Received 7/25/2019 1:24:02 PM Supreme Court Western District

Filed 7/25/2019 1:24:00 PM Supreme Court Western District
25 WAP 2019

IN THE SUPREME COURT OF PENNSYLVANIA

No. 25 WAP 2019

COMMONWEALTH OF PENNSYLVANIA,

Appellee,

v.

LAVELLE JOHNSON,

Appellant.

Brief of Amici Curiae the American Civil Liberties Union of Pennsylvania and the Pennsylvania Association of Criminal Defense Lawyers in Support of Appellant Lavelle Johnson

---

Appeal from the order of the Superior Court of Pennsylvania entered October 18, 2018 at No. 1082 WDA 2017

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

Andrew Christy
Pa. I.D. No. 322053
American Civil Liberties Union of Pennsylvania
P.O. Box 60173
Philadelphia, PA 19102
(215) 592-1513 x138

Michael Witsch
Pa. I.D. No. 313884
Armstrong Teasdale LLP
2005 Market Street, 29th Floor
Philadelphia, PA 19103
(267) 780-2000

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

Counsel continued on next page

Bradley Winnick
Pa. I.D. No. 78413
President, Pennsylvania Association of
Criminal Defense Lawyers
Of counsel
Chief Public Defender
Dauphin County Public Defender's
Office
2 South Second Street, 2nd Floor
Harrisburg, PA 17101
(717) 780-6393

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Other Authorities

STATEMENT OF INTEREST OF AMICUS CURIAE

The American Civil Liberties Union of Pennsylvania ("ACLU") is an affiliate of the American Civil Liberties Union, a nationwide, nonprofit, nonpartisan organization of over 1.5 million members. Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other federal courts 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). The ACLU of Pennsylvania is an affiliate of the ACLU that has a long-standing interest in protecting Pennsylvanians' rights to privacy. This case raises fundamental questions about the scope of Article I, Section 8 of the Pennsylvania Constitution and the safeguards it provides in the face of new technologies used by every Pennsylvanian. We submit this Brief to aid the Court in applying this provision in the modern era.

The Pennsylvania Association of Criminal Defense Lawyers ("PACDL") is a professional association of attorneys admitted to practice before the Supreme Court of Pennsylvania and 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]

ARGUMENT

A. Introduction

This case presents a fundamental and highly consequential issue in Fourth Amendment and Article I, Section 8 jurisprudence: what limitations are necessary to ensure that the increasingly vast law enforcement enterprise of 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 in light of its historical recognition of the privacy interests inherent in our Constitutional framework. *See generally* Seth F. Kreimer, *Still Living After Fifty Years: A Census of Judicial Review Under the Pennsylvania Constitution of 1968*, 71 Rutgers L. Rev. 287, 291 (2019).

Fortunately, new technology not only provides the ability to store vast amounts of private information and documents, but also software and programs that facilitate narrow, targeted searches of these devices where courts have determined that there is probable cause for criminal searches. This amicus brief

[1] No other entity authored or paid for this brief.

sets forth an approach that permits legitimate searches, and which, at the same time, protects against general warrants and overbroad searches consistent with Fourth Amendment and Article I, Section 8 principles.

This case is paradigmatic of the new world of search and seizure practices. Mr. Johnson was present in an apartment (along with several others) at the time of a warrantless entry. He was not a resident of the apartment and while the initial search conducted by the police disclosed drugs and weapons in the residence, there were none in his immediate possession. Incident to his arrest on these garden-variety drug and weapon charges, police seized Mr. Johnson's cell phones and, four months later, secured a search warrant that authorized as full a search of these devices as was technologically feasible. The overly broad search warrant application sought:

> All information stored in the body of these cellular phones . . . but not limited to the cell phone number that is connected to these cell phones and the security numbers used to secure the phones, direct connect numbers, carrier IP number, voice mail, text messages (SMS) and the phone numbers associated with these cell phone numbers, picture(s) messages (MMS) and the phone numbers associated with those pictures, any and all internet history and IP addresses, and phone book and/or contact list and all listed incoming and all missed calls, i.e. history in this cell phone.

Even more, the officers also requested permission to search for and seize:

> [A]ny and all electronic and/or digital data contained within the cellular telephone or its storage medias/memory cards, such as incoming/outgoing calls, call logs, emails, personal calendars,

> cellular internet usage, wireless internet usage, GPS data, contact information, text messages, voice mails, notes, photographic images, IP addresses, contact information, and voice recordings whether or not the electronic and/or digital data has been erased, hidden password protected or encrypted.

