No. 19-618

IN THE

Supreme Court of the United States

JON ERIC SHAFFER,

Petitioner,

v.

COMMONWEALTH OF PENNSYLVANIA,

Respondent.

On Petition for a Writ of Certiorari to the Supreme Court of Pennsylvania

BRIEF OF THE DKT LIBERTY PROJECT, THE DUE PROCESS INSTITUTE, AND REASON FOUNDATION AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

JESSICA RING AMUNSON
Counsel of Record
ANDREW C. NOLL
JENNER & BLOCK LLP
1099 New York Ave., NW
Suite 900
Washington, DC 20001
(202) 639-6000
jamunson@jenner.com

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTIONAL PROVISIONS

OTHER AUTHORITIES

INTEREST OF *AMICI CURIAE*[1]

Amici curiae are non-profit organizations dedicated to the protection of individual liberties, especially those guaranteed by the Constitution of the United States. *Amici* have a particular interest in defending individual liberties against novel and unprecedented government encroachment in today's digital world. The vast amount of sensitive and personal information available on Americans' digital devices necessarily means that searches of those devices "would typically expose to the government far more than the most exhaustive search of a home." *Riley v. California*, 573 U.S. 373, 396-97 (2014). The decision of the Pennsylvania Supreme Court below, therefore, poses a serious threat to individual liberty. *Amici* are the following:

The DKT Liberty Project was founded in 1997 to promote individual liberty against encroachment by all levels of government. The Liberty Project is committed to defending privacy, guarding against government overreach, and promoting every American's right and responsibility to function as an autonomous and independent individual. The Liberty Project espouses vigilance against government overreach of all kinds, but especially with respect to restrictions on individual civil liberties. In particular, over the past two decades the

---

[1] Pursuant to Rule 37.2(a), counsel for *amici curiae* provided timely notice to counsel of record for all parties of *amici*'s intention to file this brief. Counsel of record for Petitioner and Respondent have both consented to the filing of this brief. Pursuant to Rule 37.6, *amici* affirm that no counsel for a party authored this brief in whole or in part, and no person other than *amici* or their counsel made a monetary contribution to this brief's preparation or submission.

Liberty Project has filed briefs as *amicus curiae* with this Court in significant cases addressing the application of the Fourth Amendment to advances in technology, including *Kyllo v. United States* (No. 99-8508), *Riley v. California* (No. 13-132), and *Carpenter v. United States* (No. 16-402).

The Due Process Institute is a bipartisan, nonprofit, public-interest organization that works to honor, preserve, and restore principles of fairness in the criminal justice system. Formed in 2018, the Due Process Institute has already participated as an *amicus curiae* before this Court in cases presenting important criminal justice issues, such as *Timbs v. Indiana*, 139 S. Ct. 682 (2019), *Mitchell v. Wisconsin*, 139 S. Ct. 2525 (2019), *United States v. Haymond*, 139 S. Ct. 2369 (2019), and *Asaro v. United States*, No. 19-107 (petition for certiorari pending).

Reason Foundation is a national, nonpartisan, and nonprofit public policy think tank, founded in 1978. Reason's mission is to advance a free society by applying and promoting libertarian principles and policies—including free markets, individual liberty, and the rule of law. Reason supports dynamic market-based public policies that allow and encourage individuals and voluntary institutions to flourish. Reason advances its mission by publishing *Reason* magazine, as well as commentary on its websites, and by issuing policy research reports. To further Reason's commitment to "Free Minds and Free Markets," Reason participates as *amicus curiae* in cases raising significant constitutional or legal issues.

SUMMARY OF ARGUMENT

Access to a digital device like a laptop, tablet, or smartphone, is rapidly becoming essential in today's interconnected world. Digital devices have become ubiquitous. Americans use their devices, and the internet connectivity they provide, to carry out essential tasks in their day-to-day lives like communicating with loved ones, applying for jobs, accessing government services, finding housing, conducting banking and other financial transactions, and attending school. Even the most basic tasks can require—or at least can be made easier by—a digital device. And when those devices break or falter, Americans quite naturally turn to third-party repair services.

