No. 19-1221

IN THE

Supreme Court of the United States

DERRICK LUCIUS WILLIAMS, JR.,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition for Writ of Certiorari to the United States Court of Appeals for the Tenth Circuit

REPLY BRIEF FOR PETITIONER

Josh Lee
FEDERAL PUBLIC DEFENDER
633 17th Street
Suite 1000
Denver, CO 80202

Shay Dvoretzky
Counsel of Record
Andrew J. M. Bentz
Parker Rider-Longmaid
JONES DAY
51 Louisiana Ave., NW
Washington, DC 20001
(202) 879-3939
sdvoretzky@jonesday.com

Counsel for Petitioner

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(continued)

Page(s)

STATUTES

INTRODUCTION

The government agrees that the circuits are split four ways on "the level and nature of the suspicion (if any) that is necessary to conduct a warrantless border search of an electronic device." Opp. 11. It does not contest that travelers arriving from abroad through Seattle, Dulles, Denver, and Miami receive different constitutional protections based solely on geographic accident. Nor does it advocate percolation—after all, in twelve majority and separate opinions, circuit judges have detailed every conceivable answer to the question presented. What's more, the government doesn't dispute that the question presented is extremely important. Nor does it bother defending the holding below that reasonable suspicion of *any* criminal activity—even of no particular crime at all, much less one with a nexus to the government's interests at the border—permits agents to rifle through a traveler's electronic devices.

Instead, the government invents vehicle concerns: Mr. Williams should have presented the Ninth Circuit's most recent decision to the Tenth Circuit earlier (he couldn't have); the Tenth Circuit did not reject the Ninth Circuit's rule (it did); Mr. Williams *might* have lost in the Fourth Circuit (he wouldn't have); and the Tenth Circuit did not decide whether the search here was "forensic" or "manual" (it doesn't matter). The first two arguments misrepresent the record. The latter two, at most, present remand questions. None would prevent the Court from deciding the question presented.

This Court's guidance is urgently needed. The Petition should be granted.

ARGUMENT

I. The government agrees that the circuit courts are divided four ways

A. As the Petition explained (at 2, 12–26), the circuits are divided four ways on the suspicion required for warrantless border searches of digital devices.

A traveler arriving in Los Angeles can rest assured, for border agents may search her electronic devices only on reasonable suspicion that the devices contain digital contraband. *United States v. Cano*, 934 F.3d 1002, 1007, 1020 (9th Cir. 2019) (Bybee, J.); *United States v. Cotterman*, 709 F.3d 952, 967–68 (9th Cir. 2013) (en banc).

A traveler arriving through Dulles receives a little less protection. Agents there need individualized suspicion that a device contains evidence of a particular offense with a "nexus to the border search exception's purposes of protecting national security, collecting duties, blocking the entry of unwanted persons, or disrupting efforts to export or import contraband." *United States v. Aigbekaen*, 943 F.3d 713, 721 (4th Cir. 2019); *see United States v. Kolsuz*, 890 F.3d 133, 143–44 (4th Cir. 2018).

But if the traveler lands in Denver, agents may search her devices on reasonable suspicion of *any* criminal activity. App. 8a–9a.

And if a traveler returns through Miami, agents may rummage through her devices with no suspicion whatsoever. *United States v. Touset*, 890 F.3d 1227, 1229, 1233–34 (11th Cir. 2018).

The split is outcome-determinative.

B. The government agrees that the circuit courts "have articulated different approaches." Opp. 11; *see* Opp. 14, 24–25 (acknowledging the approaches). It nonetheless wrongly urges this Court to abstain because the Ninth Circuit might go en banc in *Cano*.

First, the Ninth Circuit cannot resolve a four-way split. Even if it sides with another circuit, three different approaches will remain, including the Fourth Circuit's, under which Mr. Williams would have prevailed. *See infra* p. 10. Notably, the Fourth Circuit recently denied rehearing in *Aigbekaen*. Order, No. 17-4109 (Feb. 24, 2020).

This Court has granted review in comparable circumstances. In *Niz-Chavez v. Barr*, No. 19-863 (cert. granted June 8, 2020), for example, the Ninth Circuit had granted rehearing and a rehearing petition was pending before the Third Circuit. Cert was nonetheless warranted because the split would remain whatever either circuit did. Cert. Reply 4, *Niz-Chavez*.

If anything, the rehearing petition in *Cano reinforces* the need for this Court's review. Whatever efforts the Ninth Circuit might expend on *Cano*, the Fourth Circuit will still require reasonable suspicion of a border-related offense, while agents in the Eleventh Circuit will remain able to explore troves of data without any suspicion at all. Until this Court intervenes, geography will dictate constitutional rights, and further circuit-court efforts will be wasteful.

