No. 19-____

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

PETITION FOR A WRIT OF CERTIORARI

AMIR H. ALI
Counsel of Record
MEGHA RAM*
RODERICK & SOLANGE
MACARTHUR JUSTICE CENTER
777 6th Street NW, 11th Fl.
Washington, DC 20001
(202) 869-3434
amir.ali@macarthurjustice.org

Counsel for Petitioner

*Admitted only in California; not admitted in D.C. Practicing under the supervision of the Roderick & Solange MacArthur Justice Center.

QUESTIONS PRESENTED

In *United States v. Jacobsen*, 466 U.S. 109 (1984), this Court held that government agents did not need a warrant to reopen an "ordinary cardboard box" because private actors had previously opened the box. *Id.* at 111. The Court reasoned that the private actors' initial search eliminated the owner's "legitimate expectation of privacy." *Id.* at 120. Because government agents could have "virtual certainty" that reopening an ordinary box would reveal "nothing else of significance," doing so was not "a 'search' within the meaning of the Fourth Amendment." *Id.* at 115-21.

In lower courts, *Jacobsen* has birthed a general exception to the Fourth Amendment, called the "private-search doctrine." It is now "one of the most convoluted and misunderstood corners to the Fourth Amendment." Ben A. McJunkin, *The Private-Search Doctrine Does Not Exist*, 2018 WIS. L. REV. 971, 972 (2018). Today, the government uses *Jacobsen* "most frequently" not to reopen a box, but for constitutionally exempt searches of digital data. *Id.* at 984. The questions are:

1. Does the "virtual certainty" that reopening "an ordinary cardboard box" will expose nothing beyond the private actor's earlier search, *Jacobsen*, 466 U.S. at 119, authorize constitutionally exempt searches of digital devices, like a personal and business laptop?

2. When the government "obtains information by physically intruding" on property, *United States v. Jones*, 565 U.S. 400, 406 n.3 (2012), is that trespass overlooked simply because a private actor previously examined the property? In other words, is *Jacobsen* rendered obsolete in light of the property-based test?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Constitutional Provisions, Statutes, and Rules

Other Authorities

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

PETITION FOR A WRIT OF CERTIORARI

Jon Eric Shaffer petitions for a writ of certiorari to review the Supreme Court of Pennsylvania's judgment in this case.

OPINIONS BELOW

The Supreme Court of Pennsylvania's opinion (Pet. App. 1a-72a) is published at 209 A.3d 957. The state court of appeals' opinion (Pet. App. 73a-84a) is published at 177 A.3d 241. The trial court's opinion (Pet. App. 85a) is unpublished.

JURISDICTION

The Pennsylvania Supreme Court entered its judgment on June 18, 2019. On August 26, 2019 and September 30, 2019, Justice Alito granted 30-day extensions of time to file this petition, for a deadline of November 13, 2019. This Court has jurisdiction pursuant to 28 U.S.C. § 1257(a).

STATUTORY AND CONSTITUTIONAL PROVISIONS INVOLVED

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

INTRODUCTION

This Court has reasoned that when a private actor searches someone's container, he or she destroys the "legitimate expectation of privacy" in that container. *United States v. Jacobsen*, 466 U.S. 109, 120 (1984). The government can therefore also open the container without it counting as a "search" under the test articulated in *Katz v. United States*, 389 U.S. 347 (1967). *Jacobsen*, 466 U.S. at 120. Under that test, the boundaries of government conduct are controlled not by the particulars of a judicially approved warrant, *see* U.S. Const. amend. IV, but by the particulars of the search that a private actor happened to conduct, *Jacobsen*, 466 U.S. at 115-16, 122-24.

In the thirty-five years since *Jacobsen*, courts have understood it to compel a standalone Fourth Amendment exception, generally referred to as the "private-search doctrine," and have relied on that exception to uphold otherwise unconstitutional government intrusions. That's what happened here. On the settled facts of this case, a private actor repairing Petitioner's laptop came across files he believed to be illicit. A government official who learned this information chose not to use it to get a warrant, and instead directed the repairperson to click around on Petitioner's laptop to reveal the contents of the files. The court below found that none of the traditional Fourth Amendment exceptions applied and resorted to the "private-search doctrine" to uphold the government's intrusion.[1]

---

[1] Although this Court has never cast its caselaw as pronouncing a general "private-search doctrine" or "private-search exception," Petitioner adopts that label because it is frequently used by lower

This petition raises two questions relating to the validity and scope of this Court's decision in *Jacobsen*:

First, this Court's holding that the Fourth Amendment did not apply when officers reopened an "ordinary cardboard box," *Jacobsen*, 466 U.S. at 111, is, today, commonly relied upon to exempt the warrantless search of digital data from constitutional scrutiny. Indeed, the Department of Justice advises its law enforcement agencies that they can rely on *Jacobsen* as authority for "Searching and Seizing Computers Without a Warrant."[2] Several times in recent terms, this Court has revisited its pre-digital Fourth Amendment caselaw when lower courts have engaged in "mechanical application" of, *Riley v. California*, 573 U.S. 373, 386 (2014), or "uncritically extend[ed] existing precedents" to the digital era, *Carpenter v. United States*, 138 S. Ct. 2206, 2222 (2018). The court below did that, and so have others. A conflict exists, and it stems from differing interpretations of *Jacobsen*'s

---

courts. Some courts have used other names to describe the same general exception. *E.g.*, *State v. Wright*, 114 A.3d 340, 342 (N.J. 2015) ("third-party intervention doctrine"). This exception, under which government intrusion is exempt from the Fourth Amendment if it can identify similar conduct by a private actor, should not be confused with the basic rule that the Fourth Amendment does not apply to wholly private action (such as the technician's initial search in this case). *See Burdeau v. McDowell*, 256 U.S. 465, 475 (1921). The private-search doctrine also should not be confused with its "close relative," the "third-party doctrine." Ben A. McJunkin, *The Private-Search Doctrine Does Not Exist*, 2018 WIS. L. REV. 971, 974 (2018); *see Carpenter v. United States*, 138 S. Ct. 2206, 2216-20 (2018).

