No. 19-4172

IN THE UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff–Appellee,

v.

JAMES TIMOTHY COBB,

Defendant–Appellant.

On Appeal from the United States District Court for the Northern District of West Virginia, Clarksburg

Case No. 1:18-cr-00033-IMK-MJA

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION & AMERICAN CIVIL LIBERTIES UNION OF WEST VIRGINIA IN SUPPORT OF APPELLANT

Nathan Freed Wessler
Brett Max Kaufman
Ezekiel Edwards
Jason D. Williamson
ACLU Foundation
125 Broad St., 18th Floor
New York, NY 10004
212.549.2500
nwessler@aclu.org

Jennifer Granick
ACLU Foundation
39 Drumm St.
San Francisco, CA 94111
415.621.2493
jgranick@aclu.org

Loree Stark
ACLU of West Virginia Foundation
P.O. Box 3952
Charleston, WV 25339
304.345.9246
lstark@acluwv.org

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 19-4172 Caption: United States v. Cobb

Pursuant to FRAP 26.1 and Local Rule 26.1,

American Civil Liberties Union and American Civil Liberties Union of West Virginia
(name of party/amicus)

who is amici, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☒ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(a)(2)(B))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☐ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: /s/ Nathan Freed Wessler Date: July 15, 2019

Counsel for: Amici

CERTIFICATE OF SERVICE

****

I certify that on July 15, 2019 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

/s/ Nathan Freed Wessler
(signature)

July 15, 2019
(date)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTERESTS OF AMICI[1]

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with more than two million members and supporters dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. 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 *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

The ACLU of West Virginia is a non-profit corporation dedicated to advancing civil liberties in West Virginia; it is an affiliate of the ACLU. Like the national organization, the ACLU of West Virginia has a long-time interest in protecting West Virginians' rights to privacy.[2]

[1] All parties consent to the filing of this brief. No party or party's counsel authored this brief or contributed money to fund the preparation or submission of this brief. No person other than amici, their members, and their counsel contributed money to fund the preparation or submission of this brief.

[2] Amici would like to thank Alexander Koster, a former student in the Advanced Technology Law & Policy Clinic at NYU School of Law, for his significant contributions to this brief.

INTRODUCTION

Every day, law enforcement agents obtain and execute search warrants for digital materials stored on desktop computers, laptops, and cell phones. The information stored on these devices is vast, diverse, and far more sensitive than information stored in a filing cabinet, or even an entire home. Nevertheless, the court below held that when there is probable cause to search a device for evidence of one crime, the investigator may randomly open any or all other digital files stored on the device. This rule would transform every warrant to search an electronic device into a general warrant, allowing investigators to peruse potentially huge quantities of private material entirely unrelated to the factual predicate for a particular investigation.

Fortunately, there are more reasonable means of conducting digital searches without eviscerating the Fourth Amendment, including by imposing *ex ante* search protocols, using forensic search tools that protect non-responsive information from human eyes, using independent third party search teams, or simply by establishing in advance that the government may only retain or use material that is actually responsive to a warrant.

Because the computer search in this case was the digital equivalent of a general search, the Court should find it unconstitutional and should provide much-

needed guidance to lower courts about how to authorize and oversee electronic devices searches consistent with the Fourth Amendment.

ARGUMENT

I. Warrants to search digital devices must be circumscribed by search protocols or other limitations to ensure that they do not become unconstitutional general warrants.

Indiscriminate searches of hard drives and other electronic storage media, even if conducted pursuant to a warrant, violate the Fourth Amendment. Like other searches, electronic-device searches must be particularized—that is, cabined to files and folders for which the affidavit in support of the warrant provides probable cause. A contrary rule would give investigating officers a free hand to examine any and all files on a hard drive, merely because some files may be subject to search. That would upend the longstanding constitutional baseline rule that searches must be particularized and cannot constitute generalized rummaging through personal and private materials.

A. Searches must be limited to materials for which there is probable cause.

In order to comply with the Fourth Amendment, a search warrant must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The particularity requirement of the Fourth Amendment is designed to ensure that those "searches deemed necessary should be as limited as possible." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

Constitutional searches must not consist of "a general, exploratory rummaging in a person's belongings." *United States. v. Robinson*, 275 F.3d 371, 381 (4th Cir. 2001) (citing *Andresen v. Maryland*, 427 U.S. 463, 480 (1976)).