Second, the Ninth Circuit is unlikely to grant rehearing anyway. Not only is Judge Bybee's opinion correct, but it "clarif[ied] *Cotterman*," *Cano*, 934 F.3d at 1007, itself an en banc decision. The Ninth Circuit

has already considered—and rejected—the government's arguments.

Finally, what more could the en banc Ninth Circuit (or a separate opinion) add to the discussion? Circuit judges have advocated every possible approach to the question presented, from a warrant requirement to no suspicion at all. Pet. 13, 26. And regardless of any rehearing vote, *Cano* exposes serious concerns with other circuits' approaches. This Court is not bound by those approaches or the circuit scorecard. But it cannot ignore the urgent need for its guidance.

This Court's decisions in *Riley v. California*, 573 U.S. 373 (2014), and *Carpenter v. United States*, 138 S. Ct. 2206 (2018), are instructive. In *Riley*, the Court adopted the approach of the divided First Circuit, *United States v. Wurie*, 728 F.3d 1, 13 (1st Cir. 2013), *aff'd sub nom*. *Riley*—the lone circuit holding that the warrant exception for searches incident to arrest does not apply to cell phones, *see id.* at 16 (Howard, J., dissenting). In *Carpenter*, the Court again disagreed with the majority approach, instead holding, consistent with just one circuit court, that individuals may have reasonable expectations of privacy in their cell-site location information. *See* 138 S. Ct. at 2219; *United States v. Graham*, 824 F.3d 421, 428 (4th Cir. 2016) (en banc), *abrogated by Carpenter*. The Court had the benefit of multiple judges' views in "majority, concurring, and dissenting opinions, highlighting the need for this Court to act." Pet. 13, *Carpenter*, No. 16-402. Same here.

II. The government does not contest that the question presented is exceptionally important

A. As the Petition explained (at 26–31), the answer to the question presented will have "a profound impact on law enforcement practices at our ports of entry and on the individuals subjected to those practices." *United States v. Vergara*, 884 F.3d 1309, 1318 (11th Cir. 2018) (J. Pryor, J., dissenting). Many—likely most—people would reasonably expect their digital data to be private. So the millions of people crossing our borders every day deserve to know what protection (if any) the Fourth Amendment affords them. And the government needs to know what it may do to safeguard our borders. The circuit conflict is intolerable.

B. The government does not contest that the question presented is important and urgently requires this Court's attention. The closest the government comes is to equate "bypassing … password protection" on a digital device with "using a tool to open a locked briefcase," Opp. 19, and to highlight its "authority to conduct suspicionless inspections" of "a vehicle's fuel tank," Opp. 12 (quoting *United States v. Flores-Montano*, 541 U.S. 149, 155 (2004)).

Those responses don't wash. *Riley* rejected the argument that "a search of all data stored on a cell phone is 'materially indistinguishable' from searches of … physical items," such as baggies, wallets, and purses. 573 U.S. at 392–93. Digital devices hold vast amounts of data that can reveal "nearly every aspect of" a person's life. *Id.* at 393, 395. Equating the search of a digital device with the search of a briefcase or gas

tank is "like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Id.* at 393.

III. The Tenth Circuit's decision is wrong, and the government does not defend it

A. The Petition explained (at 31–34) that the Tenth Circuit wrongly concluded that reasonable suspicion of *any* criminal activity permits officers to search a traveler's laptop. *Riley* confirms that exceptions to the warrant requirement extend only so far as their rationales, 573 U.S. at 385–91, and the government has pointed to no need to search travelers' digital devices without reasonable suspicion tied to its border interests, much less any reason to think that requiring specific reasonable suspicion would threaten border security.

Most Americans would be shocked to learn that agents may copy their hard drives on a mere claim of suspicious circumstances with no connection to the government's border interests. Rightly—and reasonably—so.

B. Tellingly, the government neither defends the Tenth Circuit's approach nor attacks the Fourth Circuit's approach, under which Mr. Williams would have prevailed. *See infra* p. 10.

Instead, the government offers (at 23–24) a one-sentence argument that the Ninth Circuit erred in relying on *Boyd v. United States*, 116 U.S. 616, 623 (1886), to explain "the distinction between seizing goods at the border because their importation is prohibited and seizing goods at the border because they may be useful in prosecuting crimes." *Cano*, 934 F.3d at 1018. In the government's view, *Boyd* was overruled by *Warden v. Hayden*, 387 U.S. 294 (1967). Not so.