That is just what happened in this case. Petitioner Jon Shaffer sought out a repair for the laptop he owned for both business and personal use from CompuGig, a laptop repair store. That repair required replacement of the laptop's hard drive and the manual copying of the laptop's contents to the new hard drive. But after finding what he thought were illicit images on Petitioner's hard drive, the repair technician called law enforcement, who seized the laptop and, under the so-called "private search" doctrine, conducted a warrantless search of Petitioner's laptop for evidence of a crime.

The "private search" doctrine is a product of a different era. In 1981—the same year that the first "portable computer" was introduced—FedEx employees working at the airport in Minneapolis-St. Paul observed that a package had been damaged in transit. Upon opening the package and finding a white

powder, the employees called the Drug Enforcement Agency ("DEA"), who came out, re-opened the package, conducted chemical field tests on the powder, and determined it was cocaine. In *United States v. Jacobsen*, 466 U.S. 109 (1984), this Court held that the agents' actions did not violate the Fourth Amendment because "there was a virtual certainty that nothing else of significance was in the package" beyond the white powder, and because inspection of the package's contents "would not tell [the agents] anything more than [they] already had been told." *Id.* at 118-19.

The digital devices of today are nothing like the cardboard boxes of yesteryear. Yet the court below and courts across the country have applied the "private search" doctrine to digital devices as if they were the equivalent of cardboard boxes. Courts do this despite the fact that modern digital devices allow individuals to now carry on their person "the digital equivalent of [their] home." *United States v. Mitchell*, 565 F.3d 1347, 1352 (11th Cir. 2009) (quotation marks omitted). A vast array of intimate details can be learned about a person from the information accessible on a digital device—personal communications, movements, health information, financial information, and other "privacies of life." *Riley*, 573 U.S. at 403 (quotation marks omitted).

Accordingly, lower courts' application of the private search doctrine to digital devices like Petitioner's cannot be squared with the Fourth Amendment or this Court's precedents. Unlike a DEA agent re-opening a cardboard box, a law enforcement officer confronted with a digital device that has been accessed by a third-party cannot possibly be certain of the device's contents or that

additional private information will not be disclosed. Nor can it seriously be maintained that a reasonable individual, by providing a laptop or other digital device to a third-party repair shop like CompuGig, thereby grants an implied license *to the government* to rifle through that device.

Without this Court's intervention, the vast amount of information accessible on digital devices will remain subject to warrantless searches. Multiple courts have taken a broad view of the private search doctrine's application to digital devices. Those courts have concluded that a private individual's search of even *a single file* on a device—or an automated algorithm that flags certain documents to be provided to law enforcement—is sufficient to expose an entire digital device, with all of its contents, to a warrantless search.

This Court should grant the petition for a writ of certiorari to clarify the applicability—if any—of the "private search" doctrine to today's digital world.

ARGUMENT

I. Digital Devices Are Essential Features Of Modern Life, Critical To Individuals' Liberty And Ability To Engage In Society.

Petitioner, Mr. Shaffer, sought to have the laptop computer he used for both personal and business activities repaired by a computer repair shop called CompuGig. *See* Pet. App. 2a. The fact that Petitioner used a laptop computer, needed to get that device repaired, and thus provided the device to a third-party to view and temporarily possess, is unexceptional. That is because digital devices—like personal computers,

smartphones, and tablets—are ubiquitous in America today.

Computer ownership, in particular, has skyrocketed over the past three decades. As of 2015, at least seventy-eight percent of households owned a desktop or laptop computer, up from eight percent in 1984, the year this Court decided *United States v. Jacobsen*. *See* Camille Ryan & Jamie M. Lewis, Am. Cmty. Survey Reports, U.S. Census Bureau, *Computer and Internet Use in the United States: 2015*, at 2-3 (2017).[2] Nearly half of American households now own tablet computers. *Mobile Fact Sheet*, Pew Research Ctr. (2019).[3] And eighty-one percent of Americans own a smartphone—an overwhelming proportion of the ninety-six percent of Americans overall who own a cell phone. *Id.* Cell phones also rapidly are replacing landlines as Americans' primary communication method. Stephen J. Blumberg & Julian V. Luke, Nat'l Ctr. for Health Statistics, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July – December 2018*, at 2 (2019).[4] The result is that, to conduct even

---

[2] https://www.census.gov/content/dam/Census/library/publications/2017/acs/acs-37.pdf.