A judicial officer authorized this search to determine whether there was evidence of "possession of illegal firearms and distribution and possession of heroin." There was no limitation as to the date or time frame of the evidence sought, limitation as to the scope of the digital data that could be searched, and no restrictions on the use of non-responsive data. Both the trial court and the Superior Court approved this wide-ranging and unregulated search:

> Unlike in [*Commonwealth v. Orie*, 88 A.3d 983 (Pa. Super. 2014)], evidence of a narcotics distribution enterprise would not be limited to a distinct period of time, a limited number of people, or a particular form of digital file. Therefore, the breadth of the search warrant was necessary and reasonable due to the digital storage capacity of the electronic device to be searched at the time.

Superior Court Opinion, at 26.

There is no reason to doubt that the search process used here is not representative of current search practices of phones and computers throughout the Commonwealth. Amici maintain that indiscriminate searches of cell phones and other electronic storage media conducted pursuant to a warrant are inconsistent with the fundamental protections of the Fourth Amendment and Article I, Section 8 of the Pennsylvania Constitution. Searches of digital devices, like all searches,

must be particularized—that is, limited to files and folders for which there is probable cause to search. But most important, to ensure that the particularity requirements are respected and implemented by law enforcement, this Court should mandate appropriate safeguards in the warrant approval process and in the post-search review by the courts.

B. Broad and Unlimited Digital Searches of Electronic Devices Violate 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 Supreme Court has addressed the problem of general warrants through the "particularity" provision of the Fourth Amendment. *See Marron v. United States*, 275 U.S. 192, 195–96 (1927) ("[N]othing is left to the discretion of the officer executing the warrant."); *see also Horton v. California*, 496 U.S. 128, 140 (1990) ("[s]crupulous adherence" to particularity requirement limits the area and duration of search); *Lo-Ji Sales v. New York*, 442 U.S 319, 325 (1979) (Fourth Amendment's particularity requirement did not permit a warrant which "left it entirely to the discretion of the officials conducting the search to decide what items were likely obscene and to accomplish their seizure"); *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"); *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). The Supreme Court has also recognized that searches of papers and documents present even "grave[r] dangers inherent in executing a warrant." *Andressen v. Maryland*, 427 U.S. 463, 482, n.11 (1976).

Article I, Section 8 of the Pennsylvania Constitution provides even greater privacy protections against general warrants. For example, where a search warrant states probable cause on one ground, it cannot then support a broader search. *Commonwealth v. Grossman*, 555 A.2d 896 (Pa. 1989). In *Grossman*, this Court ruled 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.

Applying this test, the Court ruled that a search warrant that stated probable cause for three files, could not support a search of over 2000 files. *Id.* at 900.[2]

Likewise, in determining the proper scope of digital searches, recent decisions by the United States Supreme Court and this Court ruling that digital searches of cell phones and other electronic devices must be conducted pursuant to a search warrant provide a compelling rationale for limiting the scope of these searches. *See, e.g.*, *Riley v. California*, 573 U.S. 373 (2014). In *Riley*, the Court explained why the well-established warrant exception of search-incident-to-arrest should not be applied with respect to digital searches. *Id.* "Absent more precise guidance from the founding era," the Court stated, "we generally determine whether to exempt a given type of search from the warrant requirement 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 is needed for the promotion of legitimate governmental interests." *Id.* at 385. 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

[2] Given this Court's prior rulings applying Article I, Section 8 in cases presenting the issue of overbroad searches, an extended *Edmunds* analysis is not essential. However, since this case presents that issue in the context of digital searches, we discuss court rulings from other state supreme courts. *Infra* at 12.

searches of cell phones outweigh the governmental interests in officer safety and preservation of evidence that underlie the exception.

The *Riley* Court understood that the highly invasive search of laptops, hard drives, and other electronically stored information implicates privacy interests far beyond traditional searches and that comparing the two "is like saying that a ride on horseback is materially indistinguishable from a flight to the moon [as] both are ways of getting from point A to point B." *Riley*, 573 U.S. at 393. In other words, wooden application of doctrine that covers traditional searches has been rejected, and "any extension of that reasoning to digital data has to rest on its own bottom." *Id.*; *see also Birchfield v. North Dakota*, 136 S. Ct. 2160 (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").