"*Hayden* rejects the 'mere evidence' rule that had long prevented the government from using warrants to obtain evidence that was not itself the instrumentality of a crime or contraband." *United States v. Molina-Isidoro*, 884 F.3d 287, 297 n.7 (5th Cir. 2018) (Costa, J., specially concurring). But "there are reasons to believe the distinction still matters when it comes to border searches"—among them, this Court's continued "rel[iance] on the detection-of-contraband rationale in supporting the government's broad border-search authority." *Id.*; *see also, e.g.*, *Aigbekaen*, 943 F.3d at 727 (Richardson, J., concurring in the judgment) (*Boyd* "purports to reflect the border-search doctrine's historical scope").

At best, the Ninth Circuit's reliance on *Boyd* reinforces the need for this Court's review: it reflects the circuits' vigorous disagreement about this Court's precedents. Just as this Court intervened in *Carpenter* to provide guidance on the application of Fourth Amendment principles to "the[] novel circumstances" presented by cell-site location information, 138 S. Ct. at 2217, it should intervene here to provide guidance on the Fourth Amendment's application to digital devices in the border-search context.

IV. This case is an excellent vehicle

A. This case is an excellent vehicle. It presents a clear legal question on undisputed facts. Mr. Williams would have prevailed in the Fourth and Ninth Circuits because agents did not have reasonable suspicion of a border-related crime (Fourth Circuit) or contraband (Ninth Circuit). Pet. 34.

B. Given the split, the government focuses principally on supposed vehicle problems. But all are illusory. And the government notably does not contend that any actually prevents this Court's review.

1. The government claims that "it is unclear that the [Tenth Circuit] understood petitioner to be advancing the specific reasonable-suspicion standard he now proposes." Opp. 16. It adds that Mr. Williams "did not properly preserve" a contraband-only argument based on the Ninth Circuit's standard. Opp. 22. Those claims misrepresent the proceedings below.

For starters, the Tenth Circuit rejected—and therefore "passed upon," *United States v. Williams*, 504 U.S. 36, 41 (1992)—both the Fourth and Ninth Circuits' standards. The Fourth Circuit requires individualized suspicion of a border-related offense. *Aigbekaen*, 943 F.3d at 721. The Ninth Circuit requires reasonable suspicion that a device contains digital contraband. *Cano*, 934 F.3d at 1007, 1020. Here, the Tenth Circuit expressly rejected Mr. Williams' argument that reasonable suspicion must be limited to violations of the laws "that border agents are tasked exclusively with upholding"—"customs laws and [laws against] the importation of contraband." App. 8a. It instead held that *any* form of reasonable suspicion suffices, because agents need not "close their eyes to suspicious circumstances." App. 8a–9a. That approach is now the law of the circuit and conflicts with the Fourth and Ninth Circuits' standards.

In addition, Mr. Williams *did* advocate both the Fourth Circuit's and Ninth Circuit's standards. *See* Petr's 10th Cir. Br. 10 n.2, 21–22, 25, 29–30, 39–40, 56 (citing *Kolsuz* (4th Cir.)); *id.* at 22, 40, 44–45, 55–57 (citing *Cotterman* (9th Cir.)); Petr's 10th Cir. Reply 4–

5, 15–16, 19–20 (citing *Kolsuz*); Petr's 10th Cir. Reply 6, 15 & n.7, 16 (citing *Cotterman*). In fact, the government even *quotes* Mr. Williams' opening brief as arguing that a search is valid only on reasonable suspicion of "a 'violation of one of the Government's border interests,'" *i.e.*, "'that [petitioner] wasn't entitled to enter the country, that he was carrying contraband, or that he was evading customs duties.'" Opp. 18 (quoting Petr's 10th Cir. Br. 27). That is precisely what the Fourth Circuit holds. *Aigbekaen*, 943 F.3d at 721. Nothing was "unclear" to the Tenth Circuit, Opp. 16, as oral argument confirms. https://www.ca10.uscourts.gov/oralarguments/18/18-1299.MP3.

To be sure, Mr. Williams cited *Cano* in a 28(j) letter. Opp. 22–23. But the government misleadingly omits that Mr. Williams filed that letter *the day* Cano *issued* (Aug. 16, 2019)—over a month before oral argument (Sept. 24, 2019); that the government responded on the merits, contending that "the Ninth Circuit gets it wrong" (without raising any procedural objection), Gov't 10th Cir. 28(j) Resp. (Aug. 29, 2019); and that the Fourth and Ninth Circuits' standards were a focus of oral argument, with judges asking questions about the type of suspicion required. Unsurprisingly, the Tenth Circuit said nothing about forfeiture.*

---

* The government's reliance (Opp. 23) on *United States v. Kimler*, 335 F.3d 1132, 1138 n.6 (10th Cir. 2003), is misplaced for the additional reason that it centers on failure to timely raise *issues* rather than *arguments* and whether "the arguments are based on authority that was readily available at the time of briefing." *Id.* Mr. Williams raised the reasonable suspicion *issue* in his opening brief, and cited *Cano* the day it issued.