[3] https://www.pewresearch.org/internet/fact-sheet/mobile/.

[4] https://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201906.pdf. Smartphones are rapidly becoming Americans' primary mode of accessing the internet, too. A "growing share" of Americans use their smartphone as their *only* means of accessing the internet, even in their homes. *Mobile Fact Sheet*, *supra*. And, even when they have a broadband internet connection available, thirty-seven percent of Americans still use a smartphone to access the internet.

basic telephone calls, more and more people are using digital devices that are really "multifunctional computer[s] that just happen to have telephone capabilities." Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 Harv. J.L. & Pub. Pol'y 403, 404 (2013). Digital devices, in short, are everywhere. So pervasive are devices like cell phones that "the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley*, 573 U.S. at 385.

Moreover, an individual's liberty and ability to meaningfully engage in society now often depends on access to a digital device. Given their omnipresence, it can be exceedingly difficult for individuals to build a community, keep in touch with loved ones, or access basic services without a digital device. Access to both "computers and a broadband Internet subscription" are "increasingly important to Americans in carrying out their day-to-day lives." Ryan & Lewis, Am. Cmty. Survey Reports, *supra*, at 1. This Court has recognized, particularly with respect to cellular phones, that the services these devices provide "are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (quoting *Riley*, 573 U.S. at 385).

Computers and internet access "open[] the door to a variety of opportunities." Ryan & Lewis, Am. Cmty.

See Monica Anderson, Pew Research Ctr., *Mobile Technology and Home Broadband 2019*, at 2 (2019), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/06/PI_2019.06.13_Mobile-Technology-and-Home-Broadband_FINAL2.pdf.

Survey Reports, *supra*, at 9. Digital devices—and the internet connectivity those devices enable—allow Americans to access health information, conduct banking, find housing, apply for jobs, access government services, or attend school and gain an education. *Id.* at 1.

Intimate family and friend associations are developed and maintained increasingly by text message and through social media, particularly among young people. *See, e.g.*, Amanda Lenhart, *et al.*, Pew Research Ctr., *Teens, Technology, & Friendships*, at 10 (2015).[5] Cell phones help families coordinate and arrange their schedules to deal with the chaos of everyday life. Judy Wajcman, Michael Bittman & Judith Brown, *Families without Borders: Mobile Phones, Connectedness and Work-Home Divisions*, 42 Sociology 635, 636 (2008).

With respect to work, the internet is a critical resource. When searching for work, a majority of U.S. adults have looked for job information online, and a near majority have applied for a job over the internet. Aaron Smith, Pew Research Ctr., *Searching for Work in the Digital Era*, at 2 (2015).[6] Today, "the top 20 private employers in the U.S., as ranked in the Fortune 500, all require job applications to be submitted online." Daniel Greene & Ifeoma Ajunwa, *Automated Hiring Platforms*

---

[5] http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/08/Teens-and-Friendships-FINAL2.pdf.

[6] https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2015/11/PI_2015-11-19-Internet-and-Job-Seeking_FINAL.pdf.

as Technological Intermediaries and Brokers, at 1 (2017) (unpublished manuscript).[7]

Even after one secures a position, business and employment demands also frequently require individuals to be connected through digital devices. Globally, more than 293 billion business and consumer emails are sent per day. Radicati Grp., Inc., *Email Statistics Report, 2019-2023*, at 2 (2019).[8] What is more, a majority of workers' jobs require them to be, at least on occasion, outside the physical boundaries of the workplace. Pew Research Ctr., *Technology's Impact on Workers*, at 2-3 (2014).[9] And since 2005, remote work has increased by 159 percent. *See* Brie Weiler Reynolds, *159% Increased in Remote Work Since 2005: FlexJobs & Global Workplace Analytics Report*, FlexJobs (July 29, 2019).[10] To make a living in today's economy, then, a laptop, smartphone, or other digital device is frequently critical—most of all for the quarter of Americans who earn some money through the "gig economy" spurred by

---

[7] http://dmgreene.net/wp-content/uploads/2014/11/GreeneAjunwa Automated-Hiring-Plaforms-as-Technological-Intermediaries-and-Brokers.pdf.