The particularity requirement is even more important when the privacy interests in the place to be searched are highly sensitive. In *Stanford v. Texas*, for example, the Supreme Court explained that "the constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas which they contain." 379 U.S. 476, 511–12 (1965). In *Berger v. New York*, the Supreme Court similarly stated that the need for particularity "is especially great in the case of eavesdropping" because such surveillance "involves an intrusion on privacy that is broad in scope." 388 U.S. 41, 56 (1967).

Searches of digital information differ from physical-world searches in critical ways. *See Riley v. California*, 573 U.S. 373, 394–95 (2014); *Carpenter v. United States*, 138 S. Ct. 2206, 2217–18 (2018). Such searches threaten to intrude on protected privacy and property interests even more severely than electronic eavesdropping or searches of books and other written materials.

For one, computers contain far *more* information of an extremely personal nature than even the most capacious filing cabinet ever could. *See Riley*, 573 U.S. at 394–95; *see also United States v. Comprehensive Drug Testing, Inc.* (*CDT*), 621

F.3d 1162, 1175 (9th Cir. 2010) (en banc) (per curiam); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542 (2005).[3] Further, new *kinds* of data are stored in digital format that can reveal extraordinarily sensitive information. Many categories of information that courts have recognized as deserving of particularly stringent privacy protections can be contained on people's electronic devices, including internet browsing history, medical records, email, privileged communications, and associational information. *See, e.g.*, *Riley*, 573 U.S. at 395; *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001); *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010). Indeed, the search of such devices "would typically expose to the government far more than the most exhaustive search of a house," not least because they "contain[] a broad array of private information *never* found in a home in any form" prior to the digital age. *Riley*, 573 U.S. at 396–97.

B. Electronic-device searches are challenging to execute because officers cannot readily tell which files are lawfully subject to search and seizure—but solutions are now available.

Digital searches require strict adherence to the Fourth Amendment's particularity requirement in order to avoid unconstitutional rummaging through private materials. To be sure, meeting this requirement can be challenging. Yet

[3] Laptops sold in 2019 can store up to four terabytes of information, the equivalent of more than 2.5 billion pages of text. *See, e.g.*, Apple, Compare Mac Models, https://perma.cc/2LT8-FN3B; LexisNexis, *How Many Pages in a Gigabyte* (2007), https://perma.cc/HN26-3ZVC.

courts and investigators have effective tools at their disposal to comply with the Fourth Amendment's command.

In the physical world, searches generally are readily particularized by the practical characteristics of the things and places for which there is probable cause. For example, officers are easily restricted to looking in only those places large enough to hold the physical items particularly described in the warrant. Police cannot open a spice box when searching for a rifle. *See, e.g.*, *Horton v. California*, 496 U.S. 128, 141 (1990). Nor can they rummage through a medicine cabinet to look for a flat-screen television. *See, e.g.*, *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013).

However, this common-sense limit is much more difficult to apply in the digital realm. Digital data for which there is probable cause may, to a human eye, look more or less the same as non-responsive off-limits information. For example, a word-processing document might contain text, images, or both—but a human observer may not readily anticipate which before opening the file. Similarly, the size of an electronic file has little bearing on the file's contents. *See id.* at 447; *United States v. Hill*, 322 F. Supp. 2d 1081, 1090–91 (C.D. Cal. 2004) (Kozinski, J.) ("There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it."), *aff'd* 459 F.3d 966 (9th Cir. 2006).

In light of this challenge, this Court in *United States v. Williams*, 592 F.3d 511, 521 (4th Cir. 2010), and the district court below, JA246, have suggested that officers have little choice but to rummage through any or all digitally stored materials to look for evidence of the crime under investigation—thereby exposing an enormous variety of private data to expansive searches and seizures. But the assumptions underlying this conclusion nearly a decade ago in *Williams* have been undermined by subsequent technological and legal developments.

