes or [to] specific types of material.”

Christie, 717 F.3d at 1164–65 (final citation omitted); *see also United States v. Galpin*, 720 F.3d 436, 446–47 (2d Cir. 2013) (recognizing that unlike the physical world, where tangible boundaries described in a warrant delimit an investigator’s discretion, cell phones and computer hard drives provide no such inherent boundaries to guide the investigator’s discretion).¹⁶

¹⁶ In *Commonwealth v. Gary*, 91 A.3d 102, 152–53 (Pa. 2014), Justice Todd authored a perceptive dissent recognizing how new technology changes privacy analysis:

[P]eople transport in their automobiles, and often store for periods of time in them, their laptops, smartphones and other digital devices, which contain a plethora of intimate and elaborate details about their daily lives, their personal financial records, their interactions with family and friends, and their innermost thoughts.

...

Additionally, the modern automobile itself is outfitted with a multiplicity of electronic devices, not in existence at the time of the *Carney* decision, which catalog, in minute detail, the personal information and life activities of the

State supreme courts have also required stringent adherence to the particularity requirement in warrants to search digital information under both the Fourth Amendment and state constitutional law. *See, e.g., People v. Hughes*, No. 158652, 2020 WL 8022850 (Mich. Dec. 28, 2020) (any deviation from particularity requirement is a warrantless search); *Wheeler v. State*, 135 A.3d 282 (Del. 2015) (requiring precise designations of materials and information to be searched and suppressing evidence that was outside the time frame of the alleged crimes and that was on DVDs or photographs not connected to the criminal conduct under investigation); *Commonwealth v. Morin*, 85 N.E.3d 949, 959–61 (Mass. 2017) (“[P]olice may not rely on the general ubiquitous presence of cellular telephones in daily life, or an inference that friends or associates most often communicate by cellular telephone, as a substitute for particularized information that a specific device contains evidence of a crime.”); *State v. Henderson*, 854 N.W.2d 616, 633 (Neb. 2014) (finding insufficiently particular a warrant authorizing search for “any and all information” on a cell phone and observing that

automobile’s user. . . . Further, today’s vehicles, using extant “Bluetooth” computer technology, can interface with an occupant’s electronic data storage device such as a mobile phone or laptop so that the car collects and stores therein the user’s telephone contact lists, song collections, video and audio recordings and a growing number of other personal electronic files.

This Court overruled *Gary* in *Commonwealth v. Alexander*, 243 A.3d 177 (Pa. 2020), based in part on the reasoning of the *Gary* dissent.

“warrant for the search of the contents of a cell phone must be sufficiently limited in scope to allow a search of only that content that is related to the probable cause that justifies the search”); *State v. Castagnola*, 46 N.E.3d 638, 659 (Ohio 2015) (requiring strict adherence to the particularity requirement sufficient to guide and limit the search process and prohibiting warrants that permit a “sweeping comprehensive search of a computer’s hard drive”); *State v. Mansor*, 421 P.3d 323, 344 (Or. 2018) (requiring significant particularity with respect to a computer search and excluding evidence from the search that exceeded the scope of the warrant); *In re Application for Search Warrant*, 71 A.3d 1158 (Vt. 2012) (approving a number of ex ante limitations on the search of computers imposed by the issuing authority); *see also State v. Dean*, 388 P.3d 24, 28 (Ariz. Ct. App. 2017) (holding that a warrant to search a computer “without any limitations on what files could be seized or how those files ‘related to specific criminal activity’” was impermissibly broad); *State v. Keodara*, 364 P.3d 777, 781 (Wash. Ct. App. 2015) (“In general, Washington courts have recognized the search of computers or other electronic storage devices gives rise to heightened particularity concerns.”).¹⁷

¹⁷ Commentators have also recognized the enormous risks to privacy in comprehensive digital searches. *See* Wayne LaFave, *Search and Seizure: A Treatise on the Fourth Amend.*, Vol. 2 § 4.10(d) (5th ed. 2018); Orin S. Kerr, *Executing Warrants for Digit. Evid.: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech. L. Rev. 1, 6 (2015); Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L. Rev. Brief 1 (2011).