[2] Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 1, 10-12 (3rd ed. 2009), *available at* https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

"pivotal test"—whether it is a narrow exemption requiring law enforcement to have an ex-ante "virtual certainty" that the object to be searched contains no other private information that could be revealed (which could virtually never be the case when it comes to digital devices) or instead calls for an ex-post assessment of whether the government "exceeded the scope of the private search." *State v. Terrell*, 831 S.E.2d 17, 28 (N.C. 2019) (Newby, J., dissenting); *United States v. Chapman-Sexton*, 758 F. App'x 437, 453 (6th Cir. 2018) (Bush, J., concurring) (observing "courts have disagreed" over "whether the best reading of *Jacobsen* requires an ex ante or an ex post analysis, or some combination of both"). Only this Court can clarify whether *Jacobsen*, decided well before the present digital age, applies to personal and business devices that today store our most intimate, sensitive, and potentially embarrassing information.

Second, the reasonable-expectations test applied in *Jacobsen* is just one way to determine whether a government's intrusion is a "search." *United States v. Jones*, 565 U.S. 400, 409 (2012). That test was "*added to*, not *substituted for*,' the traditional property-based understanding of the Fourth Amendment." *Florida v. Jardines*, 569 U.S. 1, 11 (2013) (quoting *Jones*, 565 U.S. at 409); *id.* at 12-15 (Kagan, J., concurring). Below, Petitioner repeatedly urged that the government-directed physical intrusion on his laptop constituted a search, yet his argument was dismissed out-of-hand as "not responsive," "inapposite," and "inapplicable" to the court's reasonable-expectations analysis. Pet. App. 38a n.14, 84a n.3. That "conflicts with relevant decisions of this Court." Sup. Ct. R. 10(c). The Court should resolve "the uncertain status of *Jacobsen* after

Jones." *United States v. Ackerman*, 831 F.3d 1292, 1307 (10th Cir. 2016) (Gorsuch, J.).

Lower courts resort to the private-search doctrine to uphold government conduct with "somewhat surprising frequency." Andrew MacKie-Mason, *The Private Search Doctrine After Jones*, 126 YALE L.J. FORUM 326, 326 (2017). Their experience has shown it to be "one of the most convoluted and misunderstood corners to the Fourth Amendment" and that confusion has peaked in the context of digital technology. Ben A. McJunkin, *The Private-Search Doctrine Does Not Exist*, 2018 WIS. L. REV. 971, 972 (2018). State judges, federal judges, law enforcement, and, most of all, accused people are bearing the costs of this confusion. The Court should resolve whether the doctrine survives and, if so, whether it extends to the digital era.

STATEMENT OF THE CASE

1. In 2015, Petitioner brought his personal and business laptop to CompuGig, a computer repair shop. Pet. App. 2a. Several days later, a technician told Petitioner his computer's hard drive was failing, and Petitioner consented to have the hard drive replaced. Pet. App. 3a.

The technician had difficulty transferring the data from Petitioner's original hard drive to his new one. The technician thus decided to manually open the individual folders on Petitioner's computer and copy the contents. Pet. App. 3a-4a. In the course of doing so, the technician saw thumbnail images (small images reflecting the contents of a computer file) that he believed to be sexually explicit photos of children. Pet. App. 4a. The technician reported this to his boss, and an administrative employee called the police. *Id*.

2. Later that day, Officer Christopher Maloney reported to CompuGig, and the storeowner and technician provided statements about the thumbnail images on the computer. *Id.* Rather than using those statements to get a warrant, Officer Maloney told the storeowner and technician that he "need[ed] to see the computer to verify these images" and, upon being taken to the computer, requested that the technician operate Petitioner's computer to reveal the images. *Id.*; R14A, R16A, R83A.[3] The technician "honor[ed] [the officer's] request" and began "clicking around" on Petitioner's computer. Pet. App. 4a, 30a; R14A, R79A. After seeing certain illicit images, Officer Maloney directed the technician to "shut down the file" and seized the laptop. Pet. App. 4a, 30a; R82A.

A detective later questioned Petitioner, who confessed to possessing illicit images, and only then obtained a warrant to search Petitioner's laptop, which revealed several illicit images. Pet. App. 4a-5a.

3. Respondent charged Mr. Shaffer with simple possession of child pornography and use of a communication facility (his laptop) to view child pornography. *See* 18 Pa. Cons. Stat. §§ 6312(d), 7512(a).

Petitioner filed a motion to suppress, arguing that Officer Maloney's warrantless direction to search his laptop was both "a violation of Defendant's reasonable expectation of privacy" and "a trespass upon his property" under the Fourth and Fourteenth Amendments. Pet. App. 5a-6a; R40A, R45A-47A, R101A-102A. Citing this Court's decision in *United States v. Jones*, 565 U.S. 400, 406-07 (2012), he urged that the reasonable-

[3] "R__" refers to Petitioner's "Reproduced Record," lodged with the Pennsylvania Supreme Court.

expectations and property-based approaches to determine whether a search occurred "are not mutually exclusive"; rather they "exist side-by-side." R45A. With respect to the reasonable-expectations test, Petitioner urged that "our personal computers . . . often contain the most private and sensitive information in our lives" and therefore the enhanced privacy interests this Court recognized in *Riley v. California*, 573 U.S. 373, 386 (2014), "naturally extend to the digital data stored on Defendant's personal laptop computer." R45A-47A. Under the property-based test, he argued that the government-directed search of his laptop, as in *Jones*, "physically occupied private property for the purpose of obtaining information." R46A (quoting *Jones*, 565 U.S. at 404).

The trial court denied Petitioner's motion to suppress. It concluded that "controlling" intermediate appellate precedent dictated that Petitioner "abandoned his privacy interest" in his computer files by tendering the computer for repair. Pet. App. 98a.