First, courts now have more experience imposing search protocols or other limitations to circumscribe digital searches, thus preventing overbroad searches that would "render[]the Fourth Amendment irrelevant." *CDT*, 621 F.3d at 1168–69, 1176 (per curiam); *see also, e.g.*, *id.* at 1179 (Kozinski, C.J., concurring) (detailing digital search protocols); *In re Appeal of Application for Search Warrant*, 71 A.3d 1158 (Vt. 2012) (same). *See infra* Part II.A.

And second, technology has changed since this Court's opinion in *Williams*. If it were ever true, it is no longer the case that in executing warrants for searches of digital information, investigators sometimes must manually "open each file on the computer and view its contents, at least cursorily, to determine whether the file [falls] within the scope of the warrant's authorization." *Williams*, 592 F.3d at 521. Today, there are readily available forensic tools that (1) do a better job of searching for information than a human review can; (2) do a better job of protecting the

privacy of non-responsive information; and (3) do a better job of ensuring that evidence seized has not been tampered with or altered in the course of an investigation. *See infra* Part II.B.

II. With technology, courts can ensure that searches of digital devices are particularized, comprehensive, and reliable without investigators rummaging through every file.

A. Courts have met the challenges posed by searches of digital devices by circumscribing those searches in various ways to ensure Fourth Amendment compliance.

There is a growing judicial recognition that courts must impose limits on digital searches—for example, via *ex ante* search protocols—to ensure Fourth Amendment protections for highly sensitive digital information. Many courts have suggested limits above and beyond those imposed on traditional physical-world searches. These limits nevertheless permit law enforcement to conduct effective investigations, but without unreasonable invasions of privacy.

For example, the *en banc* Ninth Circuit has recognized that the digital age calls for "greater vigilance on the part of judicial officers in striking the right balance between" law-enforcement interests and privacy, and in ensuring that digital searches do "not become a vehicle for the government to gain access to data which it has no probable cause to collect." *CDT*, 621 F.3d at 1177 (per curiam).[4]

[4] In *CDT*, the government obtained a warrant to search the electronically-stored drug-testing records of ten Major League Baseball players. 621 F.3d at 1166 (per curiam). When executing the warrant, however, agents examined the drug-testing

The various opinions in *CDT* proposed a menu of potential solutions in the form of *ex ante* search protocols, without which magistrates should deny search warrants for digital data. *See id.* at 1179–80 (Kozinski, C.J., concurring) ("summ[ing] up" the court's guidance).

One option is to require the use of independent review teams to "sort[], segregat[e], decod[e] and otherwise separat[e] seizable data (as defined by the warrant) from all other data," so as to shield investigators from exposure to information beyond the scope of the warrant. *Id.* at 1179; *see id.* at 1168–72 (per curiam). Another is to require the use of technology, including "hashing tools," to identify responsive files "without actually opening the files themselves." *Id.* at 1179 (Kozinski, C.J., concurring). And yet another is to "waive reliance upon the plain view doctrine in digital evidence cases," full stop—in other words, to agree not to take advantage of the government's unwillingness or inability to conduct digital searches in a particularized manner. *Id.* at 1180; *see id.* at 1170–71 (per curiam). Regardless of the method chosen, however, it "must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents." *Id.* at 1180 (Kozinski, C.J., concurring).

---

records of hundreds of other players whose files were intermingled with those of the ten players named in the warrant. *Id.*

Courts now regularly implement versions of these solutions. For example, in Vermont, magistrates may design and supervise "targeted searches" by "restricting law enforcement's search to those items that met certain parameters based on dates, types of files, or the author of a document." *See In re Search Warrant*, 71 A.3d at 1184. Similarly, the Tenth Circuit requires that computer search warrants affirmatively limit the search to evidence of specific federal crimes or specific types of material, and investigators are prohibited from indiscriminately opening every file on a hard drive. *See United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005); *United States v. Burgess*, 576 F.3d 1078, 1091 (10th Cir. 2009) ("If the warrant is read to allow a search of all computer records without description or limitation it would not meet the Fourth Amendment's particularity requirement."). Other courts have similarly held that, under the Fourth Amendment's particularity requirement, law enforcement may need to use date-range restrictions, or other limitations, to prevent the potential for "general rummaging" when searching electronically stored information such as email accounts. *See, e.g.*, *In re Search of Info. Associated with Email Addresses Stored at Premises Controlled by Microsoft Corp.*, 212 F. Supp. 3d 1023, 1037 (D. Kan. 2016)*; In re [REDACTED]@gmail.com*, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) (denying a search warrant for a particular email account because "there [was] no date restriction of any kind").