[8] https://www.radicati.com/wp/wp-content/uploads/2018/12/Email-Statistics-Report-2019-2023-Executive-Summary.pdf.

[9] https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2014/12/PI_Web25WorkTech_12.30.141.pdf.

[10] https://www.flexjobs.com/blog/post/flexjobs-gwa-report-remote-growth/.

digital platforms. Aaron Smith, Pew Research Ctr., *Gig Work, Online Selling and Home Sharing*, at 2 (2016).[11]

In myriad other ways—from the critical to the mundane—digital devices and the connectivity they enable are necessary features of modern life. Banking requires, or at least is made easier through, computers and other digital devices. *See* Bd. of Governors of the Fed. Reserve Sys., *Consumers and Mobile Financial Services 2016*, at 8 (Mar. 2016).[12] Emergency alerts can more easily be disseminated to the public through digital devices, and internet connectivity can have life-saving consequences. If unable to reach 911, many adults report that they "would try to contact responders through a digital means such as e-mail, websites or social media." *Web Users Increasingly Rely on Social Media to Seek Help in a Disaster*, PR Newswire (Aug. 9, 2010, 9:39 AM).[13] And, if they knew of someone who needed help, a significant percentage of people report that they would "ask other people in their social network to contact authorities," would "post a request for help directly on a response agency's Facebook page," or would "send a direct Twitter message to responders." *Id.*

---

[11] http://assets.pewresearch.org/wp-content/uploads/sites/14/2016/11/17161707/PI_2016.11.17_Gig-Workers_FINAL.pdf.

[12] https://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201603.pdf.

[13] https://www.prnewswire.com/news-releases/web-users-increasingly-rely-on-social-media-to-seek-help-in-a-disaster-100258889.html.

Unfortunately, digital devices also break. And when that happens, people (like Petitioner here) often seek to have them repaired. In 2012, for example, it was reported that the Apple Genius Bar serviced approximately 50,000 people *per day* worldwide—amounting to more than 18 million appointments per year. Jim Dalrymple, *Apple Stores See 300 Million Visitors in FY 2012, 50,000 Genius Bar Visits a Day*, Loop (Aug. 20, 2012, 9:36 AM)[14]; Buster Hein, *Apple's Genius Bar Services Over 18 Million People A Year, And Other Crazy Stats*, Cult of Mac (Aug. 20, 2012).[15] By 2015, that number had increased to 95,000 customers per day. Steve Kovach, *10 Mind-Blowing Facts About the Apple Store*, Bus. Insider (Mar. 13, 2015, 10:20 AM).[16] In fact, sales of the most recent iPhone model dropped precisely because people are now likely to repair their iPhones rather than purchase new ones. *See, e.g.*, Jason Koebler, *Tim Cook to Investors: People Bought Fewer New iPhones Because They Repaired Their Old Ones*, Vice (Jan. 2, 2019, 5:56 PM).[17]

The record in this case, then, reflects the position many individuals are likely to find themselves in today: having provided a digital device to a third-party.

---

[14] https://www.loopinsight.com/2012/08/20/apple-stores-see-300-million-visitors-in-2012-50000-genius-bar-visits-a-day/.

[15] https://www.cultofmac.com/185762/did-you-know-apples-genius-bar-services-over-18-million-people-a-year/.

[16] https://www.businessinsider.com/apple-store-facts-2015-3.

[17] https://www.vice.com/en_us/article/zmd9a5/tim-cook-to-investors-people-bought-fewer-new-iphones-because-they-repaired-their-old-ones.

Consequently, it is unsurprising that "[o]ne of the most common factual situations giving rise to private search analysis in computer cases involves repair technicians" observing possible "evidence of illegal activity" while "attempting to fix a client's computer." Benjamin Holley, Note, *Digitizing the Fourth Amendment: Limiting the Private Search Exception in Computer Investigations*, 96 Va. L. Rev. 677, 684 (2010). Petitioner's situation is likely to recur only more frequently as digital devices continue to proliferate.