The court rejected Petitioner's argument that the search of his laptop was "improper based on a trespass analysis." Pet. App. 99a. Referring to its earlier analysis, the court reasoned that Petitioner "should have known that he was risking exposure of the computer files contained on the hard drive." *Id.* The court reasoned that where the technician's initial search of the computer "was explicitly or implicitly permitted by" Petitioner, it "makes no sense" to conclude that the subsequent, government-directed search was a trespass. *Id.* The government search could be justified by the fact that the technician had "properly" seen the files just "shortly before." *Id*. The court thus found "no basis for concluding" that Officer Maloney trespassed

on Petitioner's effects. Pet. App. 100a. The court acknowledged that its conclusion conflicted with then-Judge Gorsuch's opinion in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016). *Id.*

4. Petitioner appealed to the Pennsylvania Superior Court. He again advanced both his reasonable-expectations and property-based arguments, and urged that this Court "made it clear that the reasonable expectation of privacy analysis set forth in *Katz* [*v. United States*, 389 U.S. 347 (1967)] was not meant to replace the traditional property based approach to the Fourth Amendment, but rather to add to it." Pet'rs Super. Ct. Br. 12-15, 20.[4] Petitioner argued that irrespective of whether the technician's earlier search was authorized or unauthorized, the government subsequently directed a search that "activated the computer and navigated to the files containing contraband images." *Id.* at 21. The government thus "trespassed upon [Petitioner's laptop], without a warrant, for the purpose of obtaining information" and therefore conducted a search under the property-based analysis. *Id.* (citing *Jones*, 565 U.S. at 404-05).

The Superior Court affirmed. It concluded that its earlier precedent was "controlling" and therefore Petitioner abandoned any reasonable expectation of privacy in the contents of his laptop by seeking repair. Pet. App. 84a.

The court relegated Petitioner's trespass argument to a footnote. It viewed Petitioner's resort to the property-based approach as an attempt "to avoid" the result compelled by its reasonable-expectations precedent. *Id.* n.3. The court rejected the property-based

[4] *Available at* 2017 WL 4697260.

test as "inapposite" and "not responsive to the trial court's finding that [Petitioner] abandoned his privacy interest in the illicit files." *Id*.

5. In a fractured, 4-1-2 decision, the Pennsylvania Supreme Court affirmed on the alternative basis of the "private-search" doctrine.

Both the majority and the two-justice dissent explicitly rejected Respondent's and lower courts' argument that Petitioner abandoned any privacy interest in his laptop by seeking repair, in all forms that the argument had been advanced. Pet. App. 18a-19a, 37a (rejecting both the "broad proposition that one abandons his expectation of privacy each time he takes a computer for repair" and the "narrower" proposition that limited this theory to repairs "that may result in the exposure of private information"); Pet. App. 70a (Saylor, C.J., dissenting) ("I agree . . . that a person does not abandon a reasonable expectation of privacy merely by turning a computer over to a repairperson to restore its functionality.").

The three opinions expressed disagreement as to the application and scope of the "private-search" doctrine:

5a. The majority held that under *United States v. Jacobsen*, 466 U.S. 109 (1984), the technician's initial "viewing of the images extinguished [Petitioner's] reasonable expectation of privacy in the images of child pornography." Pet. App. 31a. Thus, "by the time Officer Maloney viewed the illegal images, [Petitioner's] expectation of privacy in them had already been compromised." Pet. App. 32a.

According to the majority, once the government has shown that "a private search was conducted," the

only inquiry under *Jacobsen* is "whether the police actions exceeded the scope of the private search." Pet. App. 28a. In the majority's view, that was "easily" resolved. Pet. App. 32a. Although the suppression hearing and all other proceedings below had "focused exclusively" on Respondent's abandonment theory, and therefore no record had been developed regarding the scope of the search or "the precise number of images" that Officer Maloney viewed, the private-search doctrine could be satisfied by Officer Maloney's offhand testimony that the technician "showed him 'the exact route taken to find the images.'" Pet. App. 4a n.4, 10a, 32a. The court thus held the Fourth Amendment was inapplicable to Officer Maloney's search of Petitioner's laptop. Pet. App. 38a.

The majority rejected Petitioner's arguments under the property-based approach and his reliance on *Riley v. California*, 573 U.S. 373 (2014) and *Carpenter v. United States*, 138 S. Ct. 2206 (2018). According to the majority, this line of cases was simply "inapplicable" because the government searches in them had not followed a search "conducted by a private individual." Pet. App. 37a-38a & n.14.

5b. Justice Wecht dissented in part, to "note [his] disagreement with the Majority's application of the private search doctrine." Pet. App. 52a. After reviewing *Jacobsen*, the "seminal case" giving rise to the private-search doctrine, Justice Wecht expressed concern that the private-search doctrine "poses readily identifiable risks to an individual's right of privacy, and entails a considerable potential for abuse." Pet. App. 53a. He then took issue with the majority's application of the private-search doctrine in two respects.

First, this Court's decision in *Jacobsen* was premised on a "significant" limitation: when it came to reopening a simple package, there "was 'a virtual certainty' that the second search would reveal nothing but what the Federal Express employees had found and reported." Pet. App. 54a. In Justice Wecht's view, "[t]he same cannot be said for a personal computer." *Id.* "[O]ne's personal computer contains a wealth of information, both private and public. Even the screen saver, wallpaper, and names of files on the home screen of a computer can expose private information about the individual who owns the computer." Pet. App. 55a. A personal computer thus "offers virtually limitless areas for exploration" and "[a]n inadvertent click on a file or tab could uncover to a state actor private information that was not part of the information collected initially by the private actor." *Id.* Thus, "[r]egardless of the path taken by [the technician] to locate the suspicious files as directed by Officer Maloney, there existed a very real potential for exposure of information not yet discovered by the private search." Pet. App. 54a-55a. In Justice Wecht's words: if the package in *Jacobsen* "could be said to have an opposite, that opposite would be a personal computer." Pet. App. 55a. He thus would have held "the private search doctrine to be inapplicable" to the search of Petitioner's laptop. *Id.*