A recent district court case from Michigan helpfully illustrates how courts are now confronting these issues. In *United States v. Stetkiw*, the government insisted, and the court was concerned, that, "individuals might hide information in a way that forces a protocol-bound investigator to overlook it." No. 18-20579, 2019 WL 2866516, at *5 (E.D. Mich. July 3, 2019) (Roberts, J.). Nevertheless, the court held that "an *ex ante* 'minimization' requirement can address concerns about potential Fourth Amendment violations of protocol-less searches, with a goal of decreasing the amount of non-responsive [electronically stored information] encountered in a search." *Id.* (citing Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates' Revolt*, 68 Emory L.J. 49, 55 (2018)). The court concluded that *ex ante* procedures would have several advantages: they would minimize contentious *ex post* review in the suppression context; they would allow for case-by-case tailoring of warrants to uncover materials whose seizure is supported by probable cause; they would permit judicial conversation over appropriate limitations; and they would help prevent even inadvertent conversions of warrants into general warrants. *See id.* While the *Stetkiw* court did not maintain that *ex ante* protocols must be required in every case, it did suggest that in order to escape such protocols, the government "should demonstrate that the level of probable cause to search [electronically stored information] is high enough to justify a search without minimization." *Id.*

B. Forensic tools enable law enforcement to conduct effective digital searches without rummaging through every file.

Requiring law enforcement to perform particularized digital searches will not interfere with legitimate investigations. Today's forensic tools enable law enforcement (or independent "clean teams") to efficiently and effectively conduct comprehensive hard drive searches, sifting out responsive material from other data, without a human looking at every file.

It is true that computer files are easy to disguise or rename. It is also true that evidence may be not only contained in an electronic file, but also in volatile memory, configuration files, or operating system data. Contrary to common assumptions (and government claims), however, these facts do not require investigators to open every file in order to locate the evidence to which the government is entitled through a search warrant. In fact, comprehensive human review can often be counterproductive or incomplete. For example, a human does not have enough time to search every file, and rummaging does not reveal evidence that may be hiding in these other forms of storage. Further, randomly opening files (as the investigator did in this case) may alter the data on the machine, risking accidental spoliation or obfuscation. *See* Madihah Saudi, *An Overview of Disk Imaging Tool in Computer Forensics* § 5.1 (SANS Institute 2019), https://perma.cc/P7QK-7WPQ ("One of the cardinal rules in computer forensics is never work on the original evidence."); Karen Kent et al. *Guide to*

Integrating Forensic Techniques Into Incident Response: Recommendations of the Nat'l Inst. of Standards & Tech. (Nat'l Inst. of Standards & Tech., Tech. Admin., U.S. Dep't of Commerce, No. 800-86, Aug. 2006), https://perma.cc/Y2N7-K65R.

Forensic software, on the other hand, offers law enforcement a tool for running particularized digital searches—that is, searches that are designed to reveal files and folders for which a warrant establishes probable cause. To be clear, in many cases, forensic software technically *searches* every file as well as other data stored on a hard drive. But the search is more *reasonable* because it becomes far less likely that non-responsive data will be exposed to investigators.

For example, EnCase Forensic Software ("EnCase") is a law enforcement search tool for hard drives and mobile devices. EnCase can be configured to search for specific files or types of data on the computer—such as emails, internet searches,[5] photographs,[6] documents,[7] files over a specified size,[8] files with a particular extension,[9] files containing personal identifying information (such as email addresses and credit card, Social Security, and phone numbers),[10] or files

[5] Guidance Software, EnCase Forensic User Guide Version 8.07, at 64–65 (2018), https://perma.cc/NN95-ZNPM.

[6] *Id.* at 62.