II. A Vast Amount Of Intimate And Personal Information Is Accessible On Digital Devices.

The Fourth Amendment protects the right of people to be secure in their "houses," "papers" and "effects." U.S. Const. amend. IV. Today, a person's papers and effects are often predominately housed on digital devices like laptop computers and cellular phones. Indeed, these devices can provide access to more information than can even be found in the "sanctity of the home," where, this Court has long maintained, "*all* details are intimate." *Kyllo v. United States*, 533 U.S. 27, 37 (2001). Digital devices, in essence, enable people to "lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read." *Riley*, 573 U.S. at 393-94. Though often smaller than a cardboard box, digital devices obviously can reveal far more information than one might find by opening a FedEx package.

This is made possible by the immense storage capability of computers, tablets, and smartphones. Most laptops provide a minimum of 500 gigabytes of storage space, although many provide far more. Mark Kyrnin,

Guide to Laptop Storage Drives, Lifewire (Nov. 12, 2019).[18] Petitioner's laptop here, in fact, had 500 gigabytes of storage capacity. *See* Pet. at 15. That is the equivalent of at least 32 million pages of Microsoft Word documents, 50 million emails, and 7.7 million image files. *How Many Pages in a Gigabyte*, LexisNexis (last visited Dec. 4, 2019).[19] Just like computers, one of the "most notable distinguishing features" of the modern cell phone "is [its] immense storage capacity." *Riley*, 573 U.S. at 393. Smartphones are no less than "minicomputers that also happen to have the capacity to be used as a telephone." *Id.*

And this is all before one accounts for the remote storage enabled by cloud computing. Remote storage like the cloud allows one to access a far greater amount of information than can be housed directly on a device. Cloud computing can enable files to be "mirrored" on the user's computer, even if stored elsewhere; thus, "[b]y merely looking at a cloud-connected device, it is impossible to know the nature or quantity of information accessible." Aya Hoffman, Note, *Lost in the Could: the Scope of the Private Search Doctrine in a Cloud-Connected World*, 68 Syracuse L. Rev. 277, 287-88, 295 (2018). The use of cloud storage is growing: by 2021, ninety-five percent of all data center internet traffic is projected to be cloud traffic. *Cisco Global Cloud Index:*

---

[18] https://www.lifewire.com/laptop-storage-drives-guide-833445.

[19] https://www.lexisnexis.com/applieddiscovery/lawlibrary/white Papers/ADI_FS_PagesInAGigabyte.pdf.

Forecast and Methodology, 2016-2021 White Paper, Cisco (Nov. 19, 2018).[20]

As a result, a hard drive like Petitioner's in this case is "the digital equivalent of its owner's home, capable of holding a universe of private information." *Mitchell*, 565 F.3d at 1352 (internal quotation marks omitted). What at one time "would have required an entire library is now contained in a two-pound block measuring 7 x 4.5 x 1.5 inches." Samuel Crecelius, Note, Lichtenberger *and the Three Bears: Getting the Private Search Exception and Modern Digital Storage 'Just Right'*, 4 Tex. A&M L. Rev. 209, 221 (2017) (footnote omitted).

This information, moreover, is "deeply personal." Kerr, *supra*, at 405. For many, digital devices hold "the privacies of life." *Riley*, 573 U.S. at 403 (quotation marks omitted). Personal messages from family members, friends, or intimate partners may be memorialized in email messages, texts, voicemails, or video files maintained on a digital device. Or a device's owner may have recorded personal writings or diaries, audio memos, or videos containing his private thoughts. Many use smartphones as their primary camera, and thus one could piece together the daily life of an individual through the photographs and videos stored on a phone or uploaded to a laptop computer.

Digital devices can also portray the movement and activity of a person over months or years. Electronic calendars are used by individuals and businesses alike, and can include particularly sensitive information like

---

[20] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html.

records of visits to medical providers, counselors or therapists, and drug or alcohol programs. Ride-sharing applications, location-based services, or check-ins and posts on social media can also provide a digital repository of an individual's daily movements. Collectively, records such as these provide "an intimate window into a person's life" and reveal "his 'familial, political, professional, religious, and sexual associations.'" *Carpenter*, 138 S. Ct. at 2217 (quoting *United States v. Jones*, 565 U.S. 400, 415 (opinion of Sotomayor, J.)).