Second, Justice Wecht criticized the majority for falling back on the private-search doctrine to uphold the search even though the argument had never been raised below and there had thus not been "any meaningful evidentiary development of the facts necessary for evaluation of the private search doctrine." Pet. App. 51a-52a. In Justice Wecht's view, the majority exacerbated the "identifiable risks" and "potential for

abuse" inherent in the doctrine by finding the private-search doctrine could be satisfied by testimony that "touched inadvertently" and "by happenstance" on the scope of the search. Pet. App. 50a-51a, 53a.[5]

5c. Chief Justice Saylor and Justice Donohue dissented and would have "reverse[d] the order [of] the Superior Court" in its entirety. Pet. App. 72a. They "respectfully differ[ed]" with the majority's willingness to resort to the private-search doctrine to uphold the government's conduct even though "the record ha[d] not been appropriately developed to allow for consideration" of the doctrine. Pet. App. 71a & n.1.

REASONS FOR GRANTING THE PETITION

This Court should resolve whether *Jacobsen* sanctioned constitutionally exempt searches of our digital devices and whether it survives *Jones*. The private-search doctrine frequently recurs to justify searches when none of the conventional Fourth Amendment exceptions apply. The application of *Jacobsen* generally, and to digital technology in particular, has and will continue to produce intractable questions and conflicts. That confusion is all gratuitous depending on the answers to the threshold questions here. This case involves the prototypical computer-search that scholars assume, that law enforcement singles out for warrantless intrusion, and that courts confront. It is an excellent and representative vehicle to address these questions.

---

[5] Justice Wecht would have accepted Respondent's argument that Petitioner "intended to grant unfettered access to the entire computer" by having his hard drive replaced and therefore abandoned any expectation of privacy in it. Pet. App. 66a & n.13. He was the sole member of the court to accept that argument.

I. This Court Should Decide Whether Its Decision About An "Ordinary Cardboard Box" Authorized The Constitutionally Exempt, Warrantless Searching Of Digital Devices.

Three times in recent terms, this Court has confronted questions regarding the application of earlier Fourth Amendment doctrine in the digital age. *See United States v. Jones*, 565 U.S. 400 (2012) (whether the installation of a GPS device is a Fourth Amendment search); *Riley v. California*, 573 U.S. 373 (2014) (whether the search-incident-to-arrest exception applies to the warrantless search of a cellphone); *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (whether the third-party doctrine applies to cellphone records).

In *Jones*, all members of the Court agreed that attaching a GPS device to a vehicle and tracking its movements constitutes a search under the Fourth Amendment. The Court made clear that consideration of the Fourth Amendment's application to new technologies not in existence at the framing requires careful scrutiny of the relevant privacy interests: "At bottom, [the Court] must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" 565 U.S. at 406 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)); *id.* at 428-31 (Alito, J., concurring in the judgment).

In *Riley*, the Court unanimously held that the search-incident-to-arrest exception does not extend to the warrantless search of a cellphone. In so doing, the Court rejected the government's analogy from ordinary containers, which have historically been subject

to warrantless search incident to an arrest, to cell-phones, which are essentially "minicomputers." 573 U.S. at 393-97. The Court explained that the analogy from container to computer was "strained as an initial matter," but "crumbles entirely" when considered in light of "cloud computing." *Id.* at 393-97. The Court cautioned that unexamined reliance on "pre-digital analogue[s]" risks causing "a significant diminution of privacy." *Id.* at 400. Accordingly, "any extension of [reasoning from decisions about analog searches] to digital data has to rest on its own bottom." *Id.* at 393.

In *Carpenter*, the Court considered whether the "logic [of cases setting forth the third-party doctrine] extends" to cell-site location information. 138 S. Ct. at 2216-17. In holding that the logic did not so extend, and thus the government's examination of the data was a search, the Court emphasized that "[w]hen confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents." *Id.* at 2222. The Court rejected the government's argument, which was premised on "mechanically applying" the third-party doctrine to new technology. *Id.* at 2219.

As Justice Wecht observed below, the same concerns should have prevented the mechanical application of *Jacobsen* to digital devices. Today's digital devices have "immense storage capacity" and store "the privacies of life," from photos, to calendars, to Internet browsing history. *Riley*, 573 U.S. at 393-94, 403. Indeed, even setting aside cloud computing, the storage capacity of Petitioner's laptop was over 30 times the storage that this Court viewed as "immense" in *Riley*. R35A (500-gigabyte capacity); *Riley*, 573 U.S. at 393-94.

The reason for limiting *Jacobsen* to simple containers was explicit in *Jacobsen* itself. There, FedEx employees opened an "ordinary cardboard box" that had been damaged in transit, "pursuant to a written company policy." 466 U.S. at 111. Upon opening the box and a 10-inch-long duct-tape tube within, the employees found bags of white powder. *Id.* Later, DEA agents arrived, reopened the package, and did a field-test to confirm the powder was cocaine. *Id.* at 111-12. This Court considered whether the agents' reopening of the package infringed "an expectation of privacy that society is prepared to consider reasonable." *Id.* at 113. The Court began from the unassailable premise that the employees' initial opening of the package, whether "reasonable or unreasonable" could not "violate the Fourth Amendment because of [its] private character." *Id.* at 115. The Court then reasoned that when reopening the box, a federal agent could have "a virtual certainty that nothing else of significance was in the package" and that "manual inspection" of the contents "would not tell [the DEA agent] anything more than he already had been told." *Id.* at 119.[6]

That "cannot be said for a personal computer." Pet. App. 54a (opinion of Wecht, J.). When the technician reported he had seen illicit images on Petitioner's laptop, Officer Maloney could not have had even remote

[6] The second half of *Jacobsen* concluded that the agents' field test did not infringe the defendant's "reasonable expectation" because it revealed only that the "white powder was cocaine." 466 U.S. at 122-23. The Court has already held that this aspect of *United States v. Place*, 462 U.S. 696 (2013) and *Jacobsen* does not survive the property-based approach. *See infra* pp. 30-31; *Jardines*, 569 U.S. at 10-11.