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *Id.* at 338.

containing certain keywords.[11] Law enforcement widely uses these forensic tools because they search regardless of how the information is stored or named. For example, while file extension search filters are imperfect (since a suspect could disguise a photo by resaving a ".jpg" to a ".doc" extension),[12] "file header" functionalities on EnCase can determine a file's format regardless of filename or extension.[13] Forensic software programs can also detect embedded file images—that is, photographs hidden inside of Microsoft Word documents.[14] And while keyword searches can be imperfect,[15] today Optical Character Recognition ("OCR")—a common forensic tool that automatically extracts text contained in graphic files, such as images or non-searchable PDFs—addresses that challenge.[16]

The tools also perform targeted searches, which enable investigators to comprehensively and efficiently home in on the digital evidence most likely to be

[11] *Id.* at 143, 246.

[12] Computer Crime & Intellectual Prop. Section, Crim. Div., U.S. Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 36 (2009), https://perma.cc/VP23-RZTJ ("DOJ Manual") (quoting *United States v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006)).

[13] Kerr, 119 Harv. L. Rev. at 545.

[14] *See, e.g.*, AccessData, Forensic Toolkit User Guide 139 (2017), https://perma.cc/E5KY-F6LY ("FTK User Guide") ("To recover embedded or deleted files, the case evidence is searched for specific file headers. . . . Embedded or deleted items can be found as long as the file header still exists.").

[15] DOJ Manual at 79.

[16] FTK User Guide at 95 ("The [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.").

warrant-responsive, while ignoring other information. Investigators can limit a search to a particular date range, allowing analysts to obtain files within temporal proximity of the relevant crime.[17] EnCase can automatically identify illegal files (such as child pornography) without a human investigator needing to open the file. Similar tools include Forensic ToolKit and Cellebrite. There are many such products on the market and available to law enforcement at the state and local level as well as to the FBI.

These facts call into question the district court's claim that there was a need to randomly open up files on the defendant's laptop to determine which files were authorized for seizure. JA247. Forensic software could conduct a more thorough search without altering the data on the original hard drive or disclosing non-responsive information to the officer.[18] These facts also explain why older case law, like *Williams*, 592 F.3d at 521, does not dictate the outcome here: that decision was premised on the unavailability of modern forensic tools that are widely used today. Technology has exacerbated the danger of general searches in the digital realm, but it may also be used to ensure that those searches comply with the Fourth Amendment going forward.

---

[17] *Id.* at 102.

[18] Indeed, the investigators in this matter had access to the state police digital lab in Morgantown, which employs "[s]ome kind of forensic tool" that eventually was used to more comprehensively examine the seized hard drive. JA129.

III. The plain-view exception to the warrant requirement should not apply to indiscriminate digital searches.

The use of *ex ante* search protocols imposed by a magistrate—whether they be assignment to "clean teams," targeted search protocols, or the use of forensic tools—would be the preferred approach in most cases. But where police do not adopt such methods, courts should firmly reject application of the "plain view" exception to the Fourth Amendment's warrant requirement.

"[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)). Among those exceptions is "plain view." *See, e.g.*, *Coolidge*, 403 U.S. 443. The plain-view exception developed in cases concerning physical-world searches, permitting the government to obtain evidence not covered by a warrant where law enforcement discovered it in the course of a lawfully authorized search. However, the application of the plain-view exception does not make sense in the context of highly invasive searches of laptops, hard drives, and other electronically stored information.

A. Exceptions to the warrant requirement are strictly circumscribed by their own justifications and the strength of government and private interests.

Exceptions to the warrant requirement do not apply automatically upon invocation; rather, they must remain "[]tether[ed]" to "the justifications underlying the . . . exception." *Gant*, 556 U.S. at 343. The government bears the burden of demonstrating that an exception to the warrant requirement ought to apply in a given context. *United States v. Jeffers*, 342 U.S. 48, 51 (1951). As the Supreme Court recently explained, this analysis requires courts to "assess[] 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*, 573 U.S. at 385. Time and time again, the Supreme Court has refused to "unmoor [warrant] exception[s] from [their] justifications . . . and transform what was meant to be an exception into a tool with far broader application." *Collins v. Virginia*, 138 S. Ct. 1663, 1672–73 (2018). Thus, the Supreme Court has chosen not to apply even well-recognized warrant exceptions where the underlying rationale for an exception is absent from a given fact pattern.