III. As This Case Shows, Courts Have a Number of Options in Preventing Overbroad Searches.

To ensure that searches of electronic devices comply with the Fourth Amendment, courts should impose limitations beginning at the point of seizure. While, in some cases, over-seizure of digital information may be necessary when investigators cannot meaningfully segregate responsive from non-responsive information on-site, that was not the case here. In particular, the officers did not need to seize computers that did not have uTorrent installed—and, in fact, they were able to use Cellebrite, a mobile device forensic tool (“MDFT”), to determine that Green’s cell phone did have uTorrent installed.

Investigators seeking a warrant to seize all cell phones and hard drives should be required to provide a plan for segregating information at the point of the seizure, where possible. *See Hill*, 459 F.3d at 978 (favoring search protocols in requests for warrants). That was not done in this case—indeed, police took a “seize everything” approach that went beyond their justification to invade Green’s privacy.

When certain electronic searches require taking devices off-site to make a complete electronic copy for forensic analysis, there must be effective limitations on the search process to ensure that police do not engage in boundless, general searches. This can be achieved with appropriate search protocols set forth in the

warrant, post-search review standards, and/or suppression remedies. Amici urge this Court to adopt a blend of both *ex ante* and post-search rules to ensure compliance with the Fourth Amendment and avoid unnecessary—and indeed, constitutionally impermissible—government rummaging through the private information of computer and cell phone owners, and the people with whom they communicate.

1. Search Protocols Imposed by the Issuing Authority

Searches should be limited by the issuing magistrate’s probable cause determination. For example, if the magistrate finds probable cause to seize an identifiable document, files created on a certain date, or other specific information, both the warrant itself and subsequent forensic search should reflect this limitation. Once that file is identified, that should end the search process.

However, where a magistrate finds probable cause to include many items not known by file name, designation, or date of creation, the magistrate should address the significant risk of broad and unregulated rummaging through non-responsive files. This risk is exacerbated by law enforcement use of powerful data extraction and analysis tools. As amicus Upturn explains, a search using an MDFT, such as the Cellebrite tool used in this case, is more invasive than a manual search because it extracts substantially more data. *See Br. Amicus Curiae of Upturn, Inc. in Supp.*

of Appellant (“Upturn Br.”) at 8–9.¹⁸ Moreover, MDFTs aggregate every file found on the device, enabling powerful data analysis that risks exposing even more personal information to the eyes of the police. *See* Upturn Br. at 9–10. The proliferation of these tools represents a dangerous expansion in law enforcement’s investigatory powers—a search far more invasive than scrolling through all text messages or emails.

To ameliorate this risk, courts should impose search protocols that limit the scope of the search by technical means, by ordering that search teams segregate responsive from non-responsive files before the information is passed to case agents, and by imposing use restrictions on evidence there was no probable cause to seize. Courts should also order that investigators log their queries to facilitate judicial oversight of digital searches. These methods would reduce the risk of law enforcement stumbling across non-responsive material whose perusal and potential retention is not justified by probable cause.

For example, in *In re Application for Search Warrant*, 71 A.3d 1158, the Vermont Supreme Court approved search protocols imposed as part of the warrant by the issuing authority, including (1) the requirement that the search be conducted by trained computer personnel separate from the case investigators, operating

¹⁸ Upturn’s insights about MDFTs, *see* Upturn Br. at 10–17, hold equally true for hard drive forensic tools, which have substantially the same functionality and capabilities.

behind a firewall and providing to the case investigators only the digital evidence related to the underlying criminal offense, *id.* at 1174, (2) specifying and limiting what search software could be used, with appropriate limits defined by relevant time periods, key words, and specific file types, *id.* at 1184, and (3) limiting copying to responsive material and requiring timely return of non-responsive files, *id.* at 1185. The court declined to eliminate the “plain-view exception” for files observed with criminal content unrelated to the search warrant, but as the majority acknowledged, *id.* at 1176–77, the prohibition on providing any of those files to the case investigator achieved a similar result.¹⁹

Search protocols could also designate independent third-party screener teams that sort, segregate, decode, and otherwise isolate seizable information (as defined by the warrant) from the troves of non-responsive personal data stored on modern devices. Such limitations would shield investigators from exposure to information beyond the scope of the warrant.

In addition, protocols could mandate that investigators run targeted searches for the files and folders contemplated by the warrant, and not rummage through data or open files at random. Investigators should be strictly prohibited from opening files with no obvious connection to the permissible seizure of evidence

¹⁹ Amici address the plain view issue below. *See infra* Section III.4.

under the warrant, lest electronic searches serve a prurient, rather than public safety, interest. As amicus Upturn explains, MDFTs and other forensic tools give unlimited access to all of the private information on electronic storage devices. Upturn Br. at 9–10. Courts can address this threat to constitutionally protected privacy by taking advantage of the features of MDFTs and other forensic tools that can narrow the search of electronically-stored data. *See* Upturn Br. at 10–17.