confidence that there was "nothing else of significance" on the laptop, or that manually navigating through Petitioner's computer, folders, and files to get to the desired images would not disclose any private information. *Jacobsen*, 466 U.S. at 119. "Even the screen saver, wallpaper, and names of files on the home screen of a computer can expose private information about the individual who owns the computer." Pet. App. 54a-55a (opinion of Wecht, J.). And "the possible intrusion on privacy is not physically limited in the same way when it comes to" a computer. *Riley*, 573 U.S. at 394. When an officer looks in an ordinary cardboard box, there is no risk that "[a]n inadvertent click on a file or tab" will uncover intimate privacies, from photos to business records to embarrassing browsing history. Pet. App. 54a-55a (opinion of Wecht, J.). But when searching a person's computer, there is "a very real potential of information not yet discovered by the private search." *Id.*[7]

Some courts have accordingly rejected attempts to extend *Jacobsen* to digital data. In *State v. Terrell*, 831 S.E.2d 17 (N.C. 2019), a woman discovered child pornography on a two-gigabyte thumb drive and reported it to law enforcement. *Id.* at 20, 25 n.2. An officer later navigated to "the folder that had been identified" by the woman to find the photo, and saw other images of

---

[7] Actually, concluding that *Jacobsen* intended to authorize computer searches would be quite a backwards trajectory. The Court in *Jacobsen* explicitly derived its rationale from the Court's fractured decision in *Walter v. United States*, 447 U.S. 649 (1980). *See Jacobsen*, 466 U.S. at 116-17. In *Walter*, the plurality held this reasoning could not justify the warrantless viewing of *an analog film reel* that had been collected from private actors. 447 U.S. 657 (opinion of Stevens, J.).

child pornography as well. *Id*. at 20. The court of appeals declined to extend *Jacobsen*, "guided by the substantial privacy concerns implicated in searches of digital data" expressed in *Riley*. Because the officer did not have the requisite "virtual-certainty," the ultimate scope of his search was "immaterial." *Id*. at 21. The North Carolina Supreme Court rejected the state's and the dissent's contention that this was an "unnecessarily restrictive" reading of *Jacobsen*. *Id.* at 22. The court reasoned that "[f]ollowing the mere opening of a thumb drive by a private individual, an officer cannot proceed with 'virtual certainty that nothing else of significance' is in the device 'and that a manual inspection of the [thumb drive] and its contents would not tell him anything more than he already had been told.'" *Id.* at 25; *see also id.* at 29 (Newby, J., dissenting) ("The majority's 'virtual certainty' test needlessly eliminates the private-search doctrine for electronic storage devices[.]").

Other courts have, like the majority below, been less circumspect. *See* Pet. App. 33a-36a & n.13 (joining a number of lower courts that "have applied the *Jacobsen* construct to the private search of a computer" and collecting cases). In *Rann v. Atchison*, 689 F.3d 832 (7th Cir. 2012), for instance, the Seventh Circuit "ruled on the application of *Jacobsen* to a subsequent police search of privately searched digital storage devices." *Id.* at 836. Adopting an earlier decision by the Fifth Circuit, the court extended *Jacobsen* to digital devices by "[a]nalogizing digital media storage devices to containers," and finding that the defendant's expectation of privacy in the contents of the "container" had already been frustrated by the private actor's partial intrusion into his digital device. *Id.* at

836-37 (endorsing *United States v. Runyan*, 275 F.3d 449 (5th Cir. 2001)).[8]

As Judge Bush, as well as Justice Newby's dissent in *Terrell*, have captured, the conflicting interpretations of *Jacobsen* flow from unclear and inconsistent language in *Jacobsen* itself—namely, "whether the best reading of *Jacobsen* requires an ex ante or an ex post analysis." *United States v. Chapman-Sexton*, 758 F. App'x 437, 453 (6th Cir. 2018) (Bush, J., concurring). For instance, the Supreme Court of North Carolina, like Justice Wecht here, understood *Jacobsen*'s "virtual certainty" language to require ex ante assurance that there was no other private information that could be encountered on the electronic device (just as the officers in *Jacobsen* could know there was "nothing else of significance" in the "ordinary cardboard box"). *See Terrell*, 831 S.E.2d at 25-26 (considering "the potential for officers to learn any number and all manner of things 'that had not previously been learned during the private search'"); Pet. App. 54a-55a (opinion of Wecht, J.). But, of course, no such assurance is possible in the context of electronic storage devices. Under this interpretation of *Jacobsen* it will thus "be the exceedingly rare case when the government has virtual certainty that no other evidence is on the physical device;" "[a]s a practical matter," then, "the private search reconstruction doctrine doesn't apply to computers." Orin Kerr, *North Carolina Court Deepens Split on Private Searches of Digital Evidence*,

---

[8] As discussed below, the analogy of containers to computers has begged additional, intractable questions that this Court would have to decide if it were to resolve both questions presented in Respondent's favor. *See infra* pp. 26-28.