This is particularly so when courts are asked to apply analog-era exceptions to new digital contexts. *See, e.g.*, *Riley*, 573 U.S. at 393; *Carpenter*, 138 S. Ct. at 2222. In *Riley*, the Court declined to extend the search-incident-to-arrest exception developed in cases involving arrestees' possession of items like cigarette packs to

the digital information contained on an arrestee's cell phone. There, the government "assert[ed] that a search of all data stored on a cell phone [was] 'materially indistinguishable' from searches of . . . physical items," but the Court issued a harsh rejoinder:

> That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.

573 U.S. at 393. Holding otherwise would have "untether[ed] the rule from the justifications underlying the [search-incident-to-arrest] exception"—that is, officer safety and evidence preservation. *Id.* at 386.

Similarly, 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. *See* 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.

The Supreme Court has limited other warrant exceptions to their justifications as well. In *Gant*, for example, 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." 556 U.S. at 346. In *Collins v. Virginia*, the Court held 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. 138 S. Ct. at 1672–73. And in *City of Los Angeles v. Patel*, the Court declined to apply the exception for closely regulated industries to warrantless searches of hotel guest registries because, unlike inherently dangerous industries with a history of government oversight such that no proprietor could have a reasonable expectation of privacy, "nothing inherent in the operation of hotels poses a clear and significant risk to the public welfare." 135 S. Ct. 2443, 2454 (2015).

Similarly, this Court recently declared in *United States v. Kolsuz*, that "[a]s a general rule, the scope of a warrant exception should be defined by its justifications." 890 F.3d 133, 143 (4th Cir. 2018) (citing *Riley*, 573 U.S. at 385–91). The Court further explained that—particularly when it comes to digital-age

searches—"where the government interests underlying a Fourth Amendment exception are not implicated by a certain type of search, and where the individual's privacy interests outweigh any ancillary governmental interests, the government must obtain a warrant based on probable cause." *Id*. As a result, in *Kolsuz*, the Court had little trouble rejecting the government's argument that the "border search exception," which is "justified by the government's power to regulate the export of currency and other goods," including "dangerous weapons," permits invasive, suspicionless searches of travelers' electronic devices conducted at a national border. *Id.* at 138. Other courts have performed similar analyses. *See, e.g.*, *United States v. Kim*, 103 F. Supp. 3d 32, 59 (D.D.C. 2015) (refusing to extend border-search exception to warrantless search of laptop computer).

B. The traditional justifications for the plain-view doctrine—law-enforcement safety and evidence preservation—do not hold up in the context of highly invasive digital searches.

As the Supreme Court explained in *Riley*, 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." 573 U.S. at 385. As discussed above, there is an enormous (and growing) privacy interest in electronic devices like laptop computers and cell phones. *See supra* Part I.A; *Riley*, 573 U.S. at 393–98. On the other hand, the

government interest justifying the plain-view exception is "the desirability 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) (citing *Coolidge*, 403 U.S. at 467–68). Applying plain view to excuse a warrantless search may make good sense where delay caused by obtaining a warrant could lead to evidence spoliation. *See, e.g.*, *Washington v. Chrisman*, 455 U.S. 1, 9 (1982); *Ker v. California*, 374 U.S. 23, 42 (1963). But a plain-view argument fails where the interests served by the application of the exception are outweighed by the privacy interests involved. *See, e.g.*, *Coolidge*, 403 U.S. at 472.

The justifications underlying plain view—evidence preservation and officer safety—are at their apex in relation to seizures, but not necessarily searches. *United States v. Jacobsen*, 466 U.S. 109, 114 (1984) ("Even when government agents may lawfully seize such a package to prevent loss or destruction of suspected contraband, the Fourth Amendment requires that they obtain a warrant before examining the contents of such a package."). This Court has been even more categorical, explaining that "[t]he 'plain-view' doctrine provides an exception to the warrant requirement for the *seizure* of property, but it does not provide an exception for a search." *United States v. Jackson*, 131 F.3d 1104, 1108 (4th Cir. 1997).