Amici recognize that judicial officers who issue warrants may not be trained on or knowledgeable about the mechanics and science of electronic searches. But a technical understanding of how forensic software operates is not necessary to impose reasonable search protocols. Judges are well acquainted with setting *ex ante* rules for how searches are conducted, such as when they order minimization of over-hearings by electronic surveillance. *See Scott v. United States*, 436 U.S. 128 (1978); *In re Application for Search Warrant*, 71 A.3d at 1170–72. In cases involving claims of privilege, judges also routinely consider limitations such as separate search teams and non-disclosure of non-responsive materials to case investigators. *See, e.g., Commonwealth v. Orie*, 88 A.3d 983, 1010 n.46 (Pa. 2014) (ordering prosecutorial “taint team” to segregate privileged information comingled within computer hard drives).

2. Post-Search Court Review

If specific protocols or other ex ante limitations on the search process are not put in place by the issuing authority, the warrant should require the investigators to craft search mechanics, using MDFTs or other forensic tools, reasonably targeted to the files and folders contemplated in the warrant. The scope of the forensic search—in terms of the reasonableness of these search mechanics and the operation of the search in practice—would then be subject to ex-post reasonableness review, in which the court would determine whether the analyst’s search technique was sufficiently tailored to finding warrant-responsive material.

As the Tenth Circuit stated in *United States v. Christie*,

[e]ven putting aside for the moment the question what limitations the Fourth Amendment’s particularly requirement should or should not impose on the government ex ante, the Amendment’s protection against “unreasonable” searches surely allows courts to assess the propriety of the government’s search methods (the how) ex post in light of the specific circumstances of each case. *See, e.g., United States v. Ramirez*, 523 U.S. 65, 71 (1998). . . . Unlike an ex ante warrant application process in which the government usually appears alone before generalist judges who are not steeped in the art of computer forensics, this ex post review comes with the benefit, too, of the adversarial process where evidence and experts from both sides can be entertained and examined.

Christie, 717 F.3d at 1166–67. The post-search review in the context of a suppression hearing must be robust, with ample opportunity for the parties to present testimony regarding the scope of the search, what steps were taken to

minimize searches and seizures of non-responsive private information and other materials, and the presentation of expert testimony.

3. Use Restrictions

In the alternative, this Court should follow the Oregon Supreme Court in imposing a restriction on law enforcement's ability to use any evidence that exceeds its authorization to search. *Mansor*, 421 P.3d at 343. As that court, under its state analogue to the Fourth Amendment, explained:

We acknowledge that, for practical reasons, searches of computers are often comprehensive and therefore are likely to uncover information that goes beyond the probable cause basis for the warrant. In light of that fact, to protect the right to privacy and to avoid permitting the digital equivalent of general warrants, we also hold that Article I, section 9 [the relevant Oregon state constitutional provision], prevents the state from using evidence found in a computer search unless a valid warrant authorized the search for that particular evidence, or it is admissible under an exception to the warrant requirement.

Id. at 326. A use restriction would limit the government, except in exigent circumstances and other narrow exceptions, to using only information that is actually responsive to—that is, particularly described by—the warrant. As one influential commentator has explained, “[t]his approach best reconciles the government’s compelling need to obtain the evidence sought in the warrant with the Fourth Amendment’s prohibition on general warrants.” Orin S. Kerr, *Executing Warrants for Digit. Evid.*, 48 Tex. Tech. L. Rev. at 11.

4. The Plain View Exception

Where the issuing authority has not properly limited the scope of the search—or where the forensic search process does not include effective protections against open-ended, overbroad searches—there should be a prohibition on the use of evidence under the plain view exception to the Fourth Amendment’s warrant requirement. Just as *Riley* rejected search incident to arrest as a basis for warrantless searches of cell phones, courts should reject application of the plain view exception to searches of electronic devices because it defeats privacy interests and incentivizes law enforcement to engage in overbroad searches. *See CDT*, 621 F.3d at 1178–1180 (Kozinski, C.J., concurring).