Both financial and healthcare information are increasingly being housed and managed by individuals on their digital devices. And even minimal information like a computer's "screen saver, wallpaper, and names of files on the home screen" can convey intimate details about a person. Pet. App. 54a-55a (opinion of Wecht, J.).

It should go without saying that individuals accordingly have a strong expectation of privacy in the contents of their digital devices. Pointedly, the court below *did not* hold that Petitioner abandoned his legitimate expectation of privacy through the simple act of providing his laptop to CompuGig for repair. *See* Pet. App. 18a-19a, 37a. For good reason. An individual does not relinquish his expectation of privacy based "solely on the act of sharing." *Carpenter*, 138 S. Ct. at 2219. As explained above, digital devices are critical for engaging in everyday life and, relatedly, necessarily must be shared with third-parties at times. Those realities cannot undermine the weighty privacy interests presented by digital devices.

III. Given Their Ubiquity And Storage Capabilities, Applying The Private-Search Doctrine To Digital Devices Cannot Be Squared With This Court's Precedents.

Lower courts' application of what has become known as the "private search" doctrine cannot be squared with the realities of digital devices or with this Court's precedents. "When confronting new concerns wrought by digital technology," this Court has "been careful not to uncritically extend existing precedents." *Carpenter*, 138 S. Ct. at 2222. The Court's reasoning in *Jacobsen*, as the Petition explains, was premised on the fact that the DEA agents there could have "virtual certainty" that "nothing else of significance" was in the cardboard box that the private individuals had already examined. 466 U.S. at 119; Pet. at 16. Given the immense amount of information that is stored directly on laptops, smartphones, and other digital devices—as well as made accessible through the cloud—it simply is not true that a law enforcement officer can be certain she will find nothing significant on a device beyond the material that a private individual already may have uncovered. "Unlike rifling through the contents of a cardboard box, a foray into one folder of a digital storage device will often expose nothing about the nature or the amount of digital information that is, or may be, stored elsewhere in the device." *State v. Terrell*, 831 S.E.2d 17, 25 (N.C. 2019).

As this Court has recognized time and again, the Fourth Amendment "was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British

officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley*, 573 U.S. at 403. The Framers' "central aim" in adopting the Fourth Amendment was "'to place obstacles in the way of a too permeating police surveillance.'" *Carpenter*, 138 S. Ct. at 2214 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

Thus, in both *Riley* and *Carpenter*, when concluding that the rationales underpinning other exceptions to the warrant requirement did not map onto the realities of cellular phones, this Court considered it highly relevant that digital devices such as cellular phones have the propensity to reveal a significant amount of information. In *Riley*, this Court unanimously refused to extend the search-incident-to-arrest exception to permit warrantless searches of cell phones because cell phones "differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." 573 U.S. at 393. Likewise, in *Carpenter*, this Court declined to apply the third-party doctrine to a person's historical cell-site records because those records supply an "all-encompassing record of the holder's whereabouts" and can provide "an intimate window into a person's life" with "just the click of a button." 138 S. Ct. at 2217-18. This Court explained that applying those exceptions to cellular phones would, in effect, closely approach the very same general warrants that the Fourth Amendment was intended to reject. *See, e.g.*, *Riley*, 573 U.S. at 403.

The same is true with the private-search doctrine and as applied to digital devices more generally. Just like a cell phone, the search of any digital device will

"typically expose to the government far more than the most exhaustive search of a home." *Id.* at 396-97. If anything, because electronic storage contains a "greater quantity and variety of information than any previous storage method, computers make tempting targets in searches for incriminating information," and even the other information they house, "irrelevant to the subject of the lawful investigation, will also be searched or seized." Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 105 (1994). Allowing a different avenue for law enforcement to evade the warrant requirement would significantly undercut this Court's decisions in *Riley* and *Carpenter*.