The plain-view doctrine developed in cases involving physical-world searches, where evidence is tangible and discrete, but searches of digital information are a poor fit for the plain-view exception because the justifications underlying the exception are, by and large, absent in this context. First, officer safety is not implicated in a controlled environment like an off-site forensics laboratory. *See generally* David H. Angeli & Christina M. Schuck, *The Plain View Doctrine and Computer Searches: Balancing Law Enforcement's Investigatory Needs with Privacy Rights in the Digital Age*, 34 Champion 18, 23 (Aug. 2010). 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. Second, evidence preservation is not at risk in a typical computer search, which normally begins with the creation of a "bitstream" copy of the target hard drive.[19] Third, where the computer hard drive is preserved pending execution of the warrant, the police have ample time to obtain additional warrants (say, for evidence of an unrelated crime) without risking evidence destruction. *See, e.g.*, Christina M. Schuck, Note, *A Search for the Caselaw to Support the Computer Search*

[19] Kerr, 119 Harv. L. Rev. at 540.

"Guidance" in United States v. Comprehensive Drug Testing, 16 Lewis & Clark L. Rev. 741, 760–61 (2012).[20]

In order to apply plain view, first, law enforcement's observation of the plain-view evidence must have taken place after an initially lawful intrusion (based on, for example, an existing warrant or exigency). *See United States v. Sifuentes*, 504 F.2d 845, 848 (4th Cir. 1974) (citing *Coolidge*, 403 U.S. at 466). Second, the evidence and its incriminating character must be "obvious to the senses"—that is, there for the seeing, out in the open, rather than obscured or hidden. *See id.* Moreover, the discovery of the material will often (if not always) be inadvertent, rather than intentional. *See id.*; *Horton*, 496 U.S. at 130.

These conditions are not regularly met in the context of searches of digital information. First, a warrant to search for *some* material on a computer does not automatically entitle the government to review *all* of the material on that computer. *See supra* Part I.A. Second, the incriminating nature of digital evidence will not immediately be "obvious to the senses" because file types, names, and sizes do not necessarily reveal their contents. *See supra* Part I.B. And last, when the government opens files one by one, it knows that it will encounter non-responsive information for which there is no probable cause—which is hardly inadvertent.

[20] Of course, the government may not retain nonresponsive data beyond the time reasonably necessary to execute its warrant. *See, e.g.*, *United States v. Ganias*, 824 F.3d 199, 226–41 (2d Cir. 2016) (en banc) (Chin, J., dissenting).

IV. This case illustrates why the plain-view exception should not apply when the government conducts an indiscriminate digital search.

The facts of this case show why permitting the government to rely on the plain-view exception to introduce evidence obtained through indiscriminate searches of digital information endangers the public's constitutional rights.

First, officers were investigating a murder case and lacked any probable cause to search the defendant's computer for child pornography. Nevertheless, the officer who searched Defendant's computer for evidence related to the homicide admitted that he intended to search for evidence of crimes unrelated to the homicide. JA116, JA118, JA124. The officer's decision to open files manually—a random, indiscriminate, and broad search method—enabled him to achieve his unconstitutional goal. *See also* JA40, JA113–14 (officer admitting that he uses the "[a]ny and all evidence of any other crimes" language in almost every search warrant for digital information); JA127 (officer "encountered" the pornographic photographs "just by going through the files"); JA128 ("I started clicking on some icons and the [pornographic] pictures came up and they were just there."). At the suppression hearing, the officer testified that "you never know what you're going to find." JA118.

This officer effectively said out loud what silently lurks in many digital-search cases: "going through files" and "clicking on icons" converts even a facially

particularized warrant into an unconstitutional general warrant.[21] *See, e.g.*, *CDT*, 621 F.3d at 1171 (per curiam) ("The government agents obviously were counting on the search to bring constitutionally protected data into the plain view of the investigating agents."). The mere fact that this was a digital search should not enable an officer to deliberately rummage for evidence of "any and all crimes," in violation of bedrock Fourth Amendment principles. *See supra* Part I.A.