Exceptions to the warrant requirement must remain “[tether[ed]]” to “the justifications underlying the . . . exception.” *Arizona v. Gant*, 556 U.S. 332, 343 (2009). In *Carpenter*, the Court rejected the government’s invocation of the “third-party doctrine”—an exception to normal Fourth Amendment protections based on individuals’ supposedly reduced expectation of privacy in information shared with others—to justify warrantless collection of digital location information held by phone companies. 138 S. Ct. at 2219–22. The Court explained that the “Government’s position fails to contend with the seismic shifts in digital technology” that untethered the traditional rationale for the third-party doctrine

from its application to an “exhaustive chronicle of location information casually collected by wireless carriers.” *Id.* at 2219.

Courts considering whether to “exempt a given type of search from the warrant requirement” must balance “the degree to which [the search] intrudes upon an individual’s privacy” against “the degree to which it is needed for the promotion of legitimate governmental interests.” *Riley*, 573 U.S. at 385. The broad and ever-increasing privacy interest in electronic devices overrides the government interest justifying the plain-view exception: “sparing police . . . the inconvenience and the risk—to themselves or to preservation of the evidence—of going to obtain a warrant.” *Arizona v. Hicks*, 480 U.S. 321, 327 (1987).

The plain-view doctrine developed in cases involving physical-world searches, where evidence is tangible and discrete, but highly invasive searches for digital information are a poor fit for the plain-view exception because the justifications underlying the exception are largely absent in this context. *See State v. Bock*, No. A169480, 2021 WL 1208543, at *6 (Or. Ct. App. Mar. 31, 2021) (explaining that the “breadth” of a digital search “is what renders the plain view doctrine inapplicable” to such searches and that “the alternative would sanction the sort of general warrant that the plain view doctrine was never meant to authorize” (citing *Mansor*, 421 P.3d at 343)). Officer safety is not implicated in a forensics laboratory. Unlike a physical object, such as a knife or gun, *see, e.g., United States*

v. Bishop, 338 F.3d 623, 628–29 (6th Cir. 2003), the digital information stored on a computer hard drive can physically endanger no one. *See also Riley*, 573 U.S. at 386–87. Moreover, evidence preservation is not at stake in a typical computer search, where police possess a copy of the hard drive. Accordingly, only where the searching agent has adhered to the constitutional limitations throughout the search process should the plain-view doctrine apply, and then only upon the issuance of an additional warrant.

CONCLUSION

The landmark rulings in *Riley* and *Fulton* make clear the dangers that new technology poses to privacy interests. These cases require rules and standards for the digital search process that will ensure that warrants do not serve as prohibited general warrants. This Court should mandate these procedures to bring current search practices into conformity with the long-standing constitutional protections against overbroad and general searches.

April 7, 2021

Respectfully submitted,

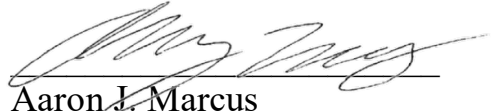


David Rudovsky
Pa. I.D. No. 15168
Kairys, Rudovsky, Messing,
Feinberg & Lin LLP
718 Arch Street



Andrew Christy
Pa. I.D. No. 322053
American Civil Liberties Union
of Pennsylvania
P.O. Box 60713

Philadelphia, PA 19106
(215) 925-2298



Aaron J. Marcus
Pa. I.D. No. 93929
Leonard Sosnov
Pa. I.D. No. 21090
Defender Association of Philadelphia
1441 Sansom Street
Philadelphia, PA 19001
(215) 568-3190

Philadelphia, PA 19102
(215) 592-1513 x138



Peter E. Krasta
Pa. I.D. No. 71009
President, Pennsylvania Association
of Criminal Defense Lawyers
Macelree Harvey, Ltd.
17 West Miner Street
West Chester, PA 19382

CERTIFICATE OF COMPLIANCE WITH WORD LIMIT

I certify pursuant to Pa.R.A.P. 531 that this brief does not exceed 7,000 words.

CERTIFICATE OF COMPLIANCE

I certify that this filing complies with the provisions of the Public Access Policy of the Unified Judicial System of Pennsylvania: Case Records of the Appellate and Trial Courts that require filing confidential information and documents differently than non-confidential information and documents.

CERTIFICATE OF SERVICE

I hereby certify that the foregoing document was served upon the parties via PACFile.

Dated: April 7, 2021

/s/ Andrew Christy
Andrew Christy