2. The government next contends (at 21) that Mr. Williams would have lost in the Fourth Circuit. (Notably, it does not say that about the Ninth Circuit.) Whether Mr. Williams would have prevailed under the Fourth Circuit's rule is at most a remand question. But, in any event, the Tenth Circuit did not suggest, and the government has not shown, that Mr. Williams would have lost in the Fourth Circuit. The Tenth Circuit did not find reasonable suspicion of any particular crime, much less a border-related offense.

The government has never identified any offense "bear[ing] some nexus to the border search exception's purposes" either. *Aigbekaen*, 943 F.3d at 721; *see* Petr's 10th Cir. Reply 19–23. Mr. Williams' past crimes, evasions about overseas travels, and listing a different address for return of his devices do not establish reasonable suspicion of any border-related offense. The generic crime of lying to a federal official, 18 U.S.C. § 1001, is not such an offense, and the Tenth Circuit did not so hold. Mr. Williams, as a U.S. citizen, was admissible. And there was no suspicion that he was smuggling contraband.

3. Finally, the government argues that no court has decided whether the search here was "forensic" or "manual," and that "a reasonable-suspicion standard should apply [only] to a 'forensic' search." Opp. 14–15, 19–20. Those arguments are meritless.

First, whether the search was "forensic" is at most a remand question. There is nothing logically "antecedent" (Opp. 20) about it. If this Court were to decide that agents must have reasonable suspicion only for a "forensic" search, it could remand for further proceedings about the kind of search. The Ninth Circuit did just that in *Cano*. 934 F.3d at 1021 & n.12.

Second, Mr. Williams has consistently maintained that the Fourth Amendment's protections do not turn on whether a search is "forensic" or "manual." Petr's 10th Cir. Reply 1–13. This Court drew no such distinction in *Riley*, and, contrary to the government (Opp. 19), the Fourth Circuit has noted that *Riley* may "call[] into question the permissibility of suspicionless manual searches." *Kolsuz*, 890 F.3d at 146 n.5.

Third, the search here *was* "forensic." "Manual" searches "are examinations of an electronic device that do not entail the use of external equipment or software." *Id.* at 146 n.6. "Forensic" searches, by contrast, "involve the connection of external equipment to a device … in order to review, copy, or analyze its contents." *Id.*

The government necessarily concedes that the search was "forensic" under that rubric: "[T]wo HSI computer forensic agents" carrying "'forensic equipment' to attempt to bypass passwords" could not unlock Mr. Williams' laptop. Opp. 4–6. Only after making "a copy of the laptop's hard drive" at "an HSI office" "[u]sing more advanced software"—EnCase, App. 5a, which "exhibit[s] the distinctive features of computer forensic examination," *Cotterman*, 709 F.3d at 963 n.9—could an agent "bypass the laptop's password and generate a list of the hard drive's contents, including deleted folders." Opp. 6. That doesn't sound like an ordinary user's "accessing the hard drive through the laptop." Opp. 7 (quoting App. 20a); *infra* p. 12.

The government also contends, citing two unpublished district court cases (at 20), that using software to bypass a password doesn't make a search "forensic." But agents didn't circumvent a password in *United States v. Smasal*, No. 15-cr-85, 2015 WL

4622246, at *8 (D. Minn. June 19, 2015), and did not use technology to guess the defendant's password in *United States v. Lopez*, No. 13-cr-2092, 2016 WL 7370030, at *1, *4, *6 (S.D. Cal. Dec. 20, 2016). The government's other case, *United States v. Saboonchi*, 990 F. Supp. 2d 536 (D. Md. 2014), doesn't help either. In finding the search there "forensic," the court focused on whether the officer went beyond the "way that a typical user would use" her device, *id.* at 547, noting that agents used specialized software to make a "bitstream copy" that they could retain to "peruse[] at a later date," *id.* at 564–66. That's what happened here too. App. 5a, 15a, 19a; *see also* Petr's 10th Cir. Br. 9–10.

* * *

The government agrees there is a four-way split on an issue of indisputably great importance. Its only arguments against cert are manufactured vehicle concerns. This case is an excellent vehicle, and both travelers and the government urgently need this Court's guidance.

CONCLUSION

The Petition should be granted.

July 7, 2020

Respectfully submitted,

Josh Lee
FEDERAL PUBLIC DEFENDER
633 17th Street
Suite 1000
Denver, CO 80202

Shay Dvoretzky
Counsel of Record
Andrew J. M. Bentz
Parker Rider-Longmaid
JONES DAY
51 Louisiana Ave., NW
Washington, DC 20001
(202) 879-3939
sdvoretzky@jonesday.com

Counsel for Petitioner