Second, the perfunctory nature of the officer's interaction with the magistrate in obtaining the second warrant illustrates how critical it is for courts like this one to ensure that magistrates require reasonable search protocols when authorizing digital searches. *See supra* Parts I.B, II.A. Here, the officer met with the magistrate—who was not familiar with the investigation, and did not ask the officer any questions—for five minutes before walking away with an approval. JA40–45, JA121–22. But as searches of digital information become more and more commonplace (and more and more capable of leading to deeply intrusive searches of material unrelated to the purposes of authorized searches), the supervisorial role

[21] This would be a different case had the officer inadvertently discovered the child pornography as a result of a targeted search query designed to obtain only evidence of the homicide. Under those facts, the discovery of the contraband files might have fallen within the plain-view exception. However, other than searching for references to "suffocation"—the mechanism of injury in Mr. Wilson's homicide—the officer did not employ targeted search techniques of any kind. JA126. Rather, as mentioned, his search method was random and indiscriminate. *Id.*

of independent magistrates will become more and more important. *See, e.g.*, *Stetkiw*, 2019 WL 2866516, at *5.

Third, neither of the justifications that underlie the traditional plain-view doctrine—evidence preservation nor officer safety—are relevant to this case. *See supra* Part III.B. Police had seized the defendant's laptop and the investigation was concerned with motive rather than any ongoing crimes. JA110. The defendant was in custody. There was no exigency or continuing danger.

CONCLUSION

For the reasons stated above, the evidence obtained after the investigator randomly opened files on the defendant's computer should have been suppressed.

Date: July 15, 2019

/s/ Nathan Freed Wessler
Nathan Freed Wessler
Brett Max Kaufman
Ezekiel Edwards
Jason D. Williamson
ACLU Foundation
125 Broad St., 18th Floor
New York, NY 10004
212.549.2500
nwessler@aclu.org
bkaufman@aclu.org

Jennifer Granick
ACLU Foundation
Speech, Privacy, and Technology Project
39 Drumm St.
San Francisco, CA 94111
415.621.2493
jgranick@aclu.org

Loree Stark
ACLU of West Virginia Foundation
P.O. Box 3952
Charleston, WV 25339
304.345.9246
lstark@acluwv.org

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify that:

This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 5,988 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionately spaced typeface using Times New Roman 14-point font.

Date: July 15, 2019

/s/ Nathan Freed Wessler
Nathan Freed Wessler

Counsel for Amici

CERTIFICATE OF SERVICE

I hereby certify that on July 15, 2019, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit by using the appellate CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

Date: July 15, 2019

/s/ Nathan Freed Wessler
Nathan Freed Wessler

Counsel for Amici

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

APPEARANCE OF COUNSEL FORM

BAR ADMISSION & ECF REGISTRATION: If you have not been admitted to practice before the Fourth Circuit, you must complete and return an Application for Admission before filing this form. If you were admitted to practice under a different name than you are now using, you must include your former name when completing this form so that we can locate you on the attorney roll. Electronic filing by counsel is required in all Fourth Circuit cases. If you have not registered as a Fourth Circuit ECF Filer, please complete the required steps at Register for eFiling.

THE CLERK WILL ENTER MY APPEARANCE IN APPEAL NO. 19-4172 as

☑ Retained ☐ Court-appointed(CJA) ☐ Court-assigned(non-CJA) ☐ Federal Defender ☐ Pro Bono ☐ Government

COUNSEL FOR: American Civil Liberties Union and American Civil Liberties Union of West Virginia as the
(party name)

☐ appellant(s) ☐ appellee(s) ☐ petitioner(s) ☐ respondent(s) ☑ amicus curiae ☐ intervenor(s) ☐ movant(s)

/s/ Nathan Freed Wessler
(signature)

Please compare your information below with your information on PACER. Any updates or changes must be made through PACER's Manage My Account.

Nathan Freed Wessler
Name (printed or typed)

(212) 549-2500
Voice Phone

American Civil Liberties Union Foundation
Firm Name (if applicable)

(212) 549 -2654
Fax Number

125 Broad Street, 18th Floor

New York, NY 10004
Address

nwessler@aclu.org
E-mail address (print or type)

CERTIFICATE OF SERVICE

I certify that on July 15, 2019 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

/s/ Nathan Freed Wessler
Signature

July 15, 2019
Date