Riley is one of several cases involving new technology in which the broad scope of the searches caused the U.S. Supreme Court to adjust long-standing precedent to increase privacy protections. *See, e.g.*, *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); *United States v. Jones*, 132 S. Ct. 945 (2012) (finding reasonable expectation of privacy in

transportation patterns surveilled by a GPS device on public streets which had long been considered areas in which one's movements had no expectation of privacy); *Kyllo v. United States*, 533 U.S. 27 (2001) (holding use of thermal imaging device violated expectation of privacy even though it detected only heat waves emanating from roof of house).

In *Commonwealth v. Fulton*, 179 A.3d 475 (Pa. 2018), this Court embraced and extended the *Riley* ruling, 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. Again, the vast amount of private and personal information on the device was a critical factor. 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*/*Wurie*, 134 S. Ct. at 2492–93. 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.

Indeed, there is a growing consensus that the storage capacity and fast data-transfer capabilities of modern digital devices present serious privacy concerns and heighten the need for protections against overbroad searches. For example, in

United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1168–69, 1176 (9th Cir. 2010) (en banc) ("*CDT*"), the court 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." In *CDT*, law enforcement officers 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 players named in the warrant. The Court set forth possible search protocols that should be considered on a case-by-case basis for limiting overbroad searches. Chief Judge Kozinski, joined by four other judges, would have gone further: when seeking a warrant to search a computer hard drive or electronic storage medium, the government must either forswear reliance upon the plain view doctrine or consent to rigid ex ante search protocols "designed to uncover only the information for which it has probable cause." *Id.* at 1178–80 (Kozinski, C.J., concurring).

In *United States v. Christie*, 717 F.3d 1156 (10th Cir. 2013), then-Judge Gorsuch likewise 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."

Id. at 1164–65; *see also United States v. Payton*, 573 F.3d 859, 862 (9th Cir. 2009) ("Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers. Such considerations commonly support the need specifically to authorize the search of computers in a search warrant . . . ."); *see also United States v. Galpin*, 720 F.3d 436, 447 (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).[3]

[3] In *Commonwealth v. Gary*, 91 A.3d 102, 152–53 (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 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

State supreme courts have also addressed the particularity and general warrant issues under both the Fourth Amendment and state constitutional law principles. *See, e.g.*, *Wheeler v. State*, 135 A.3d 282 (Del. 2015) (requiring precise designations of materials and data 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. 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 "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. Reid*, 945 A.2d 26 (N.J. 2008) (noting New Jersey Constitution affords greater protection against unreasonable searches and seizures than the Fourth

---

> 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.

Amendment, and finding a reasonable expectation of privacy in the subscriber information provided to internet service providers); *State v. Castagnola*, 46 N.E.3d 638 (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 (Or. 2018) (requiring significant particularity with respect to a computer search and excluding evidence from the search that went beyond the search authorized by the issuing authority); *In re Application for Search Warrant*, 71 A.3d 1158 (Vt. 2012) (approving a number of limitations on the search process of computers ex ante imposed by the issuing authority); *State v. Hinton*, 319 P.3d 9 (Wash. 2019) (en banc) ("Text messages can encompass the same intimate subjects as phone calls, sealed letters, and other traditional forms of communication that have historically been strongly protected under Washington law."); *see also State v. Dean*, 388 P.3d 24, 28 (Ariz. 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); *People v. Appelton*, 199 Cal. Rptr. 3d 637, 644 (Cal. App. 5th 2016) ("[A] search of defendant's mobile electronic devices could potentially expose a large volume of documents or data, much of which may have nothing to do with illegal activity. These could include, for example, medical records, financial records, personal

diaries, and intimate correspondence with family and friends."); *State v. Keodara*, 364 P.3d 777, 781 (Wash. App. 2015) ("In general, Washington courts have recognized the search of computers or other electronic storage devices gives rise to heightened particularity concerns").[4]

With each passing year, the privacy interests at stake in searches of computer hard drives, laptops, smart phones, or electronic storage medium become even stronger, far outstripping the privacy concerns implicated in physical-world searches. A decade ago, a typical commercially available 80-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." *See CDT*, 621 F.3d at 1175 ("[E]ven inexpensive electronic storage media today can store the equivalent of millions of pages of information."). Laptops sold in 2019 can store up to four terabytes,[5] the equivalent of more than 2.5 billion pages of text.[6] The quantity of information accessible via a laptop or a smart

---

[4] Commentators also recognize the enormous risks to privacy in open-ended and comprehensive digital searches. *See* WAYNE LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT, VOL. 2 § 4.10(d) (5th ed. 2018); Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech. L. Rev. 1, 6 (2015); P. Ohm, Response, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L. Rev. 1, In Brief (2011).