In addition, in *United States v. Jones*, this Court emphasized that separate and apart from the reasonable expectations standard, a "physical intrusion" by the government to "occup[y] private property for the purpose of obtaining information" constitutes a search within the meaning of the Fourth Amendment. 565 U.S. 400, 404-05 (2012). Thus, the Fourth Amendment is "understood to embody a particular concern for government trespass upon the areas" enumerated in the amendment. *Id.* at 406. A reasonable individual, by providing a laptop or other digital device to a third-party repair shop like CompuGig, would not consider herself to have relinquished her possessory interest in her property to any and all third-parties. And certainly it cannot seriously be maintained that an individual who provides a device to a repair shop thereby grants an implied license *to the government* to rifle through that device or review any material that the repair shop

employees happen to view. *See* Andrew MacKie-Mason, *The Private Search Doctrine After* Jones, 126 Yale L.J. Forum 326, 331 (2017) (under trespass theory, "[t]he fact that someone has previously entered or interfered does almost nothing to erode the interest in exclusion"). The decision below cannot be squared with *Jones*.

IV. Without This Court's Intervention, Digital Devices Will Remain Subject To Expansive Warrantless Searches By Law Enforcement.

Absent this Court's intervention, the private-search doctrine will continue to be used by law enforcement to gain access to the wide range of sensitive information that this Court's precedents otherwise place beyond reach without a warrant. That is because, "[t]oday, the private-search doctrine arises most frequently in cases involving private searches of digital data." Ben A. McJunkin, *The Private-Search Doctrine Does Not Exist*, 2018 Wis. L. Rev. 971, 984. Particularly in those circuits that have taken a broad view of the doctrine's application to digital devices, there exist significant opportunities for law enforcement abuse.

The approach taken by the Fifth and Seventh Circuits is emblematic of the broad reading of the private-search doctrine, which places individuals' intimate details at risk of search any time they hand their devices over to a third-party. These courts have held that *any* access to a digital device's contents, even to a handful of files, opens up the entire device for further inspection by law enforcement—without a warrant or any restriction on law enforcement's search.

In *United States v. Runyan*, the Fifth Circuit, analogizing CD-ROMs, floppy disks, and thumb drives to closed containers, concluded that "police do not exceed" the scope of a private search "when they examine more items within a closed container than did the private searchers." 275 F.3d 449, 464 (5th Cir. 2001). There, the defendant's ex-wife had seized a number of CDs, floppy disks, and thumb drives and viewed files on some, but not all, of those materials. *Id.* at 462. With respect to the disks that the defendant's ex-wife had reviewed only in part, the Court held that law enforcement may go on to examine without a warrant "more files on each of the disks than did the private searchers." *Id.* at 464. District courts in the Fifth Circuit have relied on *Runyan* when considering private searches of more modern devices. One court has held that an entire cellular phone is made subject to a warrantless law enforcement search whenever a private search *of any kind* has been conducted. *See Garcia v. City of Loredo*, No. 5:10-cv-30, 2011 WL 9559236, at *3-4 (S.D. Tex. Sept. 1, 2011) (finding it "unnecessary" to determine whether the private individual "viewed all the content contained in the cell phone as part of her initial search" because, "[w]hen city officials viewed the contents of the cell phone, the scope of their search was limited to a single container, the cell phone, which had previously been privately searched"), *aff'd*, 702 F.3d 788 (5th Cir. 2012).

The Seventh Circuit's more recent application of the private-search doctrine to "digital storage devices"—a zip drive and camera memory card—is even more striking. In *Raan v. Atchison*, the court adopted the

Fifth Circuit's reasoning in *Runyan*, and described the Fifth Circuit's holding as concluding that "a search of *any material* on a computer disk is valid if the private party who conducted the initial search had viewed *at least one file on the disk*." 689 F.3d 832, 836 (7th Cir. 2012) (emphasis added). The Seventh Circuit applied that reasoning to the police's search of a zip drive that the court assumed private individuals had reviewed, at least in part, given those individuals' representation to police that the devices contained illicit images. *Id.* at 837-38. Any subsequent search of the digital storage devices, the court held, did not violate the Fourth Amendment. *Id.* at 838.

As one district court has rightly cautioned, the approach these courts have taken, in effect, "permit[s] the government to conduct a warrantless search of the entirety of a computer and all of its unopened files based upon the earlier identification of merely one contraband file or image." *United States v. Howe*, No. 09-CR-6076L, 2011 WL 2160472, at *13 (W.D.N.Y. May 27, 2011), *report and recommendation adopted by*, 2012 WL 1565708 (W.D.N.Y. May 1, 2012), *aff'd in part*, 545 F. App'x 64 (2d Cir. 2013).