THE VOLOKH CONSPIRACY, (Aug. 23, 2019), https://reason.com/2019/08/23/north-carolina-court-deepens-split-on-private-searches-of-digital-evidence/; *see also Terrell*, 831 S.E.2d at 29, 32 (Newby, J., dissenting) ("[W]ith electronic storage devices, there is never a 'virtual certainty' that a government searcher will not discover other unopened material" and therefore the effect of the majority's opinion is to "eliminate[] the private-search doctrine for electronic storage devices[.]").[9]

On the other hand, lower courts that uphold digital searches under *Jacobsen* have understood the "pivotal test" to be not ex-ante virtual certainty, but "the degree to which [the additional invasion of defendant's privacy by the government] exceeded the scope of the private search." *Terrell*, 831 S.E.2d at 28 (Newby, J., dissenting) (alteration in original); *see also, e.g.*,

---

[9] *See also* Brianna M. Espeland, *Implications of the Private Search Doctrine in A Digital Age: Advocating for Limitations on Warrantless Searches Through Adoption of the Virtual File Approach*, 53 IDAHO L. REV. 777, 833 (2017) ("Due to the unique characteristics of digital devices, it is virtually impossible for law enforcement to be sufficiently certain of what they will find upon the digital device."); John M. Walton III, *Virtually Certain to Frustrate: The Application of the Private Search Doctrine to Computers and Computer Storage Devices*, 43 N. KY. L. REV. 465, 485-86 (2016) ("In light of the extensive privacy interests at stake, and the impracticability of applying the private search doctrine to computers, courts should preclude the government's use of the private search doctrine when the 'container' involved is a computer[.]"); Dylan Bonfigli, *Get A Warrant: A Bright-Line Rule for Digital Searches Under the Private-Search Doctrine*, 90 S. CAL. L. REV. 307, 330 (2017) ("[C]ourts should adopt a rule like the one seen in *Riley*—a bright-line rule that exempts digital searches from the private-search exception.").

Runyan, 275 F.3d at 463 ("[U]nder *Jacobsen*, confirmation of prior knowledge does not constitute exceeding the scope of a private search."); Pet. App. 32a (viewing the relevant question as whether Officer Maloney ultimately followed the "exact route taken" or "expanded upon [the technician's] actions"). For these courts, application of the Fourth Amendment is judged "from an ex post perspective (that is, after the results of the warrantless search are known)." *Chapman-Sexton*, 758 F. App'x at 452 (Bush, J., concurring).

Other lower courts have, like *Jacobsen* itself, operated on "some combination of both" an ex-ante and ex-post analysis within the same opinion. *Id.* at 453. In *United States v. Lichtenberger*, 786 F.3d 478 (6th Cir. 2015), for instance, the Sixth Circuit held the government's search of a laptop unconstitutional based principally on an ex-ante approach, concluding that the officer's "lack of 'virtual certainty' when he reviewed the contents of [the defendant's] laptop is dispositive." *Id.* at 490. But at other points, the court identified "the correct inquiry" as "whether [the government-directed] search remained within the scope of [the private actor's] earlier one." *Id.* at 485.

Only this Court can settle what *Jacobsen* meant and whether that meaning lets the government search digital devices free of the Fourth Amendment.

II. The Court Should Resolve "The Uncertain Status Of *Jacobsen* After *Jones*."

The reasonable-expectations test "is but one way to determine if a constitutionally qualifying 'search' has taken place." *United States v. Ackerman*, 831 F.3d 1292, 1307 (10th Cir. 2016) (Gorsuch, J.). It "'has been

added to, not *substituted for*,' the traditional property-based understanding of the Fourth Amendment." *Florida v. Jardines*, 569 U.S. 1, 11 (2013) (quoting *United States v. Jones*, 565 U.S. 400, 409 (2012)). The property-based approach "establishes a simple baseline." *Id.* at 5. "When 'the Government obtains information by physically intruding' on persons, houses, papers, or effects, 'a "search" within the original meaning of the Fourth Amendment' has 'undoubtedly occurred.'" *Id.* (quoting *Jones*, 565 U.S. at 406 n.3).

The property-based test "keeps easy cases easy," *id.*, and that is so here. There has never been any dispute that the challenged government search involved physical intrusion of Petitioner's laptop. *See* Pet. App. 4a; R83A (Officer Maloney testifying that the technician "click[ed] around" on Petitioner's laptop "at [his] request" to reveal the images); R79A (technician testifying that he was "honoring [Officer Maloney's] request" by clicking through the contents of Petitioner's computer to reveal the images). Under *Jones*, that ends the inquiry: That Officer Maloney "learned what [he] learned only by physically intruding on [Petitioner's] property to gather evidence is enough to establish that a search occurred." *Jardines*, 569 U.S. at 11. *Jacobsen*'s analysis of the impact of a private actor's earlier search is of no consequence. Put simply, when one physically trespasses on someone's property, it has never been a defense for the trespasser to say, "but he did it too!" *See* Andrew MacKie-Mason, *The Private Search Doctrine After Jones*, 126 YALE L.J. FORUM 326, 327 (2017) ("A prior private search may destroy a person's expectation of privacy, but it does not change whether the police trespassed on a constitutionally protected area in order to obtain information.").

By dismissing Petitioner's trespass argument as "inapposite" and "not responsive" to reasonable-expectations analysis, Pet. App. 84a n.3, and then finally as "inapplicable" because *Jones* did not involve an earlier search "conducted by a private individual," Pet. App. 38a n.14, the decisions below contravene this Court's precedent. As mentioned above, *Jacobsen* was explicitly and exclusively grounded in the reasonable-expectations test. *See Jacobsen*, 466 U.S. at 113 (stating the inquiry before the Court as whether the agents' reopening of the package infringed "an expectation of privacy that society is prepared to consider reasonable"); *id.* at 122 (explicitly limiting the Court's inquiry of "whether this can be considered a 'search' subject to the Fourth Amendment" to "did it infringe an expectation of privacy that society is prepared to consider reasonable?"). The significance this Court attached to whether the searching agent had a "virtual certainty" and never "exceeded the scope of the private search" was that it showed the agent "infringed no legitimate expectation of privacy." *Id.* at 119-20; *see also MacKie-Mason*, *supra*, at 327, 329 ("The Court's reasoning [in *Jacobsen*] turned entirely on an analysis of the package owner's reasonable expectation of privacy" test and is "irrelevant to the trespass definition of a search under *Jones*.").