[5] *See Compare Mac models*, APPLE, https://www.apple.com/mac/compare/ (last visited Mar. 10, 2019).

[6] *See How Many Pages in a Gigabyte*, LEXISNEXIS, (2007), https://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf .

phone increases exponentially once one takes into account cloud-based storage. *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").

Not only do computers contain a great quantity of data, they also contain a diverse array of information—much of it exceedingly sensitive. Information deserving of stringent privacy protections are contained on electronic devices, including internet browsing history,[7] medical records,[8] email,[9] privileged communications,[10] and associational information.[11] 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. Thus, where this type of personal

---

[7] *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.").

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

[9] *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.").

[10] *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).

[11] *Riley*, 573 U.S. at 396 ("Mobile application software on a cell phone, or 'apps,' offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news . . . ."); *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 subject to a governmental search, privacy protections must be proportionally stronger.

C. Regulating the Search Process

The electronic search stage typically involves taking the devices off site, making an electronic copy (the "image" that replicates the original) and then searching the image for the evidence authorized by the warrant. Given the massive amount of information that may be stored on the devices, even if the warrant has particularized what may be seized, there must be effective limitations on the search process to ensure against prohibited general searches. This can be achieved with appropriate ex ante search protocols, post-search review standards, and suppression remedies. We discuss the options and urge this Court to adopt a blend of both ex ante and post-search rules.

1. Limits Imposed by the Issuing Authority

The probable cause determination itself should impose implicit limits on the search process. For example, if the warrant authorizes seizure of an identifiable document or other specific information, or of files created on a certain date, the forensic search should be so limited and once (and if) the file is identified that should end the search process. However, where probable cause may include many items, not known by file name or designation or date of creation, the issue becomes how broad and unregulated a forensic search may be employed.

Courts have approved search protocols that limit the scope of the search by technical means, by identity of the searching agents, and by use restrictions on evidence found that is outside of what was authorized. In *In re Application for Search Warrant*, 71 A.3d 1158, the Vermont Supreme Court upheld a number of limiting protocols imposed by the issuing authority. These included (1) the requirement that the search be conducted by trained computer personnel separate from the case investigators, operating behind a firewall, and permitting the searching agent to provide to the case investigator only the digital evidence relating to the underlying criminal offense, (2) specifying and limiting what search software could be used, with appropriate limits defined by relevant time periods, key words, and specific file types, and (3) limiting copying to responsive material and requiring timely return of non-responsive. The court refused to eliminate the "plain view" exception for files observed with criminal content unrelated to the search warrant, but as the majority acknowledged the prohibition on providing any of those files to the case investigator achieved a similar result.[12]

All of these pre-search limitations can enforce the particularity requirement. Search protocols that include independent third-party screener teams that sort, segregate, decode and otherwise separate seizable data (as defined by the warrant)

[12] We address the plain view issue, *infra* at 23.

shield investigators from exposure to information beyond the scope of the warrant. As Judge Kozinski stated in *CDT*: "Thus, if the government is allowed to seize information pertaining to ten names, the search protocol should be designed to discover data pertaining to those names only, not to others, and not those pertaining to other illegality." *CDT*, 621 F.3d at 1179 (Kozinski, C.J., concurring).

In addition, protocols may mandate use of modern forensic software that provides tools for running targeted searches for the files and folders contemplated by the warrant. For cell phones, these include programs such as EnCase Mobil Investigator. *See EnCase Mobile Investigator*, GUIDANCE SOFTWARE, https://www.guidancesoftware.com/docs/default-source /document-library/product-brief/encase-mobile-investigator-product-overview.pdf?sfvrsn=66f569a2_22. For computers, filters on EnCase Forensic ("EnCase"), can limit the search to specific files or types of data, such as emails, internet searches, photographs, documents, files over a specified size, files with a particular extension, files containing personal identifying information (such as email addresses and credit card, Social Security, and phone numbers), or files containing certain keywords.[13]

[13] Guidance Software, EnCase Forensic User Guide Version 8.07 62–65, 143, 246, 338 (2018), http://encase-docs.opentext.com/documentation/encase/forensic/8.07/Content/Resources/External%20Files/EnCase%20Forensic%20v8.07%20User%20Guide.pdf [hereinafter EnCase User Guide].