And, as technology advances, law enforcement has even greater opportunities to take advantage of these courts' broad conception of the private-search doctrine. Recently, the Fifth Circuit considered a computer algorithm that a cloud hosting service automatically applied to files uploaded to its service. The algorithm identified in each file "hash values"—"short, distinctive identifiers" that allow computer users to compare two files' contents. *United States v. Reddick*, 900 F.3d 636,

636, 637-38 (5th Cir. 2018), *cert. denied*, 139 S. Ct. 1617 (2019). If the uploaded files' hash values matched the hash values of known illicit images, the file and the uploader's IP address were passed along to law enforcement. *Id.* at 638. The Fifth Circuit concluded that the cloud hosting service's "automatic[] review[]" through its algorithm was an inspection "by a private actor" that allowed the government to invoke the private-search doctrine. *Id.* at 639.

In other words, the Fifth Circuit concluded that an automated review by a computer program—and not a human—is a "private search" sufficient to allow law enforcement to conduct a subsequent warrantless search. Others have rightly questioned whether such a mechanized approach to hash values, where the private actor "never opened [the file] itself" is consistent with *Jacobsen*—never mind whether *Jacobsen* itself can be squared with this Court's decision in *Jones*. *United States v. Ackerman*, 831 F.3d 1292, 1305-06 (10th Cir. 2016) (Gorsuch, J.); *id.* at 1307 ("Reexamining the facts of *Jacobsen* in light of *Jones*, it seems at least possible the Court today would find that a 'search' did take place there.").

In any event, without this Court's review of the decision below, some courts will continue to apply their settled precedent that any search by a private actor of a digital device opens up the entire device to a subsequent search by law enforcement. Law enforcement can then search a laptop, like Petitioner's, *without a warrant* and *without consent*. Accepting this approach would provide a ready exception to the warrant requirement that evades this Court's insistence that recognized

exceptions to the warrant requirement do not automatically apply in the context of digital devices. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2222.

Obviously, it is precisely when other recognized exceptions to the warrant requirement—like exigent circumstances or knowing and voluntary consent—are not applicable that the government would be forced to resort to the private-search doctrine. Thus, the only compelling reason for law enforcement to rely on the doctrine is to avoid the hassle of obtaining a warrant.

In fact, the Department of Justice specifically identifies the private search doctrine as a basis for searching and seizing a computer without a warrant. A Department of Justice search and seizure guide specifically argues that that the Fifth Circuit's approach in *Runyan*, discussed above, permits "a warrantless search by law enforcement of *the computer's entire contents*" following a third party's "search of a single file on a computer." Computer Crime & Intellectual Prop. Section Criminal Div., Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, at 11 (3d ed. 2009) (emphasis added).[21] Accordingly, the federal government informs its law enforcement officials that, so far as some courts have held, officials may take advantage of the doctrine to access even more information on a computer than may have been accessed by a private individual.

That result is irreconcilable with the Fourth Amendment. The warrant requirement "serves a high

---

[21] https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

function" by interposing "a magistrate between the citizen and the police" to neutrally "weigh the need to invade [an individual's] privacy in order to enforce the law," and to particularly describe the scope and limits of any subsequent search. *McDonald v. United States*, 335 U.S. 451, 455 (1948). Indeed, even the Department of Justice acknowledges that the private search doctrine is not necessary to ultimately access digital materials. That is because "the information gleaned from the private search will often provide the probable cause needed to obtain a warrant for a further search"—without the need for a warrantless search by law enforcement. DOJ, *Searching and Seizing Computers*, *supra*, at 12.

Digital devices are necessary to individuals' everyday lives and their ability to engage with society. But they also make accessible a vast array of intimate information. This Court should grant review to reconsider the approaches taken by some lower courts that have insulated expansive warrantless searches by law enforcement from Fourth Amendment protection.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

December 16, 2019

Respectfully submitted,

JESSICA RING AMUNSON
Counsel of Record
ANDREW C. NOLL
JENNER & BLOCK LLP
1099 New York Ave., NW
Suite 900
Washington, DC 20001
(202) 639-6000
jamunson@jenner.com

Counsel for Amici Curiae