Contrast the conclusion below that *Jones* is somehow "inapplicable" where the government can point to a private search with the Tenth Circuit's reaction to the same question. That court said it "cannot see how [a lower court] might ignore *Jones*'s potential impact" on *Jacobsen*. *Ackerman*, 831 F.3d at 1307. In *Ackerman*, the government invoked the private-search doctrine after searching the defendant's email and at-

tachments, arguing that AOL, a private actor, had already searched the defendant's email, including one of the attachments. A unanimous panel explained that the government search was unlawful under both the reasonable-expectations and the property-based approach. Addressing the latter, the court explained that the warrantless opening of an email "pretty clearly" qualified "as exactly the type of trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment." *Id.* at 1307-08 (collecting historical authorities). Application of the property-based approach thus led to the "pretty intuitive" result that the government "conducted a 'search' when it opened and examined [the defendant's] email." *Id.* at 1308. Considering the impact of *Jones* on *Jacobsen* generally, the court viewed it as "at least possible th[is] Court today would find that a 'search' did take place." *Id.*

The Court should grant certiorari to resolve "the uncertain status of *Jacobsen* after *Jones*." *Id.* at 1307.

III. Resolving These Questions Is Important.

The private-search doctrine arises with "somewhat surprising frequency." MacKie-Mason, *supra*, at 326. When it does arise, it is often as a fallback because no established exception justifies the government's conduct—just as occurred here. *See* Pet. App. 43a-45a (opinion of Wecht, J.) ("The private search doctrine did not make any appearance in this case until it surfaced as the Commonwealth's third line of argument in its brief to this Court."). And when it does arise, the accused's property and privacy rights are resolved according to "one of the most convoluted" areas of Fourth Amendment law that "has proven confounding in hard cases." Ben A. McJunkin, *The Private-Search Doctrine*

Does Not Exist, 2018 WIS. L. REV. 971, 972-73 (2018). As a result, *Jacobsen* endures in lower courts through a series of "ad-hoc limitations" and, as one would expect, has and will continue to generate conflicts. *Id.* at 973 & nn.10-11, 982-86; *see also e.g.*, *State v. Wright*, 114 A.3d 340, 349-51 (N.J. 2015) (describing conflict as to whether *Jacobsen* allows the warrantless search of a home).[10]

Today, the private-search doctrine recurs most frequently in the context of digital searches. McJunkin, *supra*, at 984. And, as covered in part above, courts have "developed widely varying approaches with dramatically different implications" and "no clear standards predominate." *See* Benjamin Holley, *Digitizing the Fourth Amendment: Limiting the Private Search*

---

[10] The leading Fourth Amendment treatise has described *Jacobsen*'s constitutional analysis as "less than perfect" and "doubt[ed] whether *Jacobsen* was rightly decided" in the first place. WAYNE R. LAFAVE, 1 SEARCH & SEIZURE § 1.8(b) (5th ed. 2019). Indeed, scholars have questioned whether the whole "private-search doctrine" is simply a "misreading" of earlier cases "that has snowballed into an undertheorized constitutional end-run." McJunkin, *supra*, at 975.

The difficulties caused by *Jacobsen* are well documented by the authorities cited throughout this petition. *See, e.g.*, *Runyan*, 275 F.3d at 461 (noting "the lack of definitive guidance from the Supreme Court and the lack of consensus among our sister circuits regarding the precise nature of the evaluation required"); *Chapman-Sexton*, 758 F. App'x at 454 n.9 (Bush, J., concurring) (collecting cases for the proposition that "this area of the law is cloudy"); Adam A. Bereston, *The Private Search Doctrine and the Evolution of Fourth Amendment Jurisprudence in the Face of New Technology: A Broad or Narrow Exception?*, 66 CATH. U. L. REV. 445, 446 (2016) (observing that "courts have struggled to consistently determine when and how" *Jacobsen* applies).

Exception in Computer Investigations, 96 VA. L. REV. 677, 677-78 (2010). What *is* clear is that, to the extent the superficial analogy of "containers" to computers applies, this Court will have to decide the series of intractable questions that perplexed lower courts:

- What is the analogous "container"? Is it:
  - The entire device?[11]
  - Just the "platter" of the hard drive that happened to be accessed?[12]
  - The folder containing the filed viewed?[13]
  - Just the file itself?[14]
  - Only the portion of the file that was "exposed" to the private actor?[15]

---

[11] *Rann v. Atchison*, 689 F.3d 832, 838 (7th Cir. 2012) (upholding device search "even if the police more thoroughly searched the digital media devices than [the private actors] did and viewed images that [the private actors] had not viewed").

[12] *United States v. Crist*, 627 F. Supp. 2d 575, 585-86 & n.7 (M.D. Pa. 2008).

[13] Samuel Crecelius, *Lichtenberger and the Three Bears: Getting the Private Search Exception and Modern Digital Storage "Just Right"*, 4 TEX. A&M L. REV. 209, 230 (2017).

[14] *United States v. Sparks*, 806 F.3d 1323, 1336 (11th Cir. 2015) (officer permitted to view the file seen by private actor, but violated Fourth Amendment by viewing additional file).

[15] Orin S. Kerr, *Searches and Seizures in A Digital World*, 119 HARV. L. REV. 531, 556 (2005).

- Or perhaps some other "organizational unit"?[16]

- Does the metaphorical container change depending on whether the device is a "personal computer," "flash drive," or other device?[17]
- Does the metaphorical container change if the device is or is not connected to the cloud?[18]
- What particular constraints must an officer put in place to have the necessary "virtual certainty" to search a device without obtaining a warrant?
  - Does the officer have a pre-search discussion about "which folders or subfolders [the private actor] opened or reviewed" and "'which subfolder of images they scrolled through to arrive at the' image"?[19]
  - Is it insufficient if the officer specifically "asked [the private actor] to show him what she had found"?[20]

---

[16] Joseph Little, *Privacy and Criminal Certainty: A New Approach to the Application of the Private Search Doctrine to Electronic Storage Devices*, 51 U.C. DAVIS L. REV. 345, 357 (2017).

[17] *Chapman-Sexton*, 758 F. App'x at 454 (Bush, J., concurring).

[18] Aya Hoffman, *Lost in the Cloud: The Scope of the Private Search Doctrine in A Cloud-Connected World*, 68 SYRACUSE L. REV. 277 (2018).

[19] *Terrell*, 831 S.E.2d at 26.

[20] *Lichtenberger*, 786 F.3d at 488 (finding this to be insufficient).

- Or, as the court below found, is it sufficient for the officer to just assert later that he believed the searches were coextensive?[21]

- Does the search of digital data become free of constitutional scrutiny when the "private actor" was a computer algorithm?[22]

Lower courts that have extended *Jacobsen* to digital devices have been forced to confront these questions and have already begun reaching contrary conclusions. But the time and energy spent on these intractable questions may be completely unnecessary depending on the answers to the questions here. The Court should decide these threshold questions about *Jacobsen*'s scope and validity.

IV. The Court Should Grant This Case.

Below, Petitioner specifically urged that the private-search doctrine has no application to digital devices, Pet. App. 21a, giving rise to a divided decision, Pet. App. 53a-55a (Wecht, J., dissenting on this point). Petitioner also specifically advanced both the reasonable-expectations and property-based tests, and repeatedly urged that those tests "are not mutually exclusive," but "exist side-by-side." R45A, R101A. The private search doctrine was the sole basis for the decision below. And both questions presented were considered and ruled on by the court below. Pet. App. 37a-39a & n.14. That makes this case a uniquely good vehicle and, to Petitioner's knowledge, the only prospect

---

[21] Pet. App. 32a.

[22] *E.g.*, *United States v. Reddick*, 900 F.3d 636, 637-39 (5th Cir. 2018), *cert. denied*, 139 S. Ct. 1617 (2019).

that squarely presents both of these questions. *Compare, e.g.*, *Terrell*, 831 S.Ed.2d at 27 n.5 (considering *Jacobsen*'s application to digital devices and declining to reach the defendant's argument under *Jones*).

Respondent has never argued harmless error. And the relevant facts are undisputed: A private actor—whether "accidental or deliberate" and "reasonable or unreasonable"—conducted an initial search of Petitioner's laptop with "no governmental involvement." *Jacobsen*, 466 U.S. at 115 & n.10. And the subsequent government search required "physically intruding" on Petitioner's laptop. *Jones*, 565 U.S. at 406 n.3.[23]

This record is extraordinary because it is ordinary. The settled facts—a repair technician's discovery on a digital device followed by a government search—reflect "[o]ne of the most common factual situations giving rise to private search analysis in computer cases." Holley, *supra*, at 684; McJunkin, *supra*, at 984 (positing the "computer repair technician [who] stumbles upon illicit material"). In fact, DOJ guidance isolates this as the "common scenario" in which the government may use the private-search doctrine to search a computer without a warrant. Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 1, 11 (3rd ed. 2009). It is thus an appropriate, representative context in which to resolve these questions.

---

[23] The fact that the search here required physical intrusion on Petitioner's laptop means this record avoids the complexities that may arise in the context of digital searches that are wholly "virtual" or "electronic." *See Ackerman*, 831 F.3d at 1308; *Jones*, 565 U.S. at 426 (Alito, J., dissenting) (noting potentially "vexing problems" in trespass cases premised on "electronic, as opposed to physical, contact").

As mentioned, Petitioner's trespass argument was dismissed again and again as "inapposite," "not responsive," and "inapplicable" to reasonable-expectations analysis. Pet. App. 38a n.14, 84a n.3. This Court has held Petitioners accountable for preserving the property-based test as an independent theory. *E.g.*, *Byrd v. United States*, 138 S. Ct. 1518, 1526-27 (2018); *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting) (explaining litigants have had "fair notice since at least [2012] that arguments like these may vindicate Fourth Amendment interests even where *Katz* arguments do not," yet "forfeited [them] by failing to preserve them"). When defendants repeatedly assert the argument and lower courts refuse to accord it independent significance—relegating it to just a dismissive footnote, *see* Pet. App. 38a n.14, 84a n.3—the Court ought to take that seriously, too.

This Court has recognized that, upon reaffirming the property-based approach in *Jones*, it will have to address the protection it affords in increments. *Carpenter*, 138 S. Ct. at 2220 & n.4; *id.* at 2268 (Gorsuch, J., dissenting). This is the logical next step. This Court has already held that Part III of *Jacobsen*, upholding the agents' field test, does not survive the property-based approach. In that part of *Jacobsen*, the Court applied *United States v. Place*, 462 U.S. 696 (1983), to hold that a search which "discloses only the presence or absence of narcotics, a contraband item" is not a "search" under the Fourth Amendment. *Jacobsen*, 466 U.S. at 124. This was so even though the agents' field test intruded on the defendant's "possessory interests protected by the [Fourth] Amendment" and, indeed, did so in a "permanent" manner by "destroying a quantity of the powder." *Id.* at 124-25. Just a few

terms ago, a state invoked this part of *Jacobsen* to argue that a search "which merely reveals contraband, and no other private fact, compromises no legitimate privacy interest and, therefore, is not a search." Br. of Petitioner 16-17, *Jardines*, 569 U.S. 1 (2013) (No. 11-564), 2012 WL 1594294 (referring to "[t]he *Jacobsen* contraband exception"); *Jardines*, 569 U.S. at 10 (noting the state's reliance on *Jacobsen*). This Court rejected that argument. It explained that that this reasonable-expectations analysis was immaterial; "[t]hat the officers learned what they learned only by physically intruding on [the defendant's] property to gather evidence is enough to establish that a search occurred." *Jardines*, 569 U.S. at 11. So, indeed, this is just the next half step.

CONCLUSION

The Court should grant certiorari.

Respectfully submitted,

AMIR H. ALI
Counsel of Record
MEGHA RAM*
RODERICK & SOLANGE
MACARTHUR JUSTICE CENTER
777 6th Street NW, 11th Fl.
Washington, DC 20001
(202) 869-3434
amir.ali@macarthurjustice.org

Counsel for Petitioner

*Admitted only in California; not admitted in D.C. Practicing under the supervision of the Roderick & Solange MacArthur Justice Center.

NOVEMBER 2019