Metadata processing on EnCase can limit the search to files corresponding to a specified creation or modification date range. Date range filters allow analysts to hone in on files within temporal proximity of a relevant crime. Further, sophisticated hashing tools on EnCase allow the automatic identification of well-known illegal files (such as child pornography) without a human investigator needing to actually open the file.[14] These forensic tools can narrow the pool of digital content that an analyst must open manually, thereby reducing the risk of law enforcement stumbling across non-responsive material whose perusal and potential retention is not justified by probable cause.

Forensic software programs can also detect embedded file images, for example, photographs hidden inside of Microsoft Word documents and optical character recognition is a common forensic tool which automatically extracts text contained in graphic files, such as images or non-searchable PDFs.[15] Today, investigators are capable of determining whether digital file is warrant-responsive without manually opening that file.

In practical terms, programs like EnCase or Cellebrite Reader allow law enforcement to conduct narrow, targeted searches in the same way that one might

---

[14] *Id.* at 279, 292.

[15] *Forensic Toolkit User Guide*, ACCESSDATA 72 (Oct. 2, 2012), https://ad-pdf.s3.amazonaws.com/FTK4-1_UG.pdf. ("The Optical Character Recognition (OCR) process lets you extract text that is contained in graphics files. The text is then indexed so that it can be[] searched[] and bookmarked.").

search a private e-mail account: to find e-mails from John Smith, a user types identifying information such as name or e-mail address into the program that filters and displays only the relevant results.

EnCase and Cellebrite function in the same basic manner. Thus, if law enforcement obtains a warrant for a cell phone that has been seized in connection with a drug or firearm investigation, the investigators would start by using software to make a mirror "image" of the device, including deleted items and those in temporary device memory. Police would then search the device by using a variety of relevant keywords such as "heroin," "dope," "guns," or "gats," or for names of suspected co-conspirators.[16] This search looks through the entire device and could permissibly disclose text messages, Snapchats, e-mails, text documents, PDFs, call logs, and contacts.

The police would also be able to search the device based on temporal factors. For example, if the warrant referenced a seizure of drugs or at a specific time and place, the police would be able to search the phone's call log and messages for a reasonable period of time—such as that day, but limited to references of contemporaneous drug or gun transactions.

[16] Cellebrite offers a publicly-available walkthrough video that explains how to use its Cellebrite Reader software: https://www.cellebrite.com/en/blog/how-to-share-review-and-interpret-your-digital-evidence-discoveries-with-cellebrite-reader/. Please note that the video requires a free registration to view.

If these searches disclosed evidence related to drug dealing or illegal firearm transactions, for example, if text messages from or to John Smith referenced a recent drug transaction, the police would then be able to search the phone for data related to "John Smith." All of these searches would be tied to the probable cause stated in the search warrant.

As in physical world searches, this process does not necessarily mean that law enforcement will not come across material unrelated to the warrant, but use of EnCase or Cellebrite makes searching a digital device technologically feasible, while at the same time protecting against broad intrusions into highly personal matters such as health care and medications, religious beliefs and associations, political affiliations, or communications with family members, friends, or paramours.

We recognize that judicial officers who issue warrants are not trained or may not be knowledgeable with the mechanics and science of electronic searches. But that fact does not justify a blanket prohibition on protocols. Judges currently have the power to permit "no-knock" warrants based on exigent circumstances, *e.g.*, *United States v. Banks*, 540 U.S. 31 (2003), to order that the search be conducted within a specified time period, and to order minimization of over hearings by electronic surveillance, *see Scott v. United States*, 436 U.S. 128 (1978); *see generally In re Application for Search Warrant*, 71 A.3d at 1170–72. Judges

routinely consider these issues in issuing search warrants, and limitations such as separate search teams and non-disclosure of non-responsive materials to case investigations, are not dependent on technical expertise.

Moreover, if the government is to be granted the power to engage in digital searches, it must ensure over time that judges authorized to order these searches (and those who review the process post-search) understand the technology that now informs modern law enforcement. Protocols should be permissible depending on the nature of the search, and as they become more common judges who issue warrants will better understand the technological issues.[17]

2. Post-Search Court Review

Even if protocols or other ex ante limitations on the search process are not required by the issuing authority, the warrant should entrust forensic analysts to craft search mechanics, using EnCase or a similar software, reasonably targeted to the files and folders contemplated in the warrant. The scope of the forensic search 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 court stated in *United States v. Christie*, 717 F.3d at 1166–67:

[17] This Court could also request the Court's Criminal Procedure Rules Committee to undertake a study of this issue and to promulgate appropriate rules and standards.

> Even 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.

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 data and other materials, and the presentation of expert testimony. The government cannot have it both ways: no ex ante limitations on the ground that they may unduly restrict the scope of the search and limited or deferential review, post-seizure. The rationale of *Riley* and *Fulton* that departs from long-standing search incident to arrest doctrine for searches of cell phones requires, as well, a credible process for determining whether the particularity requirement has been fully honored.

3. The Plain View Exception

Where the issuing authority has not properly limited the scope of the search or 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 search warrant requirement. Just as *Riley* rejected search incident to arrest as a basis for warrantless searches of cell phones, the plain view exception can defeat privacy interests and incentivize law enforcement to engage in overbroad searches. *See CDT*, 621 F.3d at 1178–1180 (Kozinski, C.J., concurring).

Exceptions to the warrant requirement upon must remain "[]tether[ed]" to "the justifications underlying the . . . exception." *Arizona v. Gant*, 556 U.S. 332, 343 (2009). Thus, in *Carpenter v. United States*, 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.

In *Gant*, 556 U.S. at 346, the Court declined to extend the search-incident-to-arrest exception to the warrantless search of a passenger compartment in

defendant-arrestee's vehicle where "unnecessary to protect law enforcement safety and evidentiary interests." And in *Collins v. Virginia*, 138 S.Ct. at 1672–73, the Court ruled that the automobile exception does not allow an officer to enter a home or its curtilage without a warrant because, unlike vehicles, the curtilage of a home is not readily mobile.

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 enormous privacy interest in electronic devices like laptop computers and cell phones overrides the government interest justifying the plain-view exception of "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, 326–27 (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. Officer safety is not implicated in a controlled environment like an off-site 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 data stored on a computer hard drive can physically endanger no one. *See Riley*, 573 U.S. at 386–87. Moreover, evidence preservation is not at risk in a typical computer search, where police possess a copy of the hard drive.

Accordingly, since plain view conditions are not usually met in the context of searches for digital information, it should be the rare case, e.g., where the searching agent has adhered to strict limitations in the search process, that the plain view doctrine should be applicable, and then only upon the issuance of an additional search warrant.[18]

CONCLUSION

The landmark rulings in *Riley* and *Fulton* make clear the dangers that new technology poses to privacy interests. Of necessity, these cases mandate new rules and standards for the search process to ensure that search warrants not duplicate prohibited general warrants.

[18] In *In re Application for Search Warrant, supra*, the Vermont Supreme Court rejected the argument that an issuing authority had the power to abrogate the judicial doctrinal of plain view. However, the Court did approve a functional equivalent to no plain view: a pre-search requirement that all non-responsive seizures be segregated by the independent forensic examiner and not turned over to the investigators or other law enforcement officers. Without protocols that prohibit use of non-responsive materials or elimination of the plain view exception in digital searches, the risks are too great that agents will engage in overbroad searches. *See, e.g.*, *United States v. Loera*, 923 F.3d 907 (10th Cir. 2019) (finding unconstitutional a search that disclosed non-responsive materials, but permitting its use under inevitable discovery doctrine).

Respectfully submitted,

Michael Witsch
Pa. I.D. No. 313884
Armstrong Teasdale LLP
2005 Market Street, 29th Floor
Philadelphia, PA 19103
(267) 780-2000

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

Andrew Christy
Pa. I.D. No. 322053
American Civil Liberties Union of Pennsylvania
P.O. Box 60173
Philadelphia, PA 19102
(215) 592-1513 x138

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

Bradley Winnick
Pa. I.D. No. 78413
President, Pennsylvania Association of Criminal Defense Lawyers
Of counsel
Chief Public Defender
Dauphin County Public Defender's Office
2 South Second Street, 2nd Floor
Harrisburg, PA 17101
(717) 780-6393

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 at the addresses and in the manner listed below:

Via PACFile and USPS

Michael Wayne Streily
Allegheny County District Attorney's Office
436 Grant Street
Pittsburgh, PA 15219

Jacob Christian McCrea
Jacob Mccrea Law LLC
429 Fourth Ave Ste 1700
Pittsburgh, PA 15219

/s/ *Andrew Christy*
Andrew Christy

Dated: July 